CAHIERS DE L'ASSOCIATION INTERNATIONALE DU DROIT DE LA MER

PAPERS OF THE INTERNATIONAL ASSOCIATION OF THE LAW OF THE SEA

9

CAHIERS DE L'ASSOCIATION INTERNATIONALE DU DROIT DE LA MER
PAPERS OF THE INTERNATIONAL ASSOCIATION OF THE LAW OF THE SEA

SICUREZZA UMANA NEGLI SPAZI NAVIGABILI: SFIDE COMUNI E NUOVE TENDENZE

HUMAN SECURITY IN NAVIGABLE SPACES: COMMON CHALLENGES AND NEW TRENDS

A cura di / Edited by

GIORGIA BEVILACQUA

EDITORIALE SCIENTIFICA

2021

Protecting HUman SEcurity with non-state-actors in the MARitime and CYber SPAce – HUMARCYSPASE

Nel Volume, realizzato grazie ai fondi della misura Open Access, VALERE 2020, sono confluiti i risultati dell'indagine svolta nell'ambito del progetto di ricerca interdisciplinare *Protecting HUman SEcurity with non-state-actors in the MARitime and CYber SPAce – HUMARCYSPASE*, finanziato dal Programma VALERE 2020: VAnviteLli per la RicERca, dell'Università della Campania *Luigi Vanvitelli*.

The volume, funded by the Open Access measure, VALERE 2020, includes the results of the research carried out within the interdisciplinary research project *Protecting HUman SEcurity with non-state-actors in the MARitime and CYber SPAce – HUMARCYSPASE*, funded by the VALERE 2020 Program of the University of Campania *Luigi Vanvitelli*.

Ringraziamenti/Acknowledgments

Desidero rivolgere i miei più sinceri ringraziamenti ai membri dell'unità di ricerca di Humarcyspase, che hanno creduto in questo progetto di ricerca e lo hanno supportato in ogni sua fase con impegno e dedizione. Sono particolarmente grata ad Ana Nikodinovska Krstevska e Olga Koshevaliska, le colleghe e amiche macedoni che ho sentito molto vicine, nonostante la distanza geografica. A voi tutti: "grazie e *ad maiora*"!

I would like to address my most sincere acknowledgemnts to the members of the Humarcyspase research unit, who trusted this research project and, with commitment and dedication, supported it in each implementing phase. I am especially grateful to Ana Nikodinovska Krstevska and Olga Koshevaliska, the Macedonian colleagues and friends that I felt nearby notwithstanding the geographical distance. To you all: "many thanks and *ad maiora*"!

Università
degli Studi
della Campania
Luigi Vanvitelli

Via San Biagio dei Librai, 39 – 80138 Napoli
www.editorialescientifica.com – info@editorialescientifica.com

ISBN 979-12-5976-142-2

INDICE / CONTENTS

ELENCO DELLE ABBREVIAZIONI / LIST OF ABBREVIATIONS

In italiano

CEDU	Convenzione Europea dei Diritti dell'Uomo
CGUE	Corte di Giustizia dell'Unione europea
Corte EDU	Corte Europea dei Diritti dell'Uomo
EMSA	Agenzia Europea per la Sicurezza Marittima
EUROSUR	Sistema di Sorveglianza delle Frontiere
IA	Intelligenza Artificiale
JRCC	Centro congiunto di ricerca e salvataggio
OCSE	Organizzazione per la Cooperazione e lo Sviluppo economico
OIM	Organizzazione Internazionale per le Migrazioni
OMPI	Organizzazione Mondiale della Proprietà Intellettuale
ONG	Organizzazioni Non Governative
OUA	Organizzazione dell'Unione Africana
UE	Unione Europea
UNHCR	Alto Commissariato delle Nazioni Unite per i Rifugiati
WSIS	Summit Mondiale sulla Società dell'Informazione

In English

AI	Artificial Intelligence
BAMF	German Asylum office
BIMS	Biometric Identity Management System
CDA	Communications Decency Act
DMCA	Digital Millennium Copyright Act
DSA	Digital Service Act
EASO	European Asylum and Support Office
ECHR	European Convention of Human Rights
ECN	European Counter-Information Network
ECtHR	European Court of Human Rights
EIGE	European Institute for Gender Equality
EMODnet	European Marine Observation and Data Network
EU	European Union
EUNAVFOR Med	European Union Naval Force in the South Central Mediterranean

EUROPOL	European Union Agency for Law Enforcement Cooperation
FRONTEX	European Border and Coast Guard Agency
GDPR	General Data Protection Regulation
IACS	International Association of Classification Societies
ICC	International Criminal Court
ICRC	International Committee of the Red Cross
IHL	International Humanitarian Law
ILC	International Law Commission
ILO	International Labour Organization
IMB	International Maritime Bureau
IMO Cyber Risk Resolution	Maritime Cyber Risk Management in Safety Management Systems Resolution'
IMO	International Maritime Organisation
IMOSAR	Search and Rescue Manual
ISM	International Safety Management
ISO	International Standardization Organization
ISP	Internet Service Provider
ISPS Code	International Ship and Port Facility Security Code
IT	Information Technologies
MAS	Multipurpose Aerial Surveillance
MERSAR	Merchant Ship Search and Rescue Manual
MOAS	Migrant Offshore Aid Station
MRCCs	Maritime Rescue Coordination Centres
MSC	IMO's Maritime Safety Committee
NCP	Non Consensual Pornography
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OES	Operators of Essential Services
OHCHR	Office of the United Nations High Commissioner for Human Rights
OT	Operational Technologies
P2P	Peer-to-peer
RHIBs	Rigid-hulled inflatable boats.
SAR	Search and Rescue
SMCs	Safety Management Certificates
SMS	Safety Management System
SOLAS	Convention on the Safety of Life at Sea
SPs	Security Packs (I and II)
SRR	Search and Rescue Region
UNCLOS	United Nations Convention on the Law of the Sea
UNCTAD	United Nations Conference on Trade and Development
UNHCR	United Nations High Commissioner for Refugees

PREFACE ON NAVIGABLE AND UNREGULABLE SPACE(S)

Mireille Hildebrandt

While a president of the United States trumpeted his plans to build a wall against immigration from Mexico, Europe faced another type of wall, made of water. The Mediterranean Sea marks the borderline between Europe and Africa. It is used as a passage from one continent to another by those wishing to flee their homeland due to war and civil war, famine, economic deprivation, an unsafe environment or, alternatively, ambition and entrepreneurial zest, coupled with a willingness to accept high risk high gain. Like the wall against Mexican immigration, the Mediterranean Sea is also used as a fence to stop those wishing to make the passage, criminalising not merely those attempting the crossing but also those who come to their rescue. In Madjidian's chapter in this Volume on the civil rescue fleet in the Mediterranean we read that "[i]n the aftermath of the Arab uprisings, migration across the Mediterranean has increased. The International Organisation on Migration ("IOM") estimates that since the beginning of 2014, at least 20,000 migrants have died trying to reach European shores".[1]

In his penetrating work on the figure of the migrant,[2] Thomas Nail invites the reader to inverse their usual default position, asking to no longer see migration as the exception to the rule, acknowledging that for most of human history we have been nomads. We may foresee 'returning' to an era where sedentary life is what needs an explanation, rather than migration. Indeed, climate change and geopolitical disruptions may uproot comfortable assumptions about mutually exclusive sovereign states that respect the principle of non-intervention with the intent of being left in peace themselves. Nail's salient work reminds me of Jean-Marie Guehenno's 1993 prophetic *The end of democracy*,[3] where Guehenno foresaw the implications of a global elite that finds easy passage across the world while (their) transnational companies engage in tax shopping, thus endangering the loyalty as well as the income that enables states to function and protect their (and other) citizens. Nail's work proposes a radical reconfiguration of our common sense, reminding us that if land were to become an *unregulable passage*, *navigable* only for those with greater military force or economic power, most of us would be in a bad place. Taking note that, at the global level, this radical inversion of the narrative on statehood, migration and belonging may have been the default all along, with so many people being subject to myriad forces that push them from one place to another – including the

[1] Taken from the website of International Migration Organisation (IMO) Missing Migrants Project, <https://missingmigrants.iom.int>.

[2] T. Nail, *The Figure of the Migrant*, Stanford University Press, 2015.

[3] J. M. Guéhenno, *La Fin de la démocratie*, Flammarion, 1993.

economic forces that drive urbanisation, the politics of authoritarian regimes or the perverse incentives that invite human trafficking.

Simultaneously, the global information and communication infrastructure (which is now largely dependent on *mobile* devices) has created a new kind of spatiality that does not consist of mutually exclusive territories but instead situates individuals, corporations and states in myriad overlapping contexts despite them remaining in the same location. Think of working from home, a coffeeshop or from a hospital bed; discussing family matters online from one's office or while commuting; running a team during one's holiday via remote video conferencing; paying via one's mobile phone or transferring crypto currencies to obtain a non fungable token (NFT). More to the point, think of a person or a corporation staying or being established in one state while working in another, doing business across borders, hacking into computing systems on another continent, spreading deep fakes to disrupt elections within another state or conducting cyberattacks against critical infrastructure of another state without declaring war – all situations where the effects of actions taken in one jurisdiction have major repercussions in another. This new spatiality, coined cyberspace, has provoked a comparison with the waters between continents. Like the high seas, cyberspace seems to be a passage between more solid spaces, allowing people to escape, meet or trade. And like the high seas cyberspace has been framed as an *unregulable* space that provides freedom from state interference.

The high seas have preserved some of their claimed unregulability, even if based on global treaties rather than natural properties. Cyberspace has, on the contrary, become a densely regulated space, consisting of portals, platforms, service providers and a set of walled gardens whose 'jurisdiction' regulates by way of a convoluted mixture of technical protocols, optimisation machines that nudge their users into preferred behaviours and a tight net of Terms of Service, consent buttons and default settings. Concurrently, states have imposed extraterritorial jurisdiction to face the implications of cyberspace-induced deterritorialization, grasping for ways to fight cybercrime, including cybersecurity attacks, child abuse, identity fraud and soon to be expected unlawful remote control over cyberphysical infrastructure in the case of the internet of things. The claimed unregulability of cyberspace has paradoxically resulted in an excess of competing technical and legal regulation, pushing sovereignty out of the boundaries that shaped both its absolutist tendencies and the 'practical and effective' protections offered by a rule of law that depends on territorial jurisdiction.[4]

Let's therefore return briefly to Grotius' famous *Mare Liberum*,[5] about the

[4] See my previous work on these issues 'Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace', *University of Toronto Law Journal*, 2013, p. 196; 'The Virtuality of Territorial Borders' *Utrecht Law Review*, 2017 <http://www.utrechtlawreview.org/articles/abstract/10.18352/ulr.380/> (08/17); and 'Text-Driven Jurisdiction in Cyberspace', in M. O'Flynn, L. Farmer, J. Hornle, D. Ormerod (eds), *The Transformation of Criminal Jurisdiction: Extraterritoriality and Enforcement* (forthcoming, Hart Publishing), OSF Preprints <https://osf.io/jgs9n/> (05/21).

[5] H. Grotius, *Free Sea,* first published by Elzevir 1609, *With William Welwod's Critique & Grotius's Reply* Introduction by D. Armitage (Liberty Fund, 2004).

freedom of the high seas. Grotius wrote it as an assignment of the Republic of the United Netherlands and the United East India Company, whose interests had to be protected against claims by the Spanish and the Portuguese over a passage that happened to be crucial to Dutch trade. His treatise won out over John Selden's *Mare Clausum* that argued the opposite,[6] claiming that the high seas, just like land, can be occupied, divided and treated like private or public property. *Mare Liberum* was not a naïve idealistic praise for freedom from sovereignty. Rather on the contrary, the ingenuity of Grotius work resides in arguing for the need to secure both sovereign independence from higher authority (internal and external sovereignty) and the interdependence of sovereign states (supposedly bringing peace and general well-being). The latter required both unhindered access to the high seas, framed as a passage between states involved in trade relationships, while also justifying sovereign defence against those endangering such trade (notably pirates). This justification was even claimed to justify *bellum justum privatum* (a just private war) or *coophandel met force* (trade supported by the private force of arms), based on Grotius' detailed exposition of what natural law allows and requires both states and private enterprise in the passage between lands.

Grotius' work has withstood the test of time because of the complex and intricate argumentation he put forward, allowing sovereign states to have their cake (independence from higher authority) and eat it too (interdependence as to their mutual economic relationships). His argument for a 'natural law of the seas' is often compared to John Perry Barlow's *Cyberspace Manifesto* on internet freedom. Compared to Grotius' seminal work, this Manifesto, which declared that states had no business on the internet, was an idealistic and dangerously naïve celebration of freedom as a space without constraints. Whereas a person sailing the high seas is not also on land, a person navigating 'cyberspace' will always also navigate 'real' space. Our embodied nature is rooted in a body that is always physically located at one place, even though our mind has been capable of traveling time and space even before we started writing. In that sense our embodiment has never stopped us from inhabiting various spaces simultaneously, due to the particular affordances of human language. For instance, when speaking with others about elsewhere, past and future, or when reading about whatever is not present in the here and now, we develop a timespace that is distinct from our embodied self. The Manifesto's exceptionalism, proclaiming a realm where governments have no authority was mistaken on two accounts. First, because governments have found many ways to exercise various types of control over what goes on in 'cyberspace' whenever it interferes with their interests, often resulting in an excess of governmental interference. Second, because to the extent that government authority has indeed been lacking, it did not deliver freedom but a new type of servitude, developed and controlled by large technology companies that configure our choice architecture in a hybrid online-offline world.

This salient Volume addresses the challenges posed by both *a lack* and *an ex-*

[6] J. Selden and M. Nedham, *Of the Dominion, or, Ownership of the Sea*, (first published by William Du-Gard 1652) The Lawboo.Exchange, 2004.

cess of sovereign power, both in the high seas and in cyberspace. More specifically it details the legal and a-legal position of migrants, most notably those traversing the Mediterranean Sea to seek refuge from political and economic hardship. The work highlights migrants' crossings in the unregulable spaces of Mediterranean waters and global cyberspaces, demonstrating in salient detail the competing jurisdictions that rule either spaces, consisting of a diversity of legislators, courts, justice authorities and police (EU, member states, Turkey, Libia) and EU agencies such as the European Police Agency (Europol), the European Border and Coast Guard Agency (Frontex), deploying systems such as the European Travel Information and Authorisation System (Etias), the European fingerprint database Eurodac, the Schengen Information System (SIS), the European Border Surveillance system (EUROSUR), which use myriad technologies to monitor, trace and track migration, from various types of biometrics (iris scanning, fingerprints), online surveillance (location and traffic data, social media postings, online behavioural data) to questionable techniques based on machine learning (to decide on reliability of refugee narratives).[7] The recently proposed EU AI Act should contribute to much needed quality control as well as to proper assessment of risks to fundamental rights.[8]

We urgently need legal, political and technological reconfigurations of cyberspace to reinvent and sustain it as a safe space. We need to explore and develop the idea and the practice of an international rule of law,[9] to make sure that individuals can *navigate* the mobile, dynamic and polymorphous spatiality that 'makes' cyberspace. At the same time, we must ensure that the high seas become *regulable* from the perspective of human rights. Neither cyberspace(s) nor the Mediterranean Sea should be free from the constraints that protects the vulnerable from the powerful. We must work to make these spaces navigable and regulable in ways that support and enable individual human agency, while ensuring that those in power treat those under their jurisdiction with equal concern and respect. Liberty without equality is *un*freedom; equality without liberty is empire (even if empire could harness unfreedom too).

[7] E. Fournier-Tombs, 'The United Nations Needs to Start Regulating the "Wild West" of Artificial Intelligence', *The Conversation*, 31 May 2021 <http://theconversation.com/the-united-nations-needs-to-start-regulating-the-wild-west-of-artificial-intelligence-161257> (09/21).

[8] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, 21.4.2021 COM(2021) 206 final. See notably Annex III under point 7.

[9] J. Waldron, 'The Rule of International Law', *Harvard Journal of Law & Public Policy*, 2006, pp.15-30.

INTRODUZIONE / INTRODUCTION

HUMAN SECURITY IN NAVIGABLE SPACES: A PREMISE

Giorgia Bevilacqua

The differences that would normally lead us to distinguish clearly and unequivocally between maritime space and cyberspace make it necessary to introduce the characteristics common to these two spaces (hereafter navigable spaces); commonalities that have made it profitable to analyze them together in the research project "HUMARCYSPACE – Protecting HUman SEcurity with non-state-actors in the MARitime and CYber SPAce".

We will begin by reviewing the origins of navigable spaces.

It is common knowledge that in antiquity the seas and oceans were considered completely free and open spaces. This was because the principle of freedom of the seas was for centuries the only rule that States could and should comply with in (almost) all marine spaces. On the basis of this legal principle, the use of such spaces had to be guaranteed to all States. The only real limit that this principle encountered was that which is typical of all regimes of freedom: in essence, respect for the equal freedom of others. It was therefore inadmissible if a State demanded to close certain zones of the sea to navigation.[1]

The expectation of a regime of freedom and the separation that it involves between sea and land, articulated in a famous study by the German legal expert Carl Schmitt,[2] draws our attention to the origins of the other space dealt with by our research: cyberspace. In the 1990s, at the time the internet was created, the Manifesto on cyberspace announced the birth of new technologies that would resist the application of territorial borders.[3] The advent of the internet would mark the end of the Nation-State based on States' mutual recognition of territorial sovereignty. Geographical borders would have no meaning in cyberspace. And, since the internet could not correspond to a real physical space, it followed that within it States would not be able to exercise the same sovereign powers that they would normally exercise on land.[4]

Just as scholars in the past held that maritime space should be given a different spatial conception, by virtue of which it could not be divided into reciprocal and exclusive jurisdictions,[5] so too did the early authors of cyberspace challenge the ex-

---

[1] B. Conforti, *Diritto internazionale*, XI Ed., Editoriale Scientifica, Napoli, 2021, p. 298 ff.

[2] C. Schmitt, *Il Nomos della terra*, Adelphi, Milano, 1998.

[3] J. P. Barlow, *A Declaration of the Independence of Cyberspace*, Switzerland, 8 February 1996, <https://www.eff.org/it/cyberspace-independence>.

[4] M. Hildebrandt, "Extraterritorial Jurisdiction to Enforce in Cyberspace: Bodin, Schmitt, Grotius in Cyberspace", *University of Toronto Law Journal*, 2013, pp. 196-224.

[5] U. Grozio, *Mare Liberum*, Liguori Editore, Napoli, 2007.

clusive exercise of sovereign powers on the web according to a territorial basis. Indeed, they argued that virtual spaces, like the seas and oceans, could not be divided with physical borders, and for this reason could not be subjected to the traditional exercise of territorial sovereignty. In other words, in the period when a legal system applicable to navigable spaces was conceived, territory could not be an object or a constitutive element of sovereignty, much less one of the spatial domains in which the sovereignty of a State is exercised and protected by international law.[6]

We will next describe a second aspect we believe navigable spaces have in common, and one that appears to be closely related to the incalculable importance such spaces have for all human beings. All through their history, navigable spaces, as well as being considered open and free, have been seen as particularly important resources for people's survival, development, and progress.

As early as the seventeenth century, the author of *Mare Liberum* explained that goods like the sun, air, and also the sea should remain accessible to everyone, given that these were gifts offered by nature to all of humanity. Over the years this conviction has strengthened. Today, on one hand scientific studies have demonstrated that marine spaces are indispensable to the survival of people on earth. Consider, for instance, the fact that over half of the oxygen we breathe comes from marine organisms, or that the seas and oceans do much to regulate the world's climate, insofar as they absorb a significant part of the carbon dioxide emissions released by human activities. On the other hand, we must recall that a series of activities take place in marine spaces that are essential for people's progress and development, ranging from the procurement of food to commercial and recreational activities.[7]

As regards cyberspace, while it would be pushing credibility to consider this a natural resource, it is less of a stretch to view it as a common good that should remain accessible to all its users. Right at the beginning of its development, in the aforementioned Manifesto, cyberspace was defined as "the new home of Mind".[8] And in this case, too, the idea that its space was of vital importance to people's survival, development, and progress has gradually strengthened. On 28 July, 2015, in the Preamble to the Declaration of Internet Rights, the Italian Parliament's Commission for Internet Rights and Responsibilities declared explicitly that "the internet has contributed decisively to a redefinition of public and private space, and to struc-

[6] On the relevance of territory for the exercise of state sovereignty on the mainland according to international law, see Conforti, cit., *supra* note 1, p. 210; R. Quadri, *Diritto internazionale pubblico*, VIII Ed., Liguori, Napoli, 1968, p. 633; M.C. Vitucci, voce "Territorio (dir. int.)", in Treccani.it, 2014, <http://www.treccani.it/enciclopedia/territorio-dir-int_(Diritto-on-line)>. On sovereignty, see J. Crawford, *Brownlie's Principles of Public International Law*, XI Ed., Oxford University Press, Oxford, 2019, p. 422 ff. For an overview of the theories regarding the legal nature of territory and the analysis of some issues posed to international law concerning both maritime and cyberspace (but also other international spaces), see C. Cinelli, *La disciplina degli spazi internazionali e le sfide poste dal progresso tecnico-scientifico*, G. Giappichelli Editore, Torino, 2020.

[7] In this respect see European Commission, Report to the European Parliament and the Council on the Implementation of the Marine Strategy Framework Directive (Directive 2008/56/EC), Brussels, 25 June 2020.

[8] Barlow, cit. *supra* note 3.

turing the relationships among people and between people and institutions. It has eliminated borders […]. It has [further] enabled the development of a more free and open society".[9] In virtually analogous fashion, except on an international level, the Parliamentary Assembly of the Council of Europe, in a Resolution from 2019 dedicated to the governance of the internet and human rights, explained specifically that:

> [t]he internet is *a common good* and universal access [to it] is a key internet governance principle. This is because the uses of the internet can influence many aspects of our daily life. The internet indeed provides modern societies with more information and knowledge, innovation and sustainable development, social justice and collective well being, freedom and democracy.[10]

There is an additional element that has led us to analyze these two spaces together, in spite of the differences that exist between them in principle: the fact that even though numerous scientific and institutional contexts have recognized the extraordinary importance of navigable spaces for all human beings, this has not prevented the progressive erosion of the regime of freedom that marine and later virtual spaces have enjoyed.[11]

So far as marine spaces are concerned, while the theoretical distinction between land and sea might continue to seem valid and effective, it is well known that for several centuries coastal States have expressed claims to so-called freedom of the seas.[12] And while the possibility of occupying a marine space continues to cause perplexity, the idea that whatever spaces are not on land should remain accessible to all corresponds by now to an antiquated notion of international maritime law. With the 1982 United Nations Convention on the Law of the Sea (UNCLOS), state jurisdiction over the sea was established (almost) definitively. As is well known, in accordance with this Convention, the ancient principle of freedom of the seas was scaled back in its content and circumscribed to a more limited area of water than in the past: the high seas. In the UNCLOS, the high seas correspond to an undefined geographic area that includes all the zones of sea that fall outside the jurisdiction of coastal States. And even if, in principle, the high seas should be subject to the regime of freedom described above, even here States have made and continue to make numerous attempts to extend their powers of jurisdiction.[13] This may happen

---

[9] Camera dei deputati (Commissione per i diritti e i doveri relativi ad Internet), *Dichiarazione dei diritti in internet*, 28 July 2015, preamble, <https://www.camera.it/leg17/1179>.

[10] Parliamentary Assembly of the Council of Europe, Resolution 2256 (2019), Internet Governance and human Rights, 23 January 2019, <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=25407&lang=en>.

[11] As regards international law on the mainland, an opposite process seems to be in force, i.e., the process of deterritorialization. See E. Milano, "The Deterritorialization of International Law, Setting the Context", in A. Di Stefano (ed.), *A Lackland Law? Territory, Effectiveness and Jurisdiction in International and EU Law*, Vol. I, Giappichelli, Torino, 2015, p. 53 ff.

[12] Conforti, cit. *supra* note 1, p. 300 ff.

[13] B. Conforti, "Does Freedom of the Seas still Exist?", *The Italian Yearbook of International Law*,

for various sorts of reasons. By way of example, we may recall news stories concerning the repeated abductions of Turkish and Italian fishermen.[14] These abductions take place because, since the 1970s, successive governments in Libya have tried to widen the exercise of their sovereign powers, especially those concerning fishing, into territorial waters extending more than seventy miles off the Libyan coast, considerably beyond the distance stipulated in the UNCLOS.

As regards virtual spaces, it seems, in a manner that is almost analogous to the situation for the seas, that States tend to exercise their sovereignty and their control of information, images, and personal data even when these are not located, or at any rate are not stored, on their national territory. In the United States, for example, the "Clarifying Lawful Overseas Use of Data (CLOUD) Act" has recently modified existing legislation, giving US law enforcement and intelligence agencies the power to obtain personal data from cloud computing companies irrespective of where those data happen to be located, and therefore even if they are stored on servers outside US territory.[15] Today, issues of encroachment in the treatment of personal data arise not only in relation to the activities performed by public bodies, but also by private organizations. A recent ruling by the Court of Justice of the European Union, for instance, originates in a complaint filed by an Austrian user of the social network Facebook, requesting that the Irish authorities prevent Facebook Ireland from transferring his personal data to Facebook Inc. in the United States.[16]

In spite of the intention shown by national States at various times, and in different ways, to exercise their sovereign powers in navigable spaces, and thus in spite of the progressive erosion of the original regime of total openness and freedom that characterized such spaces, our research demonstrates how the peculiarities of these spaces may favor the spread of illegal and criminal activities. That makes the need to promote the security of those navigating both the seas and the web particularly acute.

In this respect, it should be understood that over the last few decades the concept of security has undergone a profound transformation. While for the majority of the twentieth century the term "security" was used in reference to the system put in place by States to protect their national interests from the claims of other States, after the end of the Cold War security continued to be a subject that captured the attention of institutions, scholars and the media at a national and international level, only its classical definition was now brought into question. A search began for a

---

1975, p. 5 ff.; G. Hofner, "Does Freedom of the Seas still Exist?", in J. Crawford, A. G. Koroma, S. Mahmoudi, A. Pellet (eds.), *The International Legal Order: Current Needs and Possible Responses*, Brill|Nijhoff, Leiden, Boston, 2017, p. 346 ff.

[14] *Libya's Gen Haftar Frees Italy Fishermen held for months*, <https://www.bbc.com/news/world-europe-55361700>.

[15] The United States Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, White Paper, April 2019, <https://www.justice.gov/opa/pressrelease/file/1153446/download>.

[16] Court of Justice of the European Union, C-311/18, *Facebook Ireland and Schrems*, Judgment of 16 July 2020.

new model of security that would be more inclusive, and above all more compatible with the new world order. There gradually emerged new categories of security, and alongside the security of the Nation-State there now came specific concepts such as transport security and environmental security. In the spaces analyzed here, discussion revolves around maritime and cyber security. However, concepts also began to emerge that were completely new and transversal, for example global security and bio-security.[17] The new category we intend to refer to here is human security.[18]

At international level the first discussion of human security seems to have taken place in 1982, in a report by the Palme Commission (named after the Swedish statistician, Olof Palme, who led it) which was formed to examine international security problems.[19] The idea at its basis was that individuals were no longer consubstantial with the State. The pairing of the words "human" and "security" in a single phrase is aimed at promoting the role of individuals more effectively. The appeal to humanity has a universal and nondiscriminatory ring to it, and is thus to the benefit of everyone.

In the 1990s this new concept of security began to be discussed in the United Nations as well. In the *Human Development Report*,[20] it is explained that the new multidimensional threats to security no longer come from States and are no longer directed at States. Similarly, in the subsequent report of the High-level Panel on Threats, Challenges and Change, called *A More Secure World: Our Shared Responsibility*, a reconceptualization of security is advanced that entails the need to place human security alongside state security. It is acknowledged that the world is dealing with new threats, or at least perceives new threats.[21] This report came in the period following the Cold War, when, rather than being killed in an armed attack, people were more likely to die from infectious diseases, famine, natural catastrophe, a terrorist attack or some other form of transnational crime; all of these threats that came from both States and non-state actors, and which threatened both States and non-state actors. Subsequently, in a General Assembly Resolution containing the results of the 2005 World Summit, greater clarity was given to the "right of people to live

---

[17] On the concept of bio-security, see P. L. Deziel, "La naissance de la biosécurité", *Raisons politiques,* 2008, pp. 77-93.

[18] On the concept of human security, see, among others, L. Axworthy, "La sécurité humaine: la sécurité des individus dans un monde en mutation", *Politique étrangère,* 1999, pp. 333-342; C. Focarelli, *La persona umana nel diritto internazionale*, Il Mulino, Bologna, 2013, p. 54; R. Paris, "Human Security: Paradigm Shift or Hot Air?", *International Security*, 2001, pp. 87-102; O. Richmond, "Human Security, the 'Rule of Law,' and NGOs: Potentials and Problems for Humanitarian Intervention," *Human Rights Review*, 2001; P. Stoett, *Human and Global Security: An Exploration of Terms*, Toronto: University of Toronto Press, 1999.

[19] Independent Commission on Disarmament, *A Common Security: A Blueprint for Survival*, 1982.

[20] UN Development Programme, *Human Development Report*, Oxford University Press, New York-Oxford, 1994, <http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf>.

[21] UN Department of Public Information, *More Secure World: Our Shared Responsibility, Report of the High-Level Panel on Threats, Challenges and Change*, UN Doc. A/59/565; for doctrine, see A. Slaughter, "Security, Solidarity, and Sovereignty: The Grand Themes of UN Reform, *The American Journal of International Law*, 2005, pp. 619-631.

in freedom and dignity, free from poverty and despair", and it was recognized that "all individuals, in particular vulnerable people, are entitled to freedom from fear and freedom from want, with an equal opportunity to enjoy all their rights and fully develop their human potential".[22] The decisive step towards defining the concept of human security was made by the General Assembly Resolution 66/290 on 10 September, 2012, with which the Member States "agreed for the first time on a common understanding on human security". Here human security is affirmed as an approach that concerns all challenges and threats to people's "survival, livelihood and dignity".[23] On the basis of this new idea, security becomes a tool that allows people to live, rather than merely survive. In this regard, some people also talk about "survival plus", an expression which, as we have mentioned, generally describes a life free from need and fear.

So far as the more specific meaning of the phrase is concerned, this can be interpreted in a number of ways. From an objective perspective, it regards already existing threats and new and emerging threats, which are transversal and widespread. The new concept of human security takes into account the fact that new threats go through and across a State's territorial borders: an event that threatens human security in one part of the world may easily produce disastrous effects in very distant areas that are not geographically contiguous to the one in which the event originates. Consequently, the measures aimed at dealing with such threats must be of a transnational nature, and above all must give the causes of such threats as much consideration as they do the impacts. From a subjective perspective, and thus from the perspective of those who have to ensure human security, in the aforementioned General Assembly Resolutions recognition continues to be given to the role of States in guaranteeing human security, while taking into account the fact that with regard to more recent issues, neither a State on its own nor a group of States working together are able to guarantee a sufficient level of security. To this end, it is necessary to strengthen the dynamics of interaction and cooperation between governments, organizations – both international and regional – civil society, and local actors.

Reference to the new concept of human security is also useful in further specifying the area of this investigation. The analysis this Volume offers is intended to ascertain the applicability of the new model of human security to navigable spaces. Until now, this model has been applied in various contexts, such as the financial, food, and environmental sectors. However, since the definition of human security is extremely wide, and also in light of the peculiarities we have highlighted as concerns navigable spaces, we intend to examine the applicability of this new model with specific reference to those spaces.[24] The analysis will cover an area of public

[22] UN General Assembly, *Resolution on the 2005 World Summit Outcome*, UN Doc. A/RES/60/1, 24 October 2005.

[23] UN General Assembly, *Resolution on Follow-up to Paragraph 143 on Human Security of the 2005 World Summit Outcome*, UN Doc. A/RES/66/290, 25 October 2012.

[24] On human security in the maritime space, see N. Severiano Teixeira, D. Marcos (eds.), *Evolving Human Security Challenges in the Atlantic Space*, Jean Monnet Network on Atlantic Studies, 2019,

international law that will benefit here from a multidisciplinary outlook, offered by scholars, legal professionals and humanitarian operators who are experts on both sociology and law (international, EU, civil, and criminal law).

This edited Volume is organized into three principal parts. The first includes this introduction and an analytical study by an economist-statistician and a computer engineer, members of the HUMARCYSPASE research group. Their study offers the scholarly community, as well as representatives of institutions and organizations in the sector, a table of risk indicators regarding human security in both maritime and cyberspace. The second and third parts of the Volume include papers, in Italian and in English, dealing with the numerous legal issues concerning human security at sea (Section I) and in cyberspace (Section II).

Specifically, Section I contains a first set of contributions that seek to reconstruct a link between migration and human security at sea. While the analytical study offered in Section I by *Francesco Schettino* demonstrates that the Mediterranean is the maritime space in which human security is most gravely threatened, the papers by *Adele Del Guercio*, *Fabio Marcelli* and *Nassim Madijadian* clarify how, within the Mediterranean space, legal questions linked to migration by sea revolve above all around the implementation of the obligation to rescue and provide a safe port of disembarkation, and have seen opposition between government authorities and non-governmental organizations (NGOs). These three papers examine various requirements of international maritime law, migration law, and human rights law, as well as studies, reports, and the rulings of numerous national courts that demonstrate and expose the urgent necessity to respect and implement these obligations. Whereas *Nassim Madjidian* highlights the practical and legal relevance of the issue in the case of the engagement of a civil rescue fleet in the Mediterranean, *Kiara Neri*, taking inspiration from the recent Maersk Etienne saga, focuses on the specific legal issues related to the rescues carried out by commercial ships.

The issues connected to the security of those who travel because they aspire to a life "free from fear" and "free from want" do not end here. After rescue and transfer to a safe place, state authorities, once again in opposition to humanitarian organizations, must tackle the question of relocating the rescued people. According to the analysis offered by *Sara Bellezza* and *Haidi Sadik*, these relocations are currently undertaken in a discriminatory manner that violates numerous fundamental freedoms and human rights of the rescued and (possibly) relocated migrants on the one hand, and of the humanitarian organizations on the other. In addition to this, while the Mediterranean is the most lethal maritime space on the planet, the analysis offered by another author in this Volume demonstrates that the security of migrants and asylum seekers is put at risk in other zones too. In particular, *Ana Nikodinovska Krstevska* moves the investigation to the eastern edges of Europe, focusing on the

---

available via Brooking Institution Press at <https://transatlanticrelations.org/wp-content/uploads/2019/10/29262-D-01_COD_EvolvingSecurity_TXT.pdf>; on human security in cyberspace, see J. Shannon and N. Thomas, "Human Security and Cyber-Security: Operationalising a Policy Framework" in R. Broadhurst, P. Crabosky (eds.), *Cyber-Crime The Challenge in Asia*, Hong Kong University Press, 2005, p. 327 ff.

violence generated by the behavior of police authorities and the relief given by NGOs in Northern Macedonia.

If in antiquity the oceans and seas were totally open spaces without borders, in the contemporary era many zones at sea form veritable maritime borders. The subject of surveillance of the external borders of the European Union (EU) is dealt with in the contribution by *Fulvio Vassallo Paleologo*, which focuses on an analysis of Regulation (EU) 2019/1896, regarding the control of the European borders and coastline.[25] His analysis takes a strong cue from the report 'Remote control: the EU-Libya collaboration in mass interceptions of migrants in the Central Mediterranean', published on 17 June, 2020 by four NGOs, which details how the new electronic systems of managing the EU's external borders, introduced by the aforementioned Regulation, have been used by EU aerial surveillance units in collaboration with Libyan coastal authorities to facilitate the interception and mass deportation of migrants, even in international waters.[26]

Innovation can be a crucial tool in ensuring greater human security at sea, and can be used by government authorities, although not only by them. In the final two contributions of this Section of the Volume, we learn how today there is a growing tendency to rely on new technologies, such as digitalization, system integration and automatization, as well as advanced ship-shore communication networks, which are aimed at improving ship performance but also, and above all, at improving the conditions of safety of the crew and passengers, who are exposed to attacks by pirates and other forms of threats, whether old or emerging. *Fenella Billing* and *Christian Frier*, in one contribution, and *Carlo Corcione*, in another, illustrate the advantages resulting from the use of such technology, but also the legal questions, practical problems, and wider issues linked to the fact that, in the period when the aforementioned UNCLOS and various other important conventions dealing with maritime safety and security were adopted, the processes of automation we see now were completely unknown, and even unimaginable.

The range of human security threats offered by the contributions collected in Section II, which is dedicated to cyberspace, is undoubtedly more varied than that presented in the previous Section. This is fully in keeping with the results that emerge in *Michele Mastroianni*'s analytical study.

In any event, Section II also includes papers that investigate the links between migrations and human security. The studies by *Olga Koshevaliska* and *Elena Maksimova*, for instance, examine the dual nature that the internet presents to migrants and refugees. Specifically, while the first author focuses on the crucial role the web plays in migrants' survival during their travels, the second author explains how this close reliance on the web makes people migrating or fleeing conflict and

[25] European Parliament and Council of the European Union, Regulation (EU) 2019/1896 of the European Parliament and of the Council on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, 13 November, 2019.

[26] Alarm Phone, Borderline-Europe, Mediterranea Saving Humans and Sea-Watch, *Remote control: The EU-Libya Collaboration in Mass Interceptions of Migrants in the Central Mediterranean*, 17 June 2020 <https://eu-libya.info/img/RemoteControl_Report_0620.pdf>.

famine even more vulnerable, and possibly even more exposed to the risk of finding themselves entrapped in other kinds of webs, particularly those of the traffickers who, as is well known, manage migrants and refugees' movements, but also their communications, profiting from their condition of extreme vulnerability. In addition to all this, both authors examine the role played by private actors involved in the protection of such people's security in cyberspace. Specifically, while *Olga Koshevaliska* dwells on the impact of innovative software-clouds created by private companies to collect and store the personal and biometric data of migrants, *Elena Maksimova* concentrates on the role played by cybertraffickers, from the recruitment to the exploitation of their victims in (real and) virtual spaces.

The problem of protecting the rights and fundamental freedoms of users is a problem that is very important to online civil society. *Maria Chiara Vitucci* examines the issue, specifically investigating the true role of hackers, actors involved in the defense of digital rights in the age of surveillance capitalism. With specific reference to the context of the COVID-19 pandemic, *Gianvito Brindisi* and *Paolo Vignola* examine the impact of the growing use on a global scale of digital platforms that, to a large degree, permit the relocation into cyberspace of (almost) any sort of work. In particular, the authors ascertain from a sociological perspective whether, and in what terms, the mass usage of such platforms and the consequent control of personal data and information may lead to a redefinition of power and law.

As in maritime space, in cyberspace too the subject of border surveillance is acquiring growing importance, and offers significant and interesting challenges to legal professionals. In regard to innovative and pioneering technologies, *Federica De Simone* ties her analysis to the problems associated with the use of new systems of artificial intelligence recently organized on a trial basis by the European Commission to prevent border crime. The subject of new technologies is enormously topical, and is being discussed in various, very different contexts. Among other issues, their use is entrusted not just to public actors, but also to private ones. By now it is common practice for search engine providers or social network companies to employ new technologies for the collection and storage of the personal and even biometric data of a large number of web users. *Federica De Simone* and *Roberta Catalano's* papers show that both European institutions and private operators seem to be leaning towards the use of facial recognition tools because of their demonstrable utility and efficiency in crime prevention *(Federica De Simone)* and the persuasiveness of advertising messages *(Roberta Catalano)*. Nonetheless, these emerging practices are not without inconveniences and problematic aspects. Above all, there is a need to find an adequate balance between the various interests in play. In approaching the subject, *Caroline Cornella* leaves behind both criminal and civil law perspectives, using international humanitarian law to examine the issues related to individuals' security when use is made of new technologies in armed conflicts.

In conclusion, the last two papers in the Section dedicated to human security in cyberspace discuss the dual nature of the internet, with its role on one hand as a promoter of knowledge and well being, and, on the other, its association with instability and criminality. Regarding its more positive aspects, *Giuliana Doria* and

Ilaria Infante recall how the arrival of the internet revolutionized the world of information, social interaction, and entertainment. Access to the web, which is now extremely easy, fast, and, in many countries, free, has shortened, if not eliminated, the distances between the users benefitting from its services, as well as between users and the contents of the web. However, in spite of the good intentions of the internet's creators, its characteristics have facilitated the spread of new illegal and criminal phenomena and fresh legal issues. Thus, looking at the less positive aspects of the web, *Giuliana Doria* orients her analysis towards so-called hate crimes, focusing in particular on "revenge porn", while *Ilaria Infante* examines digital piracy, focusing in particular on the various liability profiles that may concern internet intermediaries according to different legal regimes.

HUMAN SECURITY: RISK INDICATORS IN NAVIGABLE SPACE

Francesco Schettino - Michele Mastroianni*

1. Maritime and Cyberspace Security: Analogies and Differences

The comparison between Cyberspace and Maritime space is an interesting topic, considering that both spaces are mainly borderless and sometimes without a well-defined law. The analogy between sea and Cyberspace is sometimes used to inspire the regulations to be adopted for Cyberspace: in 2015, Adm. Rogers, the then-head of National Security Agency, declared: *I'd like to see if we can create something equivalent to the maritime world in the cyber world that enables us to keep moving information, keep moving commerce, keep moving ideas on a global basis.*[1]

There are some scholars that propose Cyberspace/Maritime space analogy. In a paper of Laprice,[2] this analogy is proposed in a Cyberwarfare perspective, and the author argued that *an effective model for looking at cyberwarfare is that of maritime "guerre de course" or commerce warfare*, and proposed to use this analogy in order to forecast possible future trends in Cyberwarfare.

In the studies of Eigloff,[3] the author investigates about the analogy between cyberspace and the sea in the age of privateering. In his studies, Eigloff compares the privateering in the sixteenth and seventeenth centuries and cybersecurity and categorizes *State actors*, *Semi-state actors* (Big Tech Companies in the role of old Merchantile Companies, patriotic/ethical hackers as privateers), and *Criminal actors* (Cybercrime as Pirates). Moreover, Eigloff also states the similarity of the regulation challenges for both spaces, and observes that *the use of non-state actors by States in cyberspace has produced unintended harmful consequences*.[4] Although this is a fascinating analogy, his approach remains state-centered, and in the following of this research, are used only the categories State and non-state actors.

---

* This paper is the result of a common research, nevertheless Section 1, 4, 5 and 6 are to be attributed to Michele Mastroianni, whereas Section 2 and 3 are to be attributed to Francesco Schettino.

[1] E. Auchard, D. Mardiste, "NSA chief urges 'safe' Internet under equivalent of Law of the Sea", Reuters, 2015, <https://www.reuters.com/article/us-cybersecurity-nsa/nsa-chief-urges-safe-internet-under-equivalent-of-law-of-the-sea-idUSKBN0OC1Z920150527> (06/21)

[2] J. Laprise, "Cyberwarfare seen through a mariner's spyglass", Proceedings of the 2005 International Symposium on Technology and Society. Weapons and Wires: Prevention and Safety in a Time of Fear, IEEE press, New York City, 2005, pp. 52-61.

[3] Egloff, F. J., "Cybersecurity and the Age of Privateering", in G. Perkovich, E. Levite (eds.) Understanding cyber conflict. Fourteen analogies, Georgetown University Press, Washington, DC, 2017, pp. 231-247.

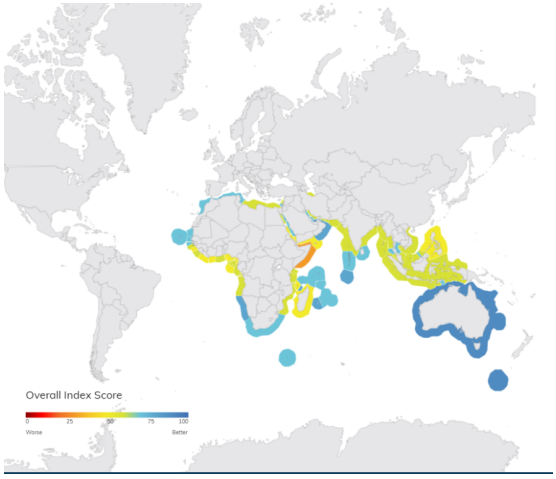
[4] Egloff, F. J. Cybersecurity and the Age of Privateering: A Historical Analogy. Cyber Studies Programme, University of Oxford, 2015.

It is also necessary to point out the differences between sea and Cyberspace navigation. Unlike what happens in Maritime human security, in Cyberspace, the user – the *passenger* of the Net - is an active and integral part of the Cybersecurity environment. The user must have the tools to defend its own security (antivirus, personal firewalls, etc.), and must adopt *safe* behavior to avoid security issues. This entails the absolute necessity for the user to be informed (and hopefully trained) on the security risks. Using others maritime metaphors, the user is both the passenger and the captain, and his *ships* are the connected devices (PC, smartphone); moreover, there are no *nautical charts* for the Net, and has to take into account that there are no safe harbors, but only a cautious and conscious behavior.

2. Human Security: Risk Indicators for the Maritime Space

Human security in Maritime Space is mainly linked to the migration and piracy phenomenon, that presently constitutes the prevalent aspect of the problem. However, some international institutions have explored these issues further, along several dimensions. Stable Seas, a program of One Earth Future,[5] for instance, produces a yearly index that captures and maps nine maritime security issues: International Cooperation; Rule of Law; Maritime Enforcement; Coastal Welfare; Blue Economy; Fisheries; Piracy and Armed Robbery at Sea; Illicit Trades; Maritime Mixed Migration. Each country is scored on each issue on a scale of 0 to 100, with 0 reflecting the worst conditions and 100 reflecting the best ones. The latest edition of the index covers 71 littoral countries in Africa, the Middle East, and the Indo-Pacific.

Figure 0 – Stable Sea Index



Source: https://www.stableseas.org/issue-areas/overview April, 8 - 2021

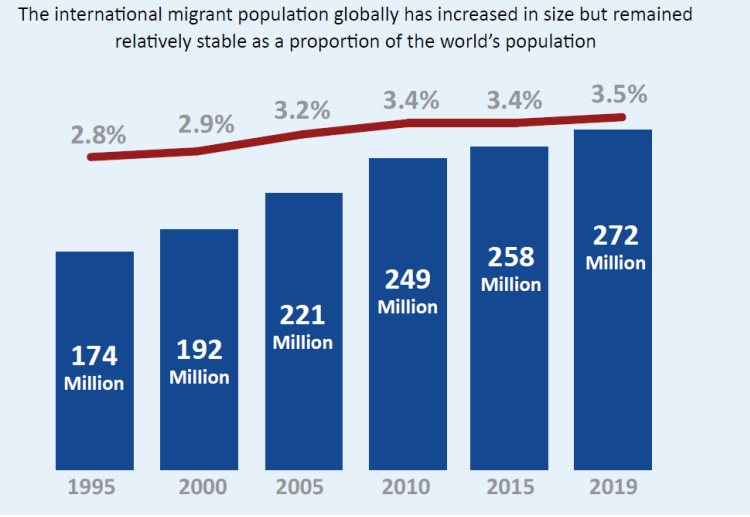
[5] *Stable Sea Index* <https://www.stableseas.org/> (04/21).

Notwithstanding the multidimensional nature of the index, Figure 0 clearly shows that maritime risk is generally higher in areas characterized by relevant migration flows (Horn of Africa, Libya, SSAs, South East of Asia; in details, Somalia, Cameroon, Nigeria and Yemen). This confirms, to some extent, that human risks in global maritime spaces can be dynamically evaluated by international migrations analysis.

Ever-increasing global migration flows have inevitably generated growing fatality risks. Actually, both the world population and the stock of migrants have been rising. The share of the world population constituted by migrants has also increased in the last 25 years - from 2.8% to 3.5% (Figure 1). The latter figures might convey the impression that the migration drama is not as severe as the "absolute" dimensions of the phenomenon would suggest, but they do testify a dynamic that is in any case significant.

The co-movement of the world population and stock of migrants suggests a sort of "endogeneity" of the migratory phenomenon, which could represent not only the spontaneous response of people to a Malthusian dynamic but also - following a Marxian approach - the consolidation of the global "reserve army of labor", particularly useful to guarantee new capital accumulation during the crisis phases. In any case, the true nature of the relationship between demographic dynamics and migratory flows remains a quasi-inexplicable puzzle.

Figure 1 – The size of global migration



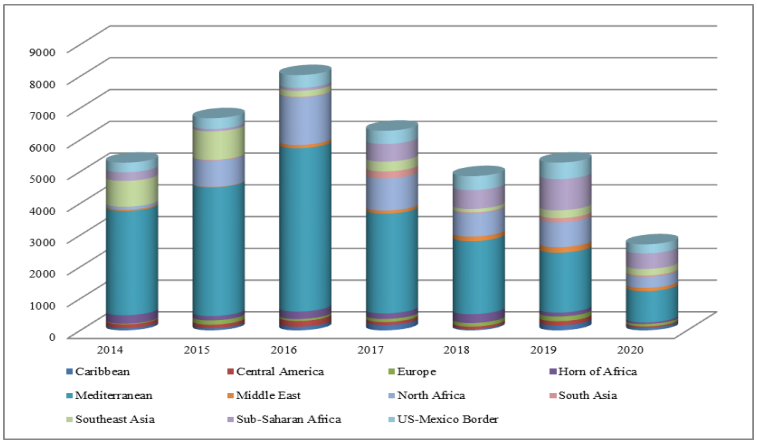
Source: World Migration Report 2020 - IOM

Comparing the world's main migratory "routes", intra-continental movements affecting Asia, Europe, and also Africa are the most relevant. Alongside this phenomenon, however, intercontinental migration flows are steadily increasing too: the most relevant are those from Asia and Africa to Europe, from Africa to Asia, and

from Central America to Northern America (see also IOM, 2020 and D'Acunto et al., 2021).[6] In other words, the role of the different continents in the process of allocation of the world population seems to respond to some extent to a precise pattern: Latin America and Africa "export" population, while North America and Europe "import" people. After a long period during which it "exported" people, Asia is rapidly changing its position and becoming the destination area of an increasing number of migrants, due principally to the impressive economic growth of PRC and India. Data concerning the direction of the migratory movement evidently indicate the important – and obvious – explanatory role of geographical proximity. In the case of Africa, most migrants move within their own continent, even as many flow towards "opulent" Europe. By the same token, most Latin American migrants go to North America due to its proximity, even if cultural and linguistic factors should in theory direct them towards the former European colonial powers.

The higher the number of people migrating, the higher is, obviously, the fatality risk. Focusing on the 2014-2020 period, Figure 2 shows a relevant increase of tragedies in the first three years. Anyway, notwithstanding a reducing trend of death and missing migrants after 2016, the absolute numbers still remain dramatically high.

Figure 2 – Death/Missing during migrations 2014-2020

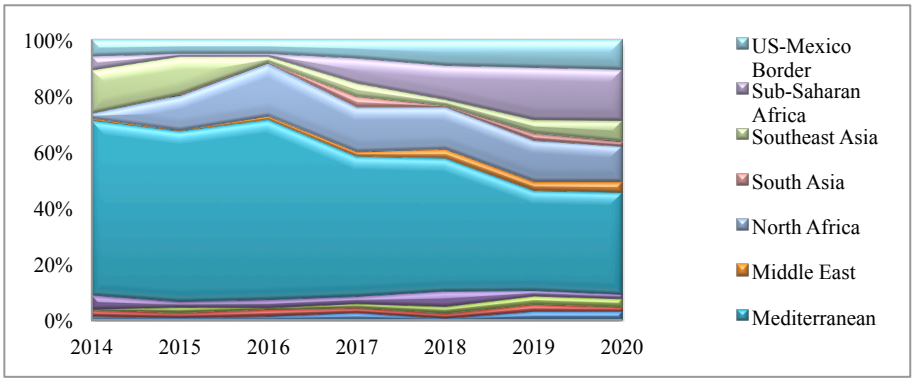


Source: Author's elaboration on IOM Missing Migrants 11-20 dataset

The Mediterranean route is clearly the most dangerous (Figure 3) in the world, accounting for over half of the global migration fatalities in 2014-2016. After 2016, as fatalities mounted both in the US-Mexico route and in Sub-Saharan Africa, the relative weight of the Mediterranean route falls below 50%.

[6] S. D'Acunto, F. Schettino and D. Suppa, *Reasons ForMigration: A Critical Approach to Economic Models*, *mimeo* 2021. IOM (2020), World Migration Report 2020 – Genève, Switzerland.

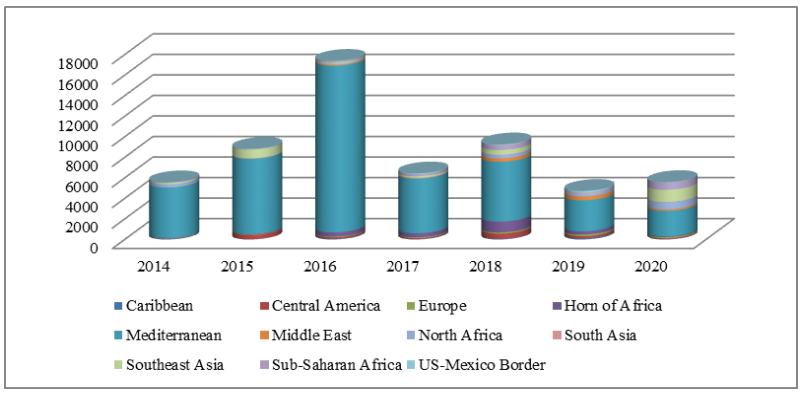
Figure 3 – Death/Missing during migrations (share of total) 2014-2020



Source: Author's elaboration on IOM Missing Migrants 11-20 dataset

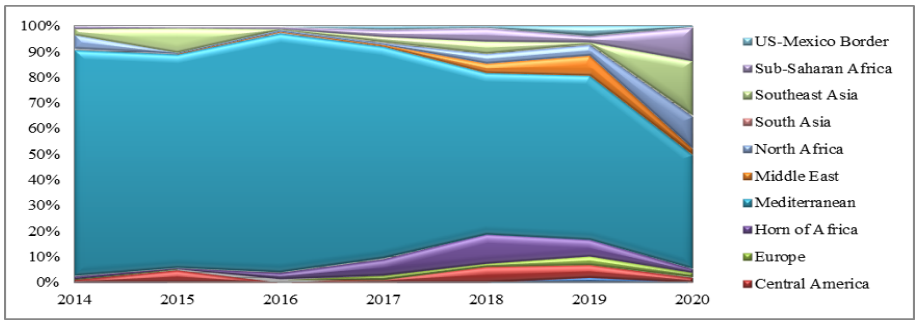
Fortunately, the number of survivors is also high. The peak has been reached in 2016 (Figure 4). In the first years of the period the quasi-totality of survivors was involved in tragedies taking place in the Mediterranean Sea. After 2017, the share of survivors in other areas increased (Figure 5). One possible explication of this trend is the changing role of NGOs. As shown in other Chapters of this volume, NGOs were crucial in salvage operations before the promulgation of the so-called "Security packs (I and II)" (SPs) by Italian government in the second half of 2018, that strongly constrained their ability to intervene.

Figure 4 - Survivors during migrations (share of total) 2014-2020



Source: Author's elaboration on Missing Migrants 11-20 dataset

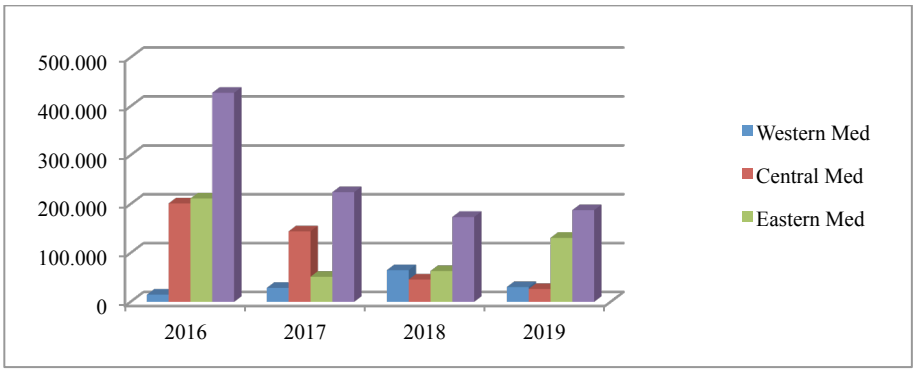
Figure 5 - Survivors during migrations (share of total) 2014-2020



Source: Author's elaboration on Missing Migrants 11-20 dataset

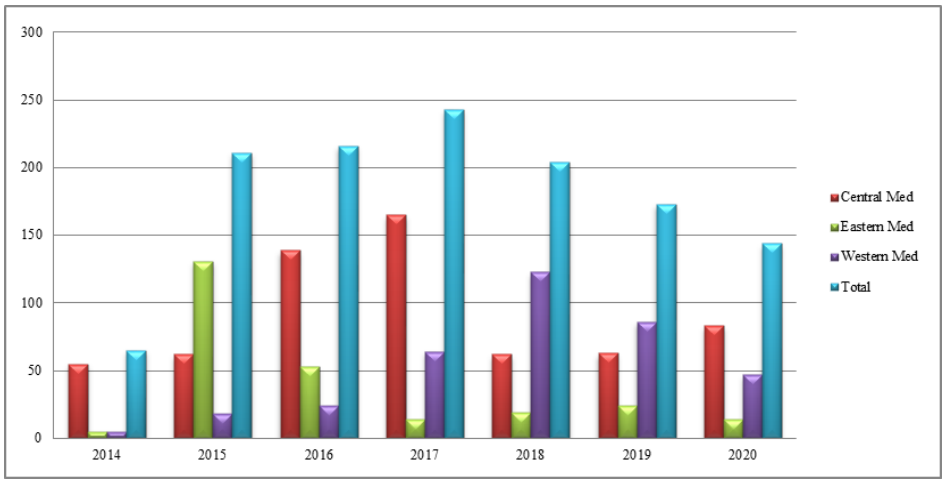
Thus, the Mediterranean Sea remains the area of the world where the risks of migration are the highest. Therefore, it deserves particular attention on our part. In 2016-2019 migration flows in the Mediterranean Sea have been declining (Figure 6). The Central route (Libya-Italy) flows decreased monotonically, and by 2019 they were the smallest. On the contrary the Eastern route (Turkey-Greece) flows fell in 2016-2017 but increased afterwards, and by 2019 became the largest (see, in particular, the dramatic situation prevailing in Lesbo Island). The Western route (Morocco-Spain) migration flows were especially large in 2018. The number of fatalities varied broadly proportionally to that of migrants (see Figure 7). Anyway, the Central and Western routes are intrinsically the most dangerous, while the Turkey-Greece one seems to be more "secure".

Figure 6 – Migrants through Mediterranean Sea by route - 2016-2019



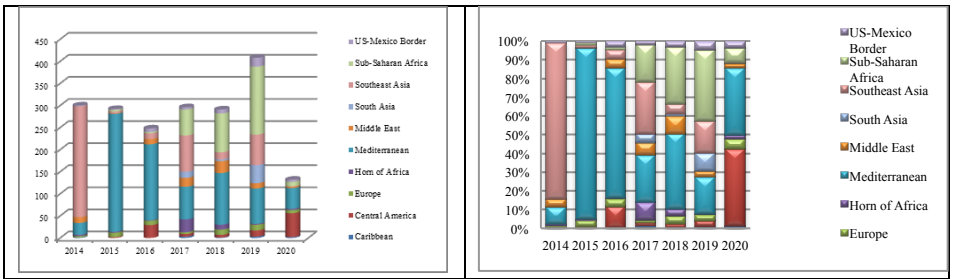
Source: Author's elaboration using IOM "Annex Med arrivals interception deaths" dataset

Figure 7 –Fatalities in the Mediterranean Sea by route - 2014-2020



Source: Author's elaboration on Missing Migrants 11-20 dataset

Figure 8 – Child Missing/Deaths



(a) Number of Child death/missing by zone | (b) Share of child death/missing by zone

Source: Author's elaboration on Missing Migrants 11-20 dataset

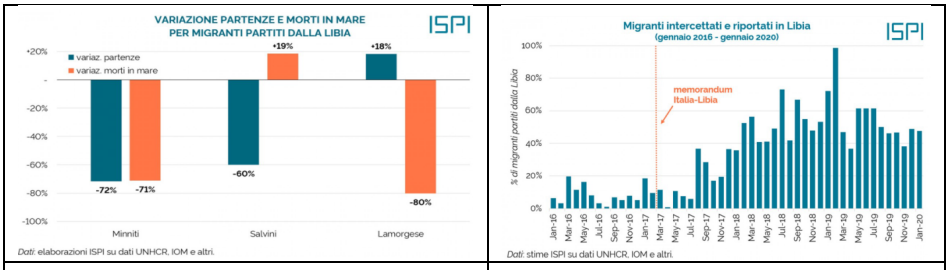
Turning to the most fragile part of the migrant population, Figure 8a shows the magnitude of child migrants' deaths. Differently from the above-discussed trends in the general migrant population, children's deaths climbed in 2019, showing that migration has become increasingly risky, especially for the younger persons.

The relevance of child deaths in the Mediterranean Sea in 2015-2016 (Figure 8b) is due principally to various major tragedies occurring close to the Italian shores. More recently, the number of casualties among children originating from SSA increased significantly, confirming the growing insecurity of the inter-African route.

All of the considered trends have been profoundly influenced by "exogenous" elements such as bi/multilateral pacts, laws and internal/external conflicts. In the case of the Western route, the Moroccan/Spanish agreement of the first months of 2019 allowed the Spanish *Salvamento Marítimo* to bring back the migrants directly

to the country of origin, with a strong impact on migration dynamics. Apropos the Central route, both the "Italy-Libya Memorandum" (February 2017) and the so-called "Security Packs (I and II)" (SPs) (promoted by the Italian government in the second half of 2018) also had a relevant effect, and they probably contributed to the observed reduction after 2016. Figure 9a reports the variation of migrants and deaths under three subsequent Italian governments. During first one, when Marco Minniti was the Ministry of the interior, the Memorandum Italy-Libya was signed, and both the number of migrants leaving the Libyan coasts and the deaths decreased dramatically (almost 70%). The effect of the SPs, during the Salvini "era", has been significantly different. The number of deaths increased by 19% - principally for the legal limitations for NGOs and other State/Not State actors introduced by these laws – while the number of migrants from Libya fell by 60%. On the contrary, Lamorgese (who is presently in office) was able to deeply attenuate the number of fatalities (-80%) notwithstanding an increase of migrants (+18%), even if she only partially modified the SPs. Finally, the Eastern route underwent a dramatic evolution due to the over one decade old Syrian war, that led to an impressive movement of refugees. Also the agreement signed between Turkey and EU at the beginning of 2016, and the uneven degree of their practical implementation had a major impact on migration flows.

Figure 9 – Focus on Italian policies on migration



(a) Deaths and Migrants by Italian government | (b) Migrants sent back to Libya

Source: Matteo Villa - Migrazioni in Italia: tutti i numeri – ISPI – 31/01/2020

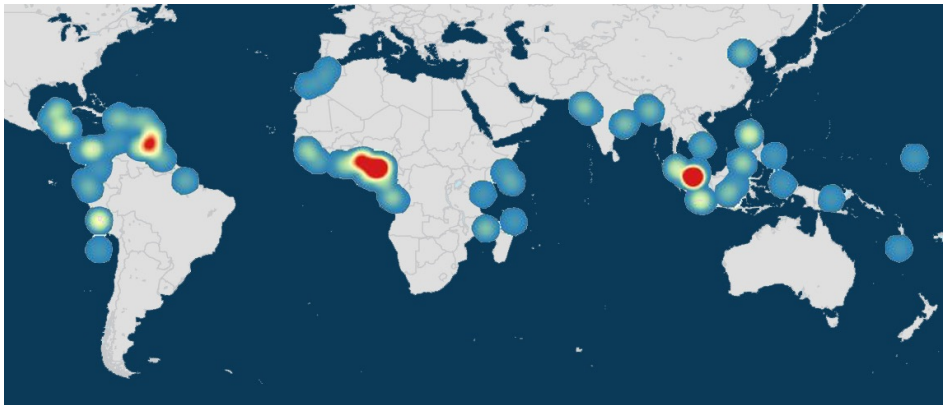
The statistical evidence presented above highlights the central role played by institutions. Migration flows and their degree of insecurity depend substantially on the way advanced capitalist countries decide to manage the phenomenon, with a view to steer public opinion. This factor is crucial to explain the recent reduction in migration flows through the Mediterranean Sea. This phenomenon, however, is only apparently positive, because it does not take into account the root cause of migration itself, i.e. the hardship suffered by millions of people that brings them to the MENA coasts. In the European countries the reduction of fatalities/arrivals is indeed often presented as a good outcome of adopted policies. Yet, as shown by Figure 9b, a decreasing number of fatalities/deaths in the Central Mediterranean route corresponds to a growing number of men and women pushed back to the Libyan

"prisons/lagers". In other words, the human tragedy funneling the migration phenomenon is far from having been solved. Actually, it has been mainly delocalized in places sufficiently far from the eyes of capitalist countries' populations, but its nature remains substantially the same.

3. Indicators for Piracy

Finally, a brief discussion on piracy and armed robbery seems to be important to better depict the Maritime security. The current phase of capitalism is in fact strictly linked to the existence of an efficient global trade. Therefore, the simple existence of more than a million seafarers on over 50,000 merchant ships transporting most of the world's cargo between ports is a necessary condition to the yearly capital accumulation. Obviously this impressive traffic attracts illicit actors that use to operate mainly when the merchant ships go through uncontrolled and high risky areas. Piracy and armed robbery incidents determine significant financial and human costs; lost and stolen cargoes, ship self-protection and other measures employed by vessels can cost more than billions of euros per year. The physical and mental consequences for victims of piracy and their family members could be important, considering that captors can be extremely violent especially to captive crews.

Figure 10 – Global Piracy and Armed Robberies – Year 2019



Source - PIRACY & ARMED ROBBERY 2020 – Stable Seas Index

The Gulf of Guinea was in 2019 the region more affected by piracy and maritime robbery (Figure 10). In the last ten years, the highest concentration of these incidents was close to the Togo and Benin coasts. Containers have typically been attacked to steal oil cargo, to ransom the vessel and crew, or to serve as a mothership to attack other vessels. East Africa, normally considered as a piracy interested zone, had only eight incidents. This is due probably to the recent collaboration of Somalia "authorities" with international partners (among others UN Office on Drugs and

Crime and EU Naval Forces ATALANTA (EUNAVFOR)) aimed at improving the legal and physical infrastructure to detain and lawfully prosecute alleged pirates who are captured. The Indo-Pacific experienced 93 incidents, while an increasing number of these phenomena happened especially in the Caribbean seas.

4. Human Security: Risk Indicators for Cyberspace

The pervasiveness of the Internet-based technologies in a variety of fields is changing our lives: industry,

agriculture, health, and even personal life are experiencing a revolution in the way data are collected, communicated, processed and stored. The vast majority of citizens, not only in the most industrialised countries, but also in the developing countries, use a PC and/or a smartphone to connect to online services for business, education, entertainment, and many other purposes; moreover, many persons use Internet of Things (IoT) devices, such as smartwatch, smart household appliance, and so on.

Sadly, along with the growth of Cyberspace, there was an exponential growth of Cybercrime; The recent Covid-19 pandemic and the consequently mandatory lockdown (and home-working activities) of business and public sector employees made the situation worse. Interpol[7] reports an increasing rate in Cybercrime activities and new emerging threats related to the pandemic. CyberEdge Group, in a survey carried out in 2020,[8] shows that more than 80% of the experts involved in the survey experienced *at least one successful attack* in the previous 12 months. Since the last 10 years, *Cybercrime has climbed to the top tier in the National Security Strategy of many EU states*[9], and Cybersecurity strategies are in the Agenda in almost all countries. The approaches used for Cybersecurity by States, International Organizations and Big Firms are mainly focused on securing the information infrastructures and online services; the Frameworks used for managing Cybersecurity are based on Feared events, Threats, Risks, Costs of Cyber Attacks with reference to *Infrastructure and Services*.

On the other side, in a recent study conducted in the Northern European Countries (Project Enablement besides Constraints: Human Security and a Cyber Multi-Disciplinary Framework in the European HighNorth - ECoHuCy), was emphasized that *current Cybersecurity Frameworks fail to acknowledge that digitalisation may*

---

[7] Interpol, Cybercrime: Covid-19 impact – August 2020, <https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf> (06/21).

[8] Cyberedge Group, Report Defense Cyberthreat 2020, <https://cyber-edge.com/wp-content/uploads /2021/02/CyberEdge-2020-CDR-Report-v1.0.pdf> (06/21).

[9] J. Armin, B. Thompson, P. Kijewski, "Cybercrime Economic Costs: No Measure No Solution", in B. Akhgar, B. Brewster (eds), *Combatting Cybercrime and Cyberterrorism. Advanced Sciences and Technologies for Security Application*s, Springer, Berlin, 2016, pp 135-155.

create new insecurities for people in their everyday life.[10] In the same study, it has been also argued that *utilising human security approaches can supplement current cybersecurity understanding and make it more inclusive to people's interests and concerns*.

In this perspective, it would be desirable to complement the usual asset-based approach with human security based approach. To do this, it is necessary to re-define Feared events, Threats, Risks ad Cost with reference to *Citizens*; this is not a completely new approach, since a similar methodology has been taken into use by General Data Protection Regulation.[11] In this Regulation Public Administrations and Firms, under certain conditions, must carry out Risk Assessment procedures in order to evaluate risks for Citizens (data subjects).[12]

In the following sections are described: an initial definition of risk indicators, the feared events that users face off, the reaction of users to attacks and the role of non-state actors in the case of Cyberspace.

5. Definition of Indicators for Cyberspace

It is not easy to assess a set of indicators for human security in Cyberspace. The vast majority of available datasets on this topic are conceived for state action and policies (such as the analysis conducted by European Union Agency for Cybersecurity[13]) or are targeted to companies and are mainly conceived to guide investments and firm strategy (such as Gartner Group[14] Reports). For this reason, and also due to the fact that HUMARCYSPASE project is mainly focused in Mediterranean area, for the study of Cyberspace indicators the Eurobarometer[15] surveys have been selected.

Eurobarometer is a series of public opinion surveys conducted regularly on behalf of the European Commission and other EU Institutions since 1973. These surveys address a wide variety of topical issues relating to the European Union throughout its member states. The aim of the surveys used in the analysis is to understand EU citizens' awareness, experiences and perceptions of cyber security is-

[10] A. Collins, "Critical Human Security and Cyberspace: Enablement Besides Constraint", in M. Salminen, G. Zojer, K. Hossain (eds), *Digitalisation and Human Security. New Security Challenges*, Palgrave Macmillan, London, 2020, pp 83-109.

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016.

[12] B. Di Martino, M. Mastroianni, M. Campaiola, G. Morelli, E. Sparaco, "Semantic Techniques for Validation of GDPR Compliance of Business Processes", in L. Barolli, F. Hussain, M. Ikeda (eds) Complex, Intelligent, and Software Intensive Systems. CISIS 2019. Advances in Intelligent Systems and Computing, vol 993. Berlin, Springer, 2020

[13] ENISA <https://www.enisa.europa.eu/>

[14] Gartner Group <https://www.gartner.com/en>

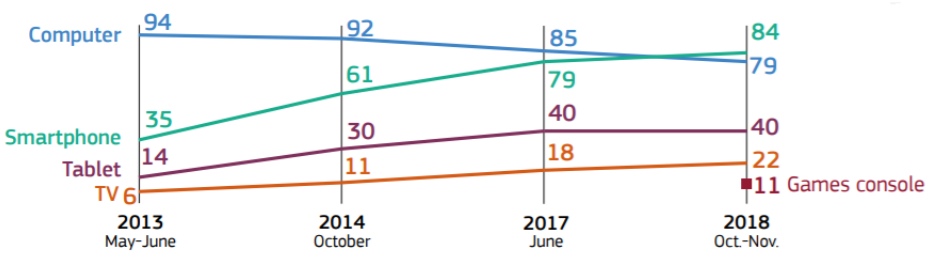
[15] Eurobarometer <https://europa.eu/eurobarometer/>

sues. Respondents were asked about many specific issues related to cyber security, for example, how much they think cybersecurity is important for EU internal security, how concerned they are about being victims of cybercrime and how they would react in a variety of situations if they were victims of these particular forms of cybercrime. Although the number of questionnaires in the survey is relatively low (*circa* 27.000), this analysis may be a good starting base to understand the users' point of view about Cybersecurity.

The Eurobarometer datasets used is *Europeans'attitudes towards Internet security*, ref. 2207/480,[16] based on data collected in October/November 2018, which was the more recent survey available on this topic in the time when the analysis was conducted.

The first thing to be noted in the 2019 survey is that the top device used for Internet access is the Smartphone, which overtook Personal Computer. In Fig. 1 is shown the devices used over the time period 2013-2018.

Figure 1 – Devices used for Internet access



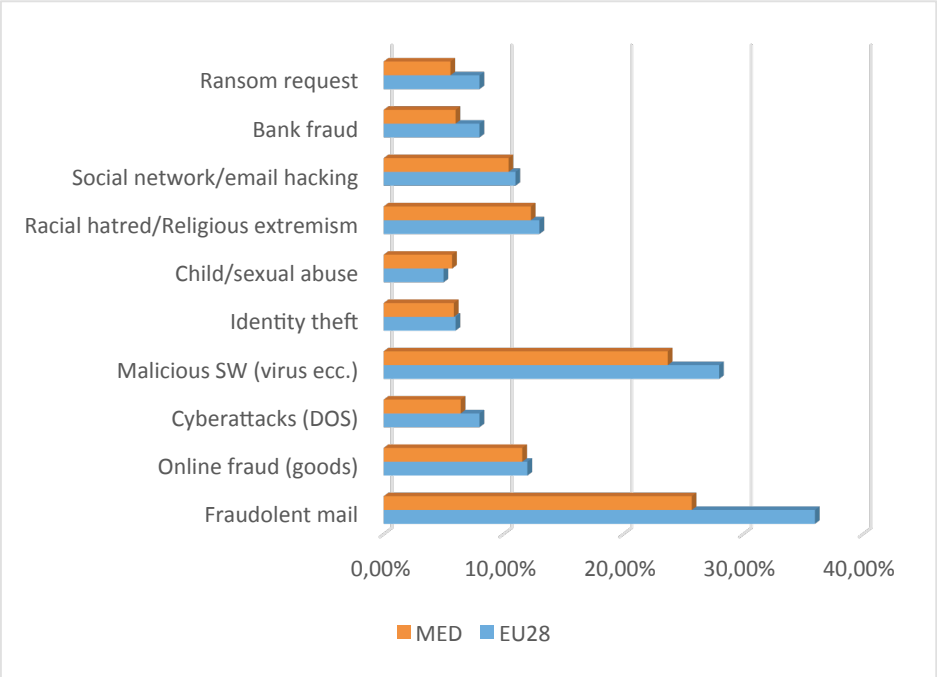
Source: Eurobarometer, dataset 2207/480.

It is of paramount importance in the analysis to assess the main threats the users have to face off in their online activity. In Fig. 2 is detailed the type of attack (or abuse) experienced by users surveyed by Eurobarometer. In the figure are shown the mean EU values and the mean values reported by users in Mediterranean countries.[17]

[16] Europeans' attitudes towards Internet security 2018, < https://europa.eu/eurobarometer/surveys/detail/2207> (06/21)

[17] It is to be noted that some users experienced more than one attack, thus the sum of percentiles may be greater than 100%.

Figure 2 – Type of attacks reported by EU and MED citizens

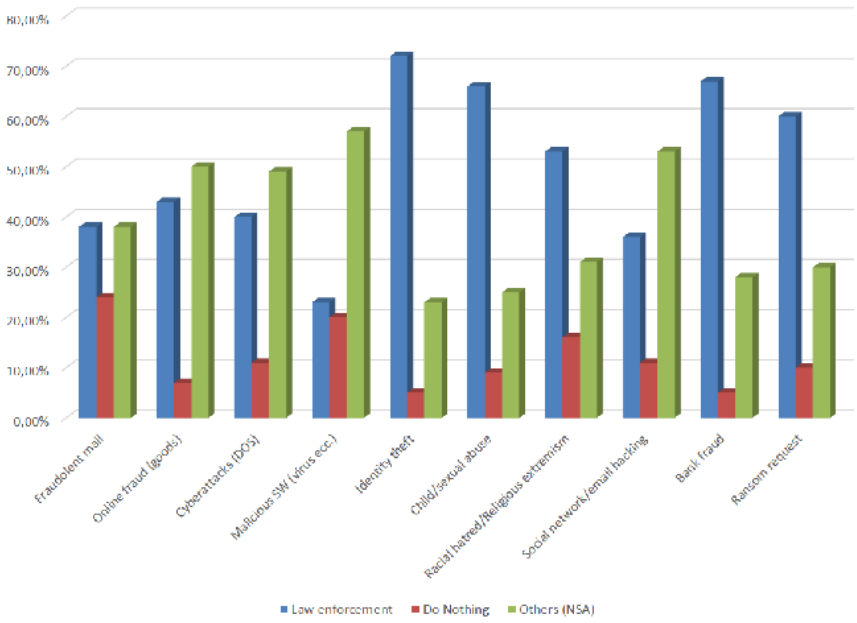


Source: Author's elaboration on Eurobarometer dataset 2207/480

The data reported in Figure 2 show that, generally speaking, the attack is less frequent in Mediterranean countries than the EU. This is probably due to the less Internet usage in that countries with respect to North European countries. However, in the case of Identity theft, there is the same mean value between EU and MED countries, and in the case of Child/sexual abuse, MED mean is higher than EU mean. This is an interesting occurrence, and worth deserve an insight in other researches.

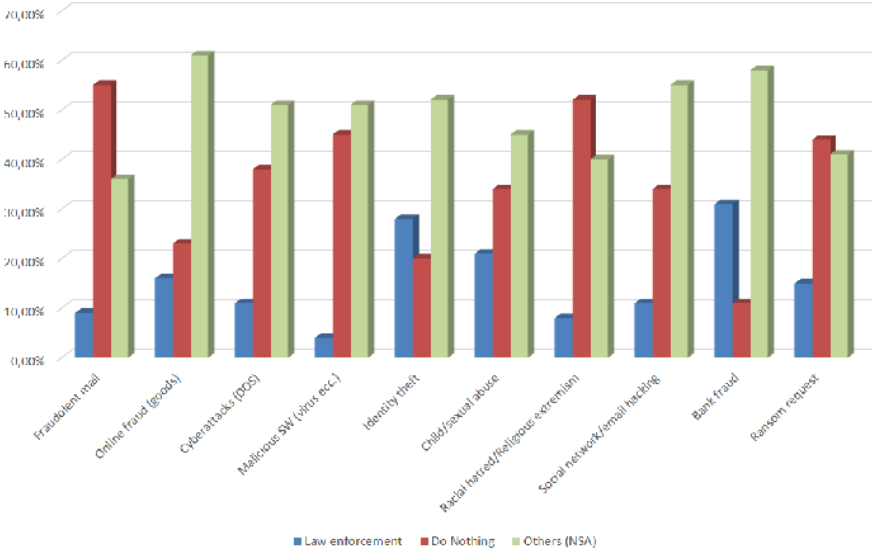
Other relevant observation may be made analyzing the users' reaction to an attack. In Eurobarometer survey, there are two groups of questions related to reactions. In the first group of questions, was asked to users which according to them should be the correct behavior (user perception); in the second group of questions, was asked to users which has been their *real* behavior once an attack has been experienced (real behavior). The results are somewhat surprising, and are shown in Fig. 3 and Fig. 4. The reactions in the figures are grouped by three categories: *Law enforcement* (the answer in the Eurobarometer questionnaire was "call Police), *Do nothing* (same question in EB questionnaire) and *Others* (sum of all other answers). The Others category groups reactions such as "call Internet provider", "call bank", "call consumer association" and so on. This category represents the non-state actors, and is important to understand which is the degree of involvement of those actors in the process of contrasting Cybercrime.

Figure 3 – Reaction to attacks (Users' perception)



Source: Author's elaboration on Eurobarometer dataset 2207/480

Figure 3 – Reaction to attacks (Real users' behavior)



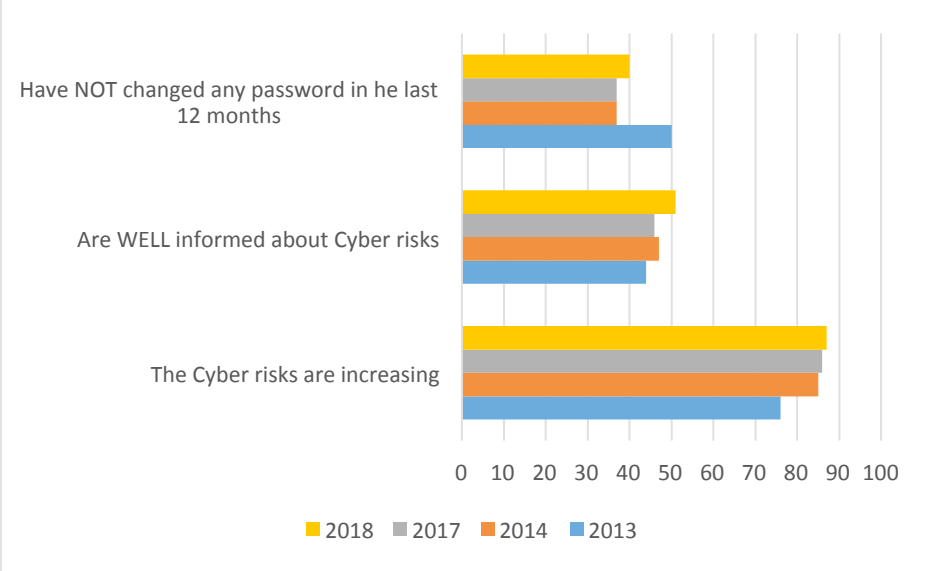
Source: Author's elaboration on Eurobarometer dataset 2207/480

The first observation that stands out from those figures is the high number of *Do nothing* reactions in fig. 4 (real behavior). If it is easy to give an explanation for this behavior in the case of Fraudulent mail, which may be perceived by users as an annoyance rather than a real threat, it is alarming that the reaction of more of 30% of users experiencing Child/sexual abuse is *Do nothing*. Deserves a deepening also the *Do nothing* reaction of many users experiencing Online fraud or Identity theft.

Another thing to note is the distance between the users' perception and their real behavior comparing Figure 3 and 4. In many cases, the users know that is necessary to communicate the problem to Law enforcement, and in particular, in the most severe cases, such as Identity theft, Bank fraud, Ransom request, but in real cases they choose to call another actor, or even to do nothing.

The Eurobarometer surveys have also underlined another worrying trend in users' behavior. The number of EU citizens are concerned about Cybercrime is growing, and also is growing the number of EU citizens that think they are well informed about Cybercrime, but they are less likely to protect themselves from Cyber risks. The following Figure 5 shows the changes from 2013 to 2018 of Cybercrime concerns and information, compared with the most basic secure behavior: the password changes in Internet services. In 2018, the 40% of users have not changed any password (email, social network, e-banking services…) in the last 12 months, while in 2017 this figure was 37%.

Figure 5 – Cyber risks and Users' behavior

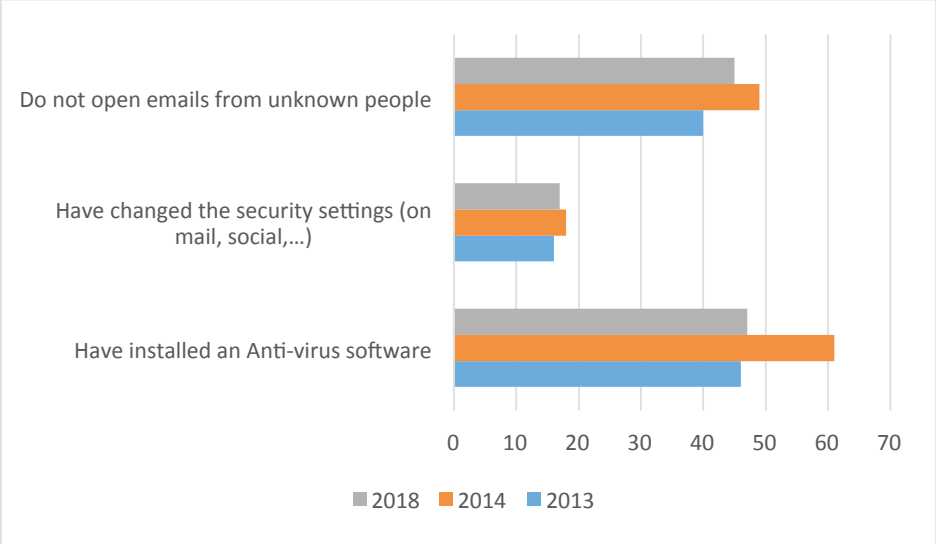


Source: Author's elaboration on Eurobarometer dataset 2207/480

The trend is confirmed by other users' behavior, as shown in Figure 6. The number of users that have installed Anti-virus software is dramatically decreasing, and so the number of users that are more likely to open mail from unknown people.

The number of users that change the security settings of software (including email, social network, …) is stable.

Figure 6 – Users' behavior



Source: Author's elaboration on Eurobarometer dataset 2207/480

The data shown in Figures 5 and 6 are EU global data, and are affected by important differences between the EU countries and between socio-demographic categories, and it is highlighted that elderly people and people with low school attendance are less likely to protect themselves from Cyber risks.

In any case, this is a worrying tread, and it is necessary to investigate the causes of the decreasing attention of people in protect themselves from the risks of Cyberspace.

6. The Role of Non-state Actors (NSA)

In the scientific literature, the difference between *State* and *non-state* actors is based not only on the legal status of those entities, but also on a significant imbalance in terms of resources and capabilities. That is not really true in the case of Cyberspace, in which the Cyber capabilities of some non-state actors (e.g. Big Tech Companies) is even, if not greater, the Cyber capability of many States. Moreover, big technological infrastructures may be held hostage by small groups of highly specialized hackers, as was the case of petroleum supply chain Cyberattack occurred in May 2021. [18]

[18] C. Hart, "Major US pipeline hit by cyber security attack", *Chartered Institute of Procurement and Supply*, 10 May 2021, <https://www.cips.org/supply-management/news/2021/may/major-us-pipeline-hit-by-cyber-security-attack-/>, (06/20).

A survey on existing public international law for norms relevant to Cybercrime was written by Schmitt and Watts in 2016. [19] In particular, this paper inspects how the principles of sovereignty, state responsibility and the jus ad bellum are particularly relevant to States engaged in struggles with non-state actors for security in Cyberspace.

A relevant study on non-state actors in Cyberspace was conducted by Sigholm.[20] In this research are examined the various non-state actors involved in Cyberspace operations, and analyzes how and when their objectives coincide with those of nation-states. In this paper may also be found a detailed list of non-state actors, their motivation, typical targets and methods. Nevertheless, it is to underline that, in the contest of that research, all non-state actors listed are seen only as "attackers" of system and services.

In the last years, some scholars have evidences that non-state actors are involved also in activities directed in defending system and services rather than attacking them. Some individual or loosely coupled groups (white-hat hackers, hacktivists, Scam baiters, …) seldom choose to act in contrast to Cybercrime in a number of ways, in most cases without any contact with law enforcement. To describe this trend, Smallridge et al. introduced the new term *Cyber vigilantes*.[21] Silva, in an interesting paper written in 2018, deepen into the same topic and claims that, although Cyber Vigilante have often caused the loss of digital evidence, obstructing law enforcement's activity in Cybercrime contrast, cyber vigilantes *have a role to play in the advancement of cybersecurity and should not be excluded from this process*. [22]

non-state actors are also involved in other crucial roles in the field of Cybersecurity contrast. In the paper of Eggenschwiler and Kulesza, is emphasized the contribution of non-state actors to the Cybersecurity, finding that non-state actors may be viewed as shapers of customary standards of responsible behavior in Cyberspace.[23]

Hence, it can be stated that scholars highlight the emerging role of non-state actors, not only as attackers, but also with an active role in defending of systems and services. It is also crucial the evaluation of the importance of non-state actors from the users' point of view.

The analysis described in the previous Section and conducted on Eurobarometer survey, and underlined in Fig. 3 and 4, shows that the role of non-state actors is of

---

[19] M. N. Schmitt, S. Watts, "Beyond state-centrism: international law and non-state actors in cyberspace", *Journal of Conflict and Security Law*, 2016, pp. 595-611.

[20] J. Sigholm, "Non-state actors in cyberspace operations", *Journal of Military Studies*, 2013, pp. 1-37.

[21] J. Smallridge, P. Wagner, J.N. Crowl, (2016). "Understanding cyber-vigilantism: A conceptual framework", *Journal of Theoretical & Philosophical Criminology*, 2016, pp. 57-70.

[22] K.K. e Silva. "Vigilantism and cooperative criminal justice: is there a place for cybersecurity vigilantes in cybercrime fighting?", *International Review of Law, Computers & Technology*, 2018, pp. 21-36.

[23] J. Eggenschwiler, J. Kulesza, "Non-State Actors as Shapers of Customary Standards of Responsible Behavior in Cyberspace", in D. Broeders, B. Van Den Berg, B. (eds.) *Governing Cyberspace: Behavior, Power and Diplomacy*, Rowman & Littlefield Publishers, London, 2020, pp. 245-262.

crucial importance. In their real behavior, the vast majority of users who opt to "*do something"*, choose to contact non-state actors, such as Telecommunication companies or banks, rather than Law Enforcement, even in the most serious cases. non-state actors therefore are in most cases the first line of defense against Cybercrime, and the collaboration between Law enforcement and non-state actors may be decisive in the contrast to Cybercrime.

SEZIONE I / SECTION I
SICUREZZA UMANA IN MARE / HUMAN SECURITY AT SEA

MIGRAZIONI VIA MARE, LUOGO DI SBARCO SICURO E PRINCIPIO DI *NON-REFOULEMENT*

Adele Del Guercio

1. Introduzione

Tra il 2015 e il 2018 le Organizzazioni non governative (ONG) impegnate nelle attività di ricerca e soccorso nel Mediterraneo centrale hanno portato in salvo circa centoventimila persone, divenendo il simbolo più evidente della solidarietà nei confronti di chi fugge da persecuzione, guerre e povertà.[1] Ciononostante – o forse proprio in ragione di ciò – diversi governi europei hanno avviato una marcata campagna di criminalizzazione, volta a screditare e a far cessare le attività di ricerca e soccorso condotte dalle organizzazioni umanitarie.[2]

In Italia la strategia di contrasto delle attività delle ONG si è articolata su due piani, governativo e giudiziario, che hanno inizialmente coinciso, per poi procedere invece autonomamente e con andamenti diversi.[3] Per quanto concerne l'operato delle autorità amministrative e del Governo, la cui trattazione esula dal presente lavoro, esso si è declinato nell'adozione di documenti privi di valore precettivo (il codice di condotta del Ministro Minniti[4]) e di normative *ad hoc* (decreto sicurezza bis[5] e decreto Lamorgese[6]); nella politica dei 'porti chiusi', reiterata strumentalmente – solo con riguardo alle navi battenti bandiera straniera che hanno compiuto salvataggi in mare – anche in occasione dell'emergenza pandemica;[7] più di recente, nell'avvio di ispezioni amministrative e nel blocco delle navi delle ONG nei porti con svariate motivazioni, tra cui il mancato rispetto dei requisiti per la navigazione, il carico eccessivo di persone o finanche reati relativi all'ambiente.[8] Per quanto

[1] AI, *Punishing Compassion. Solidarity on Trial in Fortress Europe*, 2020, p. 54.

[2] FRA, *June 2021 Update – Search and Rescue (SAR) Operations in the Mediterranean and Fundamental Rights*, 2021.

[3] L. Masera, "Il contrasto amministrativo alle ONG che operano soccorsi in mare, dal codice di condotta di Minniti, al decreto Salvini bis e alla riforma Lamorgese: le forme mutevoli di una politica costante", in *Questione giustizia*, 15.06.2021.

[4] Codice di condotta per le ONG impegnate nelle operazioni di salva-taggio dei migranti in mare, 2017.

[5] D.l. 14 giugno 2019, n. 53, convertito con modificazioni dalla l. 8 agosto 2019, n. 77. Sulle criticità del decreto sicurezza bis si rinvia a G. Cataldi, "Il "decreto sicurezza bis" alla prova degli impegni internazionali dello Stato in materia di diritto del mare. Alcune osservazioni", *Diritti umani. Cronache e battaglie*, fasc. 3, 2019, pp. 439-454.

[6] D.l. 21 ottobre 2020, n. 130, convertito con modificazioni dalla l. 18 dicembre 2020, n. 173.

[7] Decreto interministeriale n. 150 del 7 aprile 2020, su cui si rinvia alle considerazioni critiche di A. Algostino, "Lo stato di emergenza sanitaria e la chiusura dei porti: sommersi e salvati", *Questione giustizia*, 21 aprile 2020.

[8] F. De Vittor, "Il Port State Control sulle navi delle ONG che prestano soccorso in mare: tutela

concerne più nello specifico gli interventi normativi, sia sufficiente rammentare – a dimostrazione delle finalità che ne hanno animato l'adozione – che il decreto sicurezza bis trovava immediata attuazione nei confronti di un'imbarcazione della ONG *Sea Watch* con a bordo 43 persone soccorse in mare internazionale, alla quale veniva negato l'ingresso nelle acque territoriali italiane. Trattasi del caso da cui ha avuto origine una significativa pronuncia della Corte di Cassazione,[9] sulla quale torneremo a breve.

Sull'apparato deterrente e repressivo approntato dal decreto sicurezza bis è successivamente intervenuto il decreto Lamorgese, che tuttavia ha confermato la possibilità di limitare o vietare il transito e la sosta nel mare territoriale (viene espunto il riferimento all'ingresso), modificando la sanzione pecuniaria (ora da 10.000 a 50.000 euro) e prevedendo la reclusione fino a due anni del Comandante della nave che non rispetti tale divieto. Nella nuova disciplina viene precisato che l'ordine di interdizione non può essere emesso nelle ipotesi di operazioni di soccorso immediatamente comunicate al centro di coordinamento per il soccorso marittimo e allo Stato di bandiera ed effettuate nel rispetto delle indicazioni della competente autorità per la ricerca e il soccorso in mare, e che le autorità italiane, nel fornire indicazioni alle imbarcazioni impegnate nei soccorsi, dovranno attenersi agli "obblighi derivanti dalle convenzioni internazionali in materia di diritto del mare", della CEDU e "delle norme nazionali, internazionali ed europee in materia di diritto di asilo". [10] Le modifiche apportate non sono nondimeno ritenute sufficienti a determinare il superamento di un apparato fortemente criminalizzante nei confronti delle organizzazioni impegnate a dare attuazione agli obblighi internazionali sul soccorso in mare,[11] apparendo piuttosto ambigue e volte a esplicare degli effetti quasi esclusivamente sul piano comunicativo e mediatico.[12]

Si ritiene opportuno a questo punto far presente che persino la Commissione eu-

---

della sicurezza della navigazione o ostacolo alle attività di soccorso?", *Diritti umani e diritto internazionale*, 2021, pp. 103-128; L. Masera, "Il contrasto amministrativo", cit. *supra* nota3. Sul punto si vedano anche le osservazioni del Tribunale di Ragusa, sez. civ., verbale d'udienza del 16 giugno 2021, in part. p. 10.

[9] Corte di Cassazione, sezione terza penale, sentenza del 6 gennaio 2020, n. 6626. Sulla sentenza cfr. C. Pitea, S. Zirulia, "L'obbligo di sbarcare i naufraghi in un luogo sicuro: prove di dialogo tra diritto penale e diritto internazionale a margine del caso *Sea Watch*", *Diritti umani e diritto internazionale*, 2020, pp. 659-687; sia consentito rinviare anche a G. Bevilacqua, A. Del Guercio, "La vicenda *Rackete*: profili di compatibilità con il diritto internazionale del mare e dei diritti umani", *Diritti dell'uomo. Cronache e battaglie*, fasc. 1, 2020, pp. 29-64, e bibliografia ivi indicata.

[10] Sulle modifiche introdotte dalle l. 73/2020 si rinvia, tra gli altri, a L. Masera, "Il contrasto amministrativo", cit.; S. Zirulia, "Dai porti chiusi ai porti socchiusi: nuove sanzioni per le navi soccorritrici nel Decreto Lamorgese", *ADiM Blog*, Analisi & Opinioni, marzo 2021, <http://www.adimblog.com/2021/03/31/dai-porti-chiusi-ai-porti-socchiusi-nuove-sanzioni-per-le-navi-soccorritrici-nel-decreto-lamorgese/>.

[11] In argomento si rinvia a P. De Sena, M. Starita, "Navigare fra istanze "stato-centriche" e "cosmopolitiche": il caso "Sea-Watch" in una prospettiva conflittuale", *SIDIBlog*, 14 luglio 2019, < http://www.sidiblog.org/2019/07/14/navigare-fra-istanze-stato-centriche-e-cosmopolitiche-il-caso-sea-watch-in-una-prospettiva-conflittuale/>.

[12] L. Masera, "Il contrasto amministrativo", cit., p. 12 ss.

ropea, nei documenti che accompagnano il nuovo Patto su immigrazione e asilo,[13] ha invitato gli Stati membri a non criminalizzare l'assistenza umanitaria e a ottemperare agli obblighi che derivano dal diritto internazionale del mare.[14] In vero, è proprio una Direttiva comunitaria che consente agli stessi di adottare sanzioni nei confronti di chiunque intenzionalmente aiuti un cittadino di paese terzo ad entrare o a transitare senza autorizzazione nel proprio territorio.[15] La Commissione precisa che l'atto normativo in questione consente di non applicare le sanzioni quando la condotta del privato abbia lo scopo di prestare assistenza umanitaria e invita espressamente gli Stati membri a distinguere tra le attività condotte per prestare assistenza umanitaria e quelle volte a favorire l'ingresso o il transito illegali (art. 1, par. 2).[16] Ci sembra tuttavia che, tenuto conto del quadro sanzionatorio e della retorica criminalizzante che si sono consolidati in molti ordinamenti europei, un mero invito non accompagnato da una proposta di modifica della Direttiva sul favoreggiamento, per di più formulato in termini così blandi, non possa sortire sostanziali mutamenti nella situazione attuale.

Esula dal campo di indagine l'approfondimento dei profili sopra accennati, per i quali si rinvia alla ricca letteratura scientifica pubblicata. Con il presente lavoro ci si propone invece di avviare una riflessione sull'altro piano di intervento, quello dell'azione giudiziaria.[17] Ci si soffermerà dunque sulla giurisprudenza resa dalle corti italiane di legittimità e di merito[18] con riguardo all'obbligo di soccorso e alla nozione di *place of safety,* anche al fine di verificarne la compatibilità con gli obblighi internazionali sui diritti umani, in special modo con il principio di *non-refoulement*.

2. La giurisprudenza sull'obbligo di soccorso e il luogo di sbarco

2.1. La sentenza della Corte di Cassazione sul caso Sea Watch 3

Si ritiene opportuno far partire la ricostruzione della giurisprudenza volta ad evidenziare la nozione di luogo di sbarco sicuro dalla sentenza resa il 16 gennaio

[13] Comunicazione della Commissione, *Un nuovo patto sulla migrazione e l'asilo*, COM (2020) 609 final del 23 settembre 2020.

[14] Commissione europea, *Orientamenti per l'attuazione delle norme dell'UE relative alla definizione e prevenzione del favoreggiamento dell'ingresso, del transito e del soggiorno illegali*, 2020/C 323/01; *Raccomandazione (UE) 2020/1365 del 23 settembre 2020 sulla cooperazione tra gli Stati membri riguardo alle operazioni condotte da navi possedute o gestite da soggetti privati a fini di attività di ricerca e soccorso*.

[15] Direttiva 2002/90/CE del Consiglio del 28 novembre 2002 volta a definire il favoreggiamento dell'ingresso, del transito e del soggiorno illegali, GU L 328, 05.12.2002, art. 1, par. 1.

[16] *Orientamenti della Commissione*, cit. *supra* nota 14, punto 5.

[17] Si vuole precisare che ad oggi la gran parte dei procedimenti si è concluso con un nulla di fatto. In argomento si rinvia a G. Cavalli, "La macchina del fango contro le ONG", *Left*, 28 maggio 2021, pp. 12-13.

[18] Faremo riferimento soprattutto alle pronunce e ai provvedimenti dei quali il testo è accessibile.

2020 dalla Corte di Cassazione sul caso della nave umanitaria *Sea Watch 3*, originato dalla decisione della Comandante Carola Rackete di far ingresso nelle acque territoriali italiane e di attraccare nel porto di Lampedusa, consentendo lo sbarco dei migranti tratti in salvo in acque internazionali ben diciassette giorni prima, malgrado l'ordine di interdizione emesso dal Ministero dell'Interno ai sensi dell'art. 1 del cd. decreto sicurezza bis, adottato appena il giorno prima. Tra l'altro è la prima volta che la Suprema Corte offre la propria interpretazione dell'obbligo di soccorso in mare.

Appena scesa dalla motonave, Carola Rackete veniva posta in stato di arresto con l'accusa di resistenza a pubblico ufficiale e di resistenza e violenza contro nave da guerra, per non aver fermato la rotta verso Lampedusa ed aver urtato la nave della Guardia di finanza durante la manovra di attracco in porto. Tuttavia il GIP di Agrigento non ne aveva convalidato l'arresto per insussistanza dei reati ascrittile,[19] in quanto la stessa aveva agito conformemente all'art. 51 c.p. La Suprema Corte ha poi respinto il ricorso con cui il Pubblico Ministero di Agrigento chiedeva l'annullamento dell'ordinanza del GIP di Agrigento. Quest'ultimo, il 19 maggio 2021, ha accolto la richiesta di archiviazione delle accuse formulate nei riguardi della Comandante, allineandosi alla valutazione di principio svolta dalla Cassazione.[20]

Non è questa la sede per una illustrazione puntuale dei fatti su cui si è pronunciata la Suprema Corte e dell'iter giuridico-argomentativo seguito. Ci si limita a far presente che, alla luce della ricostruzione della disciplina rilevante in materia di ricerca e soccorso operata dal GIP di Trapani, la suddetta Corte ha rigettato la lettura restrittiva avanzata dal PM di Agrigento, secondo cui sarebbe sufficiente, per ottemperare agli obblighi di diritto del mare e sui diritti umani cui l'Italia è vincolata, prendere a bordo i naufraghi in pericolo in mare e metterli in sicurezza sulla nave. Sostiene invece la Suprema Corte, e tale orientamento è certamente conforme al regime internazionale del mare, che l'obbligo di soccorso non esaurisce i suoi effetti con il recupero dei naufraghi a bordo dell'imbarcazione, "ma comporta l'*obbligo accessorio* e *conseguente* di sbarcarli in un luogo sicuro (cd. "place of safety") (par. 9, corsivo aggiunto). Al fine della individuazione del porto di sbarco la Cassazione richiama le fonti internazionali rilevanti in materia, tra cui la Convenzione SAR[21] e le Linee-guida dell'IMO sul trattamento delle persone soccorse in mare.[22] Appare particolarmente degno di nota che la Suprema Corte abbia voluto precisare che la

[19] Tribunale di Agrigento, Uff. Gip, ordinanza del 2 luglio 2019.

[20] Tribunale di Agrigento, Uff. Gip., Decreto di archiviazione, 14 aprile 2021, che ha accolto la richiesta di archiviazione della Procura della Repubblica presso il Tribunale ordinario di Agrigento, del 19 gennaio 2021. Per un primo commento si rinvia a F. Vassallo Paleologo, "Si archivia anche il caso *Rackete* ma i soccorsi umanitari rimangono nel mirino", *ADIF*, 3 giugno 2021, <https://www.a-dif.org/2021/06/03/si-archivia-anche-il-caso-rackete-ma-i-soccorsi-umanitari-rimangono-nel-mirino/>.

[21] Convenzione internazionale sulla ricerca e il soccorso (SAR), adottata il 27 aprile 1979, recepita dall'Italia con il D.P.R. n. 662/1994.

[22] Resolution MSC.167 (78) del 20.05.2004, *Guidelines on the treatment of persons rescued at sea*.

nave in mare non può costituire un luogo sicuro, se non temporaneamente, non solo perché è esposta ad eventi meteorologici avversi, ma soprattutto in quanto "non consente il rispetto dei diritti fondamentali delle persone soccorse", tra cui si colloca il "diritto a presentare domanda di protezione internazionale …, operazione che non può certo essere effettuata a bordo di una nave" (par. 9). In tal modo viene offerta una lettura estensiva dell'obbligo di soccorso, che non comporta esclusivamente il salvataggio e la presa a bordo delle persone in difficoltà in mare, e nemmeno può dirsi esaurito con lo sbarco sulla terraferma, benché si tratti di un elemento *accessorio* e *conseguente* dello stesso obbligo di soccorso, ma ha quale corollario la possibilità di *chiedere asilo*. Trattasi di una interpretazione costituzionalmente orientata, basata su una lettura sistematica e organica delle fonti giuridiche vincolanti per l'Italia, in particolare della Costituzione, la quale, all'art. 10, co. 3, sancisce per l'appunto il diritto di asilo; e delle norme internazionali, consuetudinarie e pattizie, che, ai sensi dello stesso art. 10, co. 1, e dell'art. 117 Cost., acquisiscono rango sovraordinato rispetto alla legislazione interna. Tra queste va collocato proprio l'obbligo internazionale di soccorso,[23] che, alla luce di quanto sostenuto dalla Suprema Corte, deve trovare completa attuazione, dalla presa a bordo dei naufraghi, allo sbarco in un *place of safety*, al riconoscimento del diritto di chiedere protezione internazionale. Anche se non richiamato espressamente, l'interpretazione della Cassazione integra il principio di *non-refoulement*, che costituisce la *conditio sine qua non* perché le persone possano fare ingresso nel territorio statale e chiedere protezione internazionale,[24] e si pone in linea con quella giurisprudenza di merito che, già da diversi anni, ha fornito una lettura *human rights oriented* della nozione di *place of safety*.

2.2. La giurisprudenza di merito: il caso Cap Anamur

Sebbene si tratti di una pronuncia non collegata ad eventi recenti, in particolare alla criminalizzazione della solidarietà consolidatasi a partire dal 2017 in Europa, vogliamo egualmente richiamare il caso *Cap Anamur*,[25] anche perché presenta degli elementi di indubbia analogia con quello della *Sea Watch 3*, sia nelle circostanze fattuali che nelle conclusioni cui giungono i due tribunali. Nel caso di specie Comandante, primo ufficiale della nave e Presidente dell'associazione umanitaria tedesca erano stati accusati di favoreggiamento dell'immigrazione clandestina ai sensi dell'art. 12 T.U. immigrazione, per aver soccorso in acque internazionali e sbarcato in territorio italiano, nell'estate 2004, trentasette persone che si trovavano a bordo di un gommone in difficoltà.

---

[23] V. M. Starita, "Il dovere di soccorso in mare e il diritto di obbedire al diritto (internazionale) del comandante della nave privata", *Diritti umani e diritto internazionale*, 2019, p. 40.

[24] Si veda anche Tribunale di Ragusa, GIP, Decreto di rigetto di richiesta di sequestro preventivo, 16 marzo 2018. Posizione confermata dal Tribunale del riesame, Trib. Ragusa, 11 maggio 2018. L. Masera, "L'incriminazione dei soccorsi in mare: dobbiamo rassegnarci al disumano?", *Questione giustizia*, <https://www.questionegiustizia.it/rivista/articolo/l-incriminazione-deisoccorsi-inmare-dobbiamo-rassegnarci-aldisumano-_549.php>.

[25] Tribunale di Agrigento, Prima sezione penale, sentenza del 7 ottobre 2009.

L'operazione di soccorso aveva avuto luogo il 20 giugno 2004 e la *Cap Anamur* si era poi diretta verso Lampedusa, ritenuta "porto più sicuro secondo la normativa internazionale, ovvero un luogo in cui fossero garantiti il rispetto dei diritti dell'uomo, l'assistenza medica e le condizioni legali per il trattamento dei migranti" (p. 12). Successivamente all'attracco a Porto Empedocle, il 12 luglio 2004, i tre imputati venivano arrestati e il natante sottoposto a sequestro. Il Tribunale di Agrigento, con sentenza del 7 ottobre 2009, n. 954, ha ritenuto che il fatto imputabile a Comandante, primo ufficiale della nave e Presidente dell'associazione umanitaria tedesca, pur potendo integrare la fattispecie criminosa contestata dall'accusa, trovava, tuttavia, "giustificazione nella scriminante di cui all'art. 51 c.p. nella specie di adempimento di un dovere imposto da una norma di diritto internazionale", scriminante che si rinveniva in un dato oggettivo, ovvero l'operazione di soccorso nei confronti di persone in difficoltà, le quali, affermavano i giudici, "ancor prima di essere "migranti" o "richiedenti asilo", sono in primo luogo "naufraghi"" (p. 26).

Richiamandosi ai trattati internazionali sul diritto del mare, i giudici sostenevano che il Comandante della *Cap Anamur* aveva l'obbligo giuridico di trarre in salvo i naufraghi in pericolo in mare e di condurli in una località sicura, che solo provvisoriamente può essere una nave. Ancora, veniva evidenziato che "il fondamento della obbligatorietà giuridica della operazione di salvataggio complessivamente intesa" riposava "non soltanto sulla esigenza di liberare la nave dal "peso" della gestione dei naufraghi, ma, anche e soprattutto, sulla necessità di garantire a questi ultimi *il diritto universalmente riconosciuto di essere condotti sulla terraferma*" (corsivo aggiunto). Dunque gli imputati avevano compiuto un'operazione di soccorso doverosa ai sensi del diritto internazionale e di quello interno. Da evidenziare che già allora la Libia, pur costituendo il porto di sbarco più vicino al punto di salvataggio, non era considerato sicuro in quanto non vi erano garantiti i diritti fondamentali della persona umana. Degno di nota – anche rispetto alle dinamiche attuali – è altresì il passaggio in cui viene rammentato che la questione relativa alla individuazione dello Stato competente ad esaminare le domande di asilo opera su un piano nettamente separato rispetto a quella del soccorso e dell'individuazione del luogo di sbarco, che non può essere determinato attraverso i criteri stabiliti dal Regolamento (CE) n. 343/2003 (cd. Dublino II).

2.3. La giurisprudenza di merito più recente

Venendo alla giurisprudenza più recente, che si riferisce precipuamente alle operazioni di salvataggio svolte negli ultimi anni dalle ONG nel Mediterraneo centrale, sono numerosi i casi che vengono in rilievo con riguardo all'oggetto del lavoro. Va innanzitutto segnalato il decreto di rigetto del GIP di Ragusa[26] della richiesta di sequestro preventivo della nave *Open Arms* da parte del P.M., in relazione al ri-

[26] Tribunale di Ragusa, Uff. GIP, Decreto di rigetto di richiesta di sequestro preventivo, 16 aprile 2018; Procura della Repubblica presso il Tribunale di Palermo, Richiesta di archiviazione, Proc. n. 9039/17 R.G.N.R. mod. 44.

fiuto della ONG di consegnare alla guardia costiera libica i naufraghi cui aveva prestato soccorso in zona SAR libica. In questo caso la causa di giustificazione, che porta ad escludere il *fumus commissi delicti*, è stata individuata nello stato di necessità ex art. 54 c.p., che, secondo il GIP, non riguarda solamente il pericolo nell'immediato per la persona soccorsa, ma anche quello che verrebbe a determinarsi in seguito allo sbarco in un *luogo non sicuro*, e tale non può considerarsi la Libia, tenuto conto delle violenze e degli abusi cui sono sottoposti i migranti.

Vale la pena evidenziare che il Tribunale di Ragusa, nel confermare il provvedimento del G.I.P., ha sostenuto che la Libia non può considerarsi sicura, alla luce del quadro politico interno incerto e conflittuale, nemmeno dopo la stipula del Memorandum di Intesa del 2 febbraio 2017,[27] che dunque non può essere richiamato a garanzia del rispetto dei diritti fondamentali dei migranti.[28] Su tale punto ci preme richiamare una consolidata giurisprudenza della Corte di Strasburgo, secondo la quale non è sufficiente aver concluso trattati internazionali che prevedono il rispetto di diritti della persona per escludere la responsabilità delle Parti contraenti nei casi di allontanamento dello straniero. A dover essere verificata è sempre la situazione *de facto*,[29] poiché la CEDU vuole offrire una tutela che sia pratica ed effettiva, non teorica e illusoria.

Proseguendo nella ricostruzione del mosaico in divenire della giurisprudenza italiana in materia di soccorso di migranti in mare, viene in rilievo la richiesta di archiviazione formulata dalla Procura della Repubblica di Palermo in relazione ad un procedimento penale in cui si ipotizzava, a carico di ignoti, la commissione dei reati di associazione per delinquere (art. 416, comma 6, c.p.) e favoreggiamento dell'immigrazione irregolare sul territorio nazionale (art. 12, d.lgs n. 286/1998).[30] Nel provvedimento, dopo aver richiamato gli obblighi internazionali di diritto marittimo, sono indicati i documenti sui diritti umani che devono regolare le operazioni di soccorso e di sbarco, alla luce dei quali gli operatori della *Sea Watch* hanno deciso correttamente di condurre i migranti soccorsi in territorio italiano. Tra gli altri, viene richiamato il principio del non respingimento. Viene dunque evidenziato che "avendo l'imbarcazione umanitaria soccorso dei migranti che si trovavano in stato di *pericolo*, la condotta trova giustificazione" nella disciplina di cui all'art. 51 c.p. per "aver adempiuto ad un obbligo imposto da una *norma giuridica internazionale*"".[31] Inoltre, le operazioni di salvataggio svolte dalla *Sea Watch* "costituiscono certamente attività di soccorso e assistenza umanitaria nei confronti dei migranti in difficoltà" e pertanto non costituiscono reato, come disposto dall'art. 12 co. 2 del d.lgs. 286/98.

In quanto alla scelta del luogo di sbarco, questo va determinato, oltre che alla

[27] Memorandum d'intesa tra lo Stato della Libia e la Repubblica Italiana, 2 febbraio 2017.

[28] Sulla cooperazione tra Italia e Libia si rinvia a A. Liguori, *Migration Law and the Externalization of Border Controls. European State Responsibility*, Routledge, London and New York, 2019.

[29] *Hirsi e altri c. Italia*, ricorso n. 27765/09, Grande Camera, sentenza del 23 febbraio 2012.

[30] Procura della Repubblica presso il Tribunale di Palermo, richiesta di archiviazione, 28 maggio 2018, che richiama il provvedimento, sopra analizzato, del G.I.P. di Ragusa sul caso *Open Arms*.

[31] Ivi, p. 5.

luce del diritto del mare, altresì nel rispetto dei diritti fondamentali delle persone soccorse. Di conseguenza, "non deve stupire che la *Sea Watch* abbia preferito effettuare lo sbarco verso le coste italiane: ciò anzi rappresenta conseguenza logica di quanto appena esposto e una corretta gestione delle operazioni di salvataggio" (p. 6). La richiesta di archiviazione accolta dal gip evidenzia come "l'assoluta mancanza di cooperazione dello Stato di Malta nella gestione degli eventi Sar" e le condizioni di instabilità politica e amministrativa riscontrabili in territorio libico non consentano di ritenere tali territori come valide alternative di luoghi sicuri.

Ancora, il GIP di Trapani, nel caso *Von Thalassa,*[32] sulla base di un'articolata ricostruzione degli obblighi internazionali di diritto del mare e di tutela dei diritti umani, ha precisato che "Rientra nell'obbligo di ricerca e soccorso in mare l'individuazione di un porto sicuro dove sbarcare le persone in pericolo di vita" (p. 26). Se il *place of safety* (POS), secondo le convenzioni di Amburgo, SOLAS[33] e SAR, gli emendamenti del 2005, le Linee guida sul trattamento delle persone soccorse in mare dell'IMO del 2004, è un luogo dove la vita e la sicurezza dei naufraghi non è più in pericolo e le necessità primarie possono essere soddisfatte,

> laddove le persone soccorse in mare, oltre che 'naufraghi', si qualifichino – in termini di status – anche come 'migranti/rifugiati/richiedenti asilo', soggetti quindi alle garanzie ed alle procedure di protezione internazionale, l'accezione del termine 'sicuro' (riferita al luogo di sbarco) si connota anche di altri requisiti, legati alla *necessità di non violare i diritti fondamentali delle persone*, sanciti dalla norme internazionali sui diritti umani …, impedendo che avvengano 'sbarchi' in luoghi 'non sicuri', che si tradurrebbero in aperte violazioni del principio di non-respingimento, del divieto di 'espulsioni collettive', e, più in generale, pregiudizievoli dei diritti di 'protezione internazionale' accordati ai rifugiati e richiedenti asilo.[34]

Ha altresì voluto precisare che, alla luce del regime internazionale del mare, "i migranti, soccorsi in mare, ave(vano) un *vero e proprio diritto soggettivo al ricovero in un POS (place of safety)*, diritto speculare all'obbligo assunto dagli Stati firmatari delle convenzioni" di soccorso.[35]

Ebbene, sostiene il GIP di Trapani, la Libia difficilmente poteva essere considerata un luogo sicuro (p. 32) al momento della conclusione del Memorandum con l'Italia ed altresì al momento della vicenda su cui si esprime, constatazione confermata anche dall'UNHCR, che aveva richiamato i disordini in atto, l'assenza di un sistema d'asilo, l'impossibilità di ottenere protezione, le modalità di detenzione dei migranti. Preso atto che in Libia si verificano gravi violenze nei confronti dei mi-

[32] GIP Trapani, sentenza del 23 maggio 2019, sulla quale si rinvia a L. Masera, "La legittima difesa dei migranti e l'illegittimità dei respingimenti verso la Libia (caso *Vos-Thalassa*)", in *Diritto Penale Contemporaneo*, 24 giugno 2019.

[33] Convenzione per la salvaguardia della vita umana in mare (SOLAS), adottata il 1novembre 1974, recepita dall'Italia con l. n. 313/1980.

[34] Ivi, p. 27.

[35] Ivi, p. 46.

granti, questi avevano "*un vero e proprio diritto soggettivo al ricovero in un POS*, diritto speculare all'obbligo assunto dagli Stati firmatari delle Convenzioni. I migranti … agirono in difesa di diritti umani ancora più pregnanti, come il diritto alla vita e all'integrità fisica", a tutela dei quali è consentito l'esercizio della legittima difesa ai sensi dell'art. 52 c.p. (p. 43). Lo sbarco in Libia, infatti, si sarebbe posto il violazione del divieto di respingimento, che, oltre ad essere sancito dal diritto internazionale pattizio e dal diritto dell'UE, "ha assunto rango consuetudinario e cogente" (p. 37). Laddove migranti e rifugiati vengano salvati in mare, "la necessità di evitare che le operazioni di sbarco avvengano in territori dove la loro vita e libertà potrebbero essere minacciate è rilevante nel determinare cosa costituisce un luogo sicuro" (p. 47).[36]

Tale orientamento giurisprudenziale è stato messo in discussione dalla Corte di appello di Palermo,[37] che, rifacendosi alle argomentazioni del PM nel provvedimento di impugnazione, ha sostenuto che il principio di *non-refoulement*, centrale – come si è visto - nell'analisi svolta dal GUP, non costituisce un diritto della persona bensì "condizione di operatività degli Stati soccorritori", non rientrando "tra i diritti personali dei migranti" (p. 4). Riteniamo non condivisibile tale lettura del divieto di respingimento che, se indubbiamente costituisce un obbligo di condotta degli Stati, nondimeno rappresenta anche un diritto della persona, come può ricavarsi dalle fonti nazionali e sovranazionali che lo codificano ed altresì dalla giurisprudenza degli organi internazionali. Sul punto torneremo a breve.

Tra l'altro è doveroso evidenziare che la posizione della Corte di appello di Palermo non è in linea con quella della Corte di Cassazione, che, come si è visto, ha 'blindato' una nozione di luogo di sbarco sicuro che integra il principio di *non-refoulement* e il diritto di asilo quali diritti irrinunciabili.[38]

2.4. La nozione di luogo di sbarco sicuro ricavabile dalla giurisprudenza

La giurisprudenza sopra richiamata mostra come si sia consolidata una lettura costituzionalmente orientata del dovere di soccorso e della nozione di luogo di sbarco sicuro, che vengono interpretati alla luce degli obblighi internazionali cui l'Italia è vincolata in virtù degli art. 10 e 117 Cost. Il parametro di riferimento è co-

---

[36] Sulla pronuncia si rinvia a L. Masera, "I migranti che si oppongono al rimpatrio in Libia non possono invocare la legittima difesa: una decisione che mette in discussione il diritto al non refoulement", in *Sistema Penale*, 21.07.2020, <https://www.sistemapenale.it/it/scheda/masera-appello-palermo-vos-thalassa-migranti-rimpatrio-libia-legittima-difesa>.

[37] Corte di appello di Palermo, IV Sezione Penale, sentenza del 3 giugno 2020, n. 1525.

[38] Va anche segnalato che si è chiusa con il non luogo a procedere l'udienza preliminare nei confronti di Matteo Salvini, nella sua qualità di Ministro dell'Interno, con riguardo al caso *Gregoretti*. <https://www.ilsole24ore.com/art/caso-gregoretti-salvini-prosciolto-non-luogo-procedere-fatto-non-sussiste-AEJSR5I?refresh_ce=1> (06/21). Mentre va registrato il rinvio a giudizio dello stesso, accusato di sequestro di persona e rifiuto d'atti d'ufficio, da parte del GUP di Palermo nell'ambito del processo *Open Arms*, originato dal diniego dello sbarco dei 147 migranti soccorsi in acque internazionali, nella zona SAR libica. <https://www.avvenire.it/attualita/pagine/palermo-salvini-rinviato-a-giudizio-open-arms> (06/21).

stituito dai diritti fondamentali della persona*, in primis* il principio di *non-refoulement*, ma altresì il diritto di chiedere asilo, situazioni giuridiche soggettive che hanno trovato riconoscimento anche da parte della Corte europea dei diritti umani.[39]

Pur senza volerci dilungare sulla ricostruzione delle fonti internazionali che vengono in rilievo a tal riguardo, ci sembra quanto meno opportuno richiamarle sinteticamente. L'art. 98 della UNCLOS[40] costituisce la pietra miliare del regime internazionale del mare in quanto codifica il dovere della solidarietà in mare, che ha acquisito nel tempo rango consuetudinario. Al par. 1 detta disposizione stabilisce l'obbligo per lo Stato di esigere che il comandante di una nave che batte la sua bandiera, nella misura in cui gli sia possibile adempiere senza mettere a repentaglio la nave, l'equipaggio o i passeggeri, presti soccorso a chiunque sia trovato in mare in condizioni di pericolo. Trattasi dunque di un obbligo cui è vincolato lo Stato contraente ma che si traduce, indirettamente, in un obbligo per il Comandante della nave,[41] il quale, tranne che in rare eccezioni, non può sottrarvisi.[42] D'altra parte, l'obbligo per il Comandante di *qualsiasi* nave di intervenire in soccorso di persone in difficoltà in mare, nella misura in cui possa farlo senza mettere a rischio la propria nave e le persone a bordo, aveva già trovato collocazione all'art. 10 della Convenzione internazionale sul salvataggio[43] e alla regola 33.4 SOLAS, che fa espresso riferimento alle navi private. Tra l'altro, se il Comandante di una nave non può esimersi dall'intervenire in soccorso di persone *in distress* su ordine del proprio Stato di bandiera o del centro di coordinamento della zona SAR in cui si trovano dette persone, nondimeno tale dovere sussiste anche in caso di autonoma iniziativa, laddove si imbatta in naufraghi o venga a conoscenza di condizioni di pericolo.[44] Né sono ammissibili interferenze da parte del proprietario, del noleggiatore, della società che gestisce l'imbarcazione o di qualunque altra persona.[45]

Dunque, il diritto internazionale del mare impone, in maniera diretta o indiretta, al Comandante di *qualsiasi* nave, pubblica o privata che sia, comprese le navi di organizzazioni umanitarie, di intervenire per prestare assistenza a *qualunque* persona si trovi in difficoltà in *qualsiasi* zona marina, "senza distinzioni relative alla nazionalità o allo status di tale persona o alle circostanze nelle quali tale persona viene trovata".[46]

---

[39] *Hirsi e altri c. Italia*, cit. *supra* nota 29, par. 202.

[40] Convenzione delle Nazioni Unite sul diritto del mare del 10 dicembre 1982, resa esecutiva dalla l. 2 dicembre 1994, n. 689.

[41] In argomento I. Papanicolopulu, "Immigrazione irregolare via mare, tutela della vita umana e organizzazioni non governative", *Diritto immigrazione e cittadinanza*, fasc. 3, 2017, p. 11.

[42] M. Starita, "Il dovere di soccorso in mare", cit. *supra* nota 23, p. 5 ss.

[43] Convenzione internazionale sul salvataggio ("Salvage"), adottata il 28 aprile 1989, recepita dall'Italia con l. n. 129/1995.

[44] I. Papanocolopulu, "Immigrazione irregolare", cit. *supra* nota 41, p. 14. Il dovere di soccorso trova una corrispondenza nel cod. nav. italiano, il quale, all'art. 1158, sanziona penalmente il Comandante che vi si sottragga.

[45] Capitolo 5, Regola 34-1 SOLAS, come modificata nel 2004.

[46] Convenzione SAR, capitolo 2.1.10. Cfr. Anche la regola 33.1 SOLAS. In dottrina v. T. Scovaz-

Tornando all'art. 90 UNCLOS, questo, al par. 2, impegna le Parti contraenti a promuovere la costituzione e il funzionamento permanente di un servizio adeguato ed efficace di ricerca e soccorso per tutelare la sicurezza marittima, collaborando con gli Stati adiacenti tramite accordi regionali. La Convenzione SAR prevede l'istituzione di zone di competenza di ciascuno Stato costiero, seppure le regole in materia non escludano che lo stesso possa operare anche al di fuori di esse, laddove si renda necessario sulla base delle circostanze di fatto. Tutti gli Stati costieri del Mediterraneo hanno provveduto ad istituire una propria zona SAR e a comunicarla all'IMO. Tuttavia negli ultimi anni si è assistito al venir meno degli stessi dagli obblighi di ricerca e soccorso e a continui conflitti di competenza, che vedono di sovente coinvolte Italia, Malta e più di recente Libia, con effetti detrimenti sul diritto alla vita delle persone che provano a raggiungere l'Europa.[47]

Le Convenzioni UNCLOS, SOLAS e SAR stabiliscono poi che l'operazione di salvataggio può considerarsi conclusa solamente con lo sbarco dei naufraghi in un luogo sicuro,[48] che solo temporaneamente può essere la nave soccorritrice.[49] Cionondimeno i suddetti trattati non individuano in modo tassativo il luogo di sbarco ma si limitano a richiamare gli Stati costieri al dovere di collaborare con le autorità dello Stato nella cui zona SAR sia avvenuto il salvataggio di modo da sollevare nel più breve tempo possibile il Comandante della nave dalla responsabilità dei naufraghi soccorsi.[50] Lo Stato nella cui zona SAR sia avvenuto il salvataggio, pertanto, non necessariamente deve costituire il luogo di sbarco ma deve farsi parte attiva per l'individuazione dello stesso.[51]

---

zi, "Human Rights and Immigration at Sea", in R. Rubio-Marín (ed.), *Human Rights and Immigration*, Oxford University Press, Oxford, 2014, p. 225.

[47] In argomento G. Cataldi, "Search and Rescue of Migrants at Sea in Recent Italian Law and Practice", G. Cataldi, A. Del Guercio, A. Liguori (eds.), *Migration and Asylum Policies*, Editoriale Scientifica, Napoli, 2020, p. 11 ss., reperibile al sito <https://www.mapsnetwork.eu/> (06/21).

[48] Par. 3.1 e 4.8 degli emendamenti alle Convenzioni SAR e SOLAS, RIS. MSC 155(78), 20 maggio 2004.

[49] Par. 6.13, *Guidelines on the treatment of persons rescued at sea*, cit.

[50] Par. 3.1.9 Convenzione SAR. Ci sembra assolutamente incompatibile con le fonti internazionali sul diritto del mare la ricostruzione operata dal Tribunale di Catania, sez. GIP, sentenza del 9 agosto 2021, resa sul caso Gregoretti, secondo cui, non essendo previsto un termine perentorio per l'indicazione del POS e per lo sbarco, questo dovrebbe avvenire non "con assoluta immediatezza" ma "in un tempo ragionevolmente rapido", che può configurarsi anche in 2-3 giorni, di modo da poter organizzare la logistica per l'accoglienza dei naufraghi (pp. 97-98). In vero, nessun trattato internazionale legittima il ritardo nell'approdo dei profughi al fine di organizzare la distribuzione tra i centri o, addirittura, tra diversi Paesi. Tra l'altro, il GIP opera una distinzione, che non si rinviene nel regime internazionale del mare, tra indicazione del POS e sbarco, quando la finalità dell'operazione di soccorso, come evidenziato *supra*, è proprio lo sbarco, costituendo l'individuazione del luogo sicuro solamente un passaggio preliminare per garantire che le persone a bordo raggiungano la terraferma nel rispetto dei loro diritti fondamentali. La sentenza del Tribunale di Catania appare discutibile anche nella ricostruzione del rapporto tra fonti internazionali e fonti interne, poiché rinviene nell'Accordo di Tavolo tecnico operativo del 12 febbraio 2019 – ovvero un mero documento interno di lavoro – la base giuridica che legittima il ritardo nell'assegnazione del POS, subordinata ai "tempi necessari" per valutare le necessità logistiche a terra e la disponibilità dei partner europei ad accogliere i profughi. Nessuna deroga di tale tipologia si rinviene nei trattati internazionali sul diritto del mare, che invece insistono sullo sbarco tempestivo delle persone soccorse.

[51] Par. 2.5 Risoluzione MSC.167(78) (adottata nel maggio 2004 dal Comitato Marittimo per la Sicurezza insieme agli emendamenti SAR e SOLAS).

Dei principi guida al fine di individuare un porto di approdo sono contenuti in alcuni documenti privi di portata giuridica obbligatoria adottati dall'IMO, che integrano il regime internazionale del mare con quello di protezione dei rifugiati e dei diritti umani. Ai sensi del par. 6.19 delle Linee guida sulle persone soccorse in mare lo sbarco non può avvenire in luoghi rispetto ai quali i naufraghi lamentino il timore di essere perseguitati. Ancora, nella guida redatta congiuntamente con l'UNCHR, viene specificato che il *place of safety* è una località dove le operazioni di soccorso si considerano concluse, e dove, oltre ad essere soddisfatte le necessità umane primarie (come cibo, alloggio e cure mediche), la sicurezza dei sopravvissuti o la loro vita non sono più minacciate.[52] Laddove, pertanto, dallo sbarco derivi la violazione del principio di *non-refoulement* il luogo individuato non può dirsi sicuro.[53]

I principi sopra richiamati indicano, dunque, in maniera chiara, che il porto di sbarco deve essere determinato nel rispetto dei diritti umani. Tale lettura emerge altresì dai documenti adottati nell'ambito del Consiglio d'Europa, in particolare dalla ris. 1821(2011) e dalla raccomandazione della Commissaria per i diritti umani adottata nel 2019[54]. Viene ivi ribadito che la sicurezza del luogo di sbarco va valutata, conformemente al diritto marittimo, ai diritti umani e al regime internazionale di protezione dei rifugiati.[55] Tra l'altro viene rimarcato il ruolo del Comandante della nave, che è nella posizione più idonea per individuare il luogo di sbarco, e al quale dunque non vanno fornite istruzioni che si possano tradurre nello sbarco dei naufraghi in un luogo non sicuro.

A venire in rilievo nel quadro sopra delineato è in special modo il principio di *non-refoulement*, che ha per la prima volta trovato codificazione all'art. 33.1 della Convenzione di Ginevra del 1951 nei confronti dei *rifugiati* ai sensi dell'art. 1A. Nondimeno il suddetto articolo ammette delle eccezioni laddove la persona sia considerata un pericolo o una minaccia per la sicurezza del paese in cui risiede, anche in ragione di una condanna definitiva per un crimine o un delitto particolarmente grave (par. 2).

Un ambito di applicazione soggettivo più ampio connota invece il principio di non respingimento che si è affermato nei sistemi internazionali di protezione dei diritti umani a partire dalla giurisprudenza resa in materia di allontanamento dello straniero sulla base dell'art. 3 CEDU, che sancisce il divieto di tortura e di trattamenti e pene inumani e degradanti. La Corte di Strasburgo ha ricavato dalla disposizione in questione, attraverso il meccanismo della protezione *par ricochet*, il divieto assoluto e inderogabile di espellere o respingere un non cittadino verso territori nei quali correrebbe il rischio di subire trattamenti lesivi della sua dignità. Tale divieto riguarda tutte le persone e non esclusivamente i *rifugiati*, ha portata assoluta e inderogabile e non ammette bilanciamenti neanche in caso di pericolo per l'ordine

[52] UNHCR, IMO, *Soccorso in mare. Guida a principi e pratiche da applicarsi a migranti e rifugiati*, 2015.

[53] UNHCR, *General legal considerations: search-and-rescue operations involving refugees and migrants at sea*, 2017.

[54] *Vite salvate. Diritti protetti. Colmare le lacune in materia di protezione dei rifugiati e migranti nel Mediterraneo*, 2019.

[55] Ivi, p. 11.

pubblico e la sicurezza, poiché è stato ricavato dal divieto di tortura che, secondo la Corte Edu, costituisce uno dei valori irrinunciabili di una società democratica.[56]

Analoga portata ha il divieto di respingimento ricavato dagli artt. 6 (diritto alla vita) e 7 (divieto di tortura e di trattamenti e pene disumani e degradanti) del Patto sui diritti civili e politici dal Comitato per i diritti umani delle Nazioni Unite e codificato all'art. 3 della Convenzione delle Nazioni Unite contro la tortura.

Il principio di *non-refoulement* è stato espressamente chiamato in causa rispetto alle migrazioni via mare fin dalla crisi indocinese, in occasione della quale l'*Executive Committee* dell'UNHCR sostenne l'applicabilità dello stesso anche in caso di esodo di massa. In particolare veniva precisato che

> In situations of large-scale influx, asylum seekers should be admitted to the State in which they first seek refuge and if that State is unable to admit them on a durable basis, it should always admit them at least on a temporary basis. In all cases the fundamental principle of non-refoulement – including non rejection at the frontier – must be scrupulously observed. [57]

Dunque dal principio di non respingimento deriverebbe, secondo l'ExCom dell'UNHCR, opinione condivisa da una dottrina autorevole,[58] il diritto di ingresso nel territorio statale, quanto meno temporaneamente, al fine di presentare domanda di asilo.

Del suddetto divieto, al quale viene attribuita portata generale,[59] è stata poi ribadita la perentorietà in tutte le circostanze, sia con riguardo alle operazioni di salvataggio, anche qualora siano avvenute in acque internazionali o nella zona SAR di un Paese terzo,[60] sia con riguardo a quelle di intercettazione, ovunque lo Stato eserciti la propria giurisdizione, anche al di fuori dei propri confini.[61] A tal riguardo la Corte di Strasburgo ha precisato che "la specificità del contesto marittimo non può portare a sancire uno spazio di non diritto all'interno del quale gli individui non sarebbero soggetti ad alcun regime giuridico che possa accordare loro il godimento dei diritti e delle garanzie previsti dalla Convenzione e che gli Stati si sono impe-

---

[56] *Saadi c. Italia*, ric. n. 37201/06, Grande Camera, sentenza del 28 febbraio 2008, par. 139.

[57] ExCom 32nd session. Contained in United Nations General Assembly Document No. 12A (A/36/12/Add.1). Conclusion, 21 ottobre 1981.

[58] G.S. Goodwin-Gill, J. McAdam, *The Refugee in International Law*, Oxford University Press, Oxford, 2007, p. 257 ss.; J.C- Hathaway, *The Rights of Refugees under International Law*, Cambridge University Press, Cambridge, 2005, p. 370 ss.

[59] UNHCR, *Advisory Opinion on the Extraterritorial Application of Non-Refoulement Obligations under the 1951 Convention relating to the Status of Refugees and its 1967 Protocol*, 2017, p. 15. Di tale opinione anche una parte della dottrina, tra gli altri J. Allain, "The jus cogens nature of non-refoulement", *International Journal of Refugee Law*, 2001, p. 533 ss.

[60] OHCHR, *Lethal Disregard Search and rescue and the protection of migrants in the central Mediterranean Sea*, 2021, p. 19. Cfr. Altresì OHCHR, *Recommended Principles and Guidelines on Human Rights at International Borders (2014), I. A.1, II.A.2, II.A.5*.

[61] UNHCR, *Advisory Opinion*, cit. In argomento si rinvia a S. Trevisanut, "The Principle of Non-Refoulement And the De-Territorialization of Border Control at Sea", *Leiden Journal of International Law*, 2014, pp. 661-675.

gnati a riconoscere alle persone poste sotto la loro giurisdizione".[62] Di conseguenza, anche in tali circostanze devono trovare ottemperanza il principio di non respingimento ex art. 3 CEDU e il divieto di espulsioni collettive di cui all'art. 4 del Prot. 4, da cui deriva, tra l'altro, il dovere di identificare le persone, svolgere colloqui personali e consentire l'accesso alle procedure di asilo. È di palese evidenza che tali operazioni non possono svolgersi a bordo di un natante, sia in quanto l'operazione di salvataggio deve concludersi nel più breve tempo possibile, poiché, come si è detto, la nave solo temporaneamente è un luogo sicuro, sia perché il personale di bordo non è formato per ricevere ed esaminare le domande di asilo, come sostenuto dalla stessa Corte europea dei diritti umani.[63]

Alla luce del quadro sopra delineato, l'UNHCR ha statuito che, in seguito ad una operazione di salvataggio o di intercettazione,

> before disembarking, transferring, or otherwise delivering or returning a person who may be in need of international protection to the territory or jurisdiction of another State, States need to ensure that the person concerned:
> - will be admitted and protected against *refoulement* there;
> - will have access to fair and efficient procedures for the determination of refugee status or, as applicable, other forms of international protection;
> - will be treated in accordance with international refugee law and human rights standards.[64]

3. Conclusioni

La giurisprudenza illustrata consente di evidenziare una nozione di luogo di sbarco sicuro improntata al rispetto dei diritti umani, in particolare del principio di *non-refoulement*, strumento di realizzazione di quella *libertà dalla paura* che costituisce una dimensione essenziale della *sicurezza umana*, da intendersi, secondo le Nazioni Unite, come "the right of people to live in freedom and dignity, free from poverty and despair".[65] A contribuire in tal senso sono le ONG, con le operazioni di ricerca e soccorso in mare e l'individuazione di un luogo di sbarco sicuro. Ma anche, come abbiamo provato a dimostrare, i giudici, baluardo dei principi fondanti dell'ordinamento italiano. Tra l'altro, gli avvenimenti registrati negli ultimi anni in Italia hanno reso manifesto lo iato tra poteri statali, l'Esecutivo, da una parte, protagonista assoluto della guerra alle ONG, il Giudiziario, dall'altro, baluardo dei diritti umani come garantiti anche nell'ordinamento internazionale, al cui rispetto l'Italia è vincolata in virtù degli artt. 10, 11 e 117 della Costituzione.

Va preso atto con rammarico che ancora al momento in cui scriviamo si assiste all'inerzia degli Stati europei rispetto agli obblighi di ricerca e soccorso, non è stata

---

[62] *Hirsi e altri c. Italia*, cit. *supra* nota 29, par. 169.

[63] *Ivi,* par. 185.

[64] UNHCR, *Advisory Opinion*, cit., par. 6. Cfr. anche OHCHR, *Lethal Disregard*, cit., pp. 16-17.

[65] AG, *Follow-up to General Assembly resolution 64/291 on human security. Report of the Secretary-General*, UN Doc. A/66/763 del 5 aprile 2012, par. 6.

sospesa la cooperazione con la guardia costiera libica,[66] giungono notizie di drammatici naufragi, diverse navi di ONG sono bloccate nei porti e non è stato raggiunto un accordo a livello UE per una operazione comune di ricerca e soccorso nel Mediterraneo né per la redistribuzione dei naufraghi tratti in salvo. Non ha sortito effetti neppure la decisione del Comitato per i diritti umani,[67] ad avviso del quale le autorità italiane sono venute meno agli obblighi di *due diligence* che derivano dall'art. 6 del Patto sui diritti civili e politici per non essere intervenute prontamente, nell'ottobre 2013, in soccorso di un'imbarcazione in *distress* con a bordo circa trecento persone, poi naufragate.[68]

In questo complesso scenario, il Mediterraneo si presenta dunque nella doppia veste di via di accesso alla salvezza per le persone costrette a migrare e, contestualmente, come spazio di non diritto, nel quale gli Stati vengono meno ai loro obblighi, in tal modo amplificando i pericoli per coloro che affrontano un viaggio considerato tra i più pericolosi. Il Mediterraneo come spazio di libertà, dunque, a fronte di politiche e strategie di *pre-entrée* nella Fortezza Europa, che non garantisce adeguati canali di accesso legale. Ma altresì spazio sottoposto a dispositivi di controllo e di negazione dei diritti, *in primis* del diritto alla vita, ma altresì del diritto a non essere respinti, di chiedere asilo e di trovare rifugio dalla persecuzione, dalle guerre, dalla povertà.

[66] Fortemente osteggiata dalle O.O.I.I. ed anche dal PE, *Stop Cooperation with and Funding to the Libyan Coastguard*, MEPs Ask, 27 April 2020; OHCHR, *Press briefing note on Migrant rescues in the Mediterranean*, 8 maggio 2020; *Unhcr Position On The Designations Of Libya As A Safe Third Country And As A Place Of Safety For The Purpose Of Disembarkation Following Rescue At Sea*, September 2020; UNSC, *Despite Calls for Libyan National Army Ceasefire Amid COVID-19 Pandemic, Unabated Fighting Could Push Libya to New Depths of Violence*, 19 May 2020.

[67] Comitato per i diritti umani, *A.S., D.I., O.I. and G.D.*, com. n. 3042/2017, decisione del 27 gennaio 2021.

[68] Ci si riferisce al cd. 'naufragio dei bambini', in cui hanno perso la vita più di duecento persone, tra cui, per l'appunto, sessanta bambini. Va anche segnalato che si è aperto il 19 gennaio 2021 il processo penale a carico del Comandante della Marina Militare e della Capitaneria di Porto in ruolo al momento del naufragio, accusati di omissione di atti d'ufficio ed omicidio plurimo aggravato per aver posto in essere condotte che portarono al fatale ritardo nel soccorso dei profughi.

LA SALVAGUARDIA DELLA VITA UMANA IN MARE COME OBBLIGO DI *JUS COGENS* DEGLI STATI

Fabio Marcelli

1. La strage intermittente e le sue cause

Il diritto nasce e si sviluppa per dare una risposta agli eventi della vita e soprattutto a quelli, tra tali eventi, che hanno un maggiore impatto di natura tragica e catastrofica. Le stragi di migranti in cerca di un futuro migliore lontano dalla propria patria, che avvengono in mare e hanno prodotto, in particolare nel Mediterraneo ma anche nell'Oceano Atlantico ed altrove, decine di migliaia di vittime negli ultimi anni,[1] appartengono senza dubbio a questa categoria di eventi tragici e catastrofici.

Uno dei tanti episodi di questo genere è quello riferito da Irini Papanicolopu in un articolo pubblicato dalla Rivista internazionale della Croce Rossa:

> These vessels become particularly dangerous if they are used to smuggle migrants, as numerous incidents that have happened in the Mediterranean Sea have demonstrated. Migrants have died on a daily basis in the Mediterranean Sea. In an instance that became famous, a small inflatable rubber dinghy, with seventy-two persons on board, was stranded for fifteen days in the Mediterranean before being washed ashore in Libya. During those days, the dinghy was approached by a military helicopter, a large military vessel and various other craft, none of which proceeded to rescue those on board. As a result of this lack of assistance, only ten people survived out of the six dozen initially on the dinghy.[2]

Episodi del genere ne sono avvenuti a bizzeffe e le vittime di questa strage a intermittenza, continua e silenziosa, si contano ormai a oltre ventimila nei soli ultimi sette anni e nel solo Mediterraneo.[3]

Al fine di stabilire quali rimedi approntare per evitarne il verificarsi, nonché di qualificare in modo giuridicamente più preciso tali eventi occorre stabilirne anzitutto le cause remote ed immediate. A seconda della natura delle cause identificate cambia infatti l'approccio giuridico da adottare. Qualora si trattasse di un evento naturale, occorrerebbe infatti limitarsi a stabilire misure preventive e a prevedere idonee azioni di salvataggio, come avviene in generale per i naufragi e le altre disgrazie marittime.

Passi di questo genere vanno ovviamente adottati anche in relazione alle morti

---

[1] Per le cifre cfr. F. Schettino, *Human Security: Risk Indicators for the Maritime Space*, in questo volume.

[2] I. Papanicolopu, "The duty to rescue in sea, at peacetime and in war: A general overview", *International Review of the Red Cross*, n. 902, agosto 2015, p. 492.

[3] Statista, Deaths of migrants in the Mediterranean Sea 2021, <www.statista.com> (03/21).

in mare, ma riescono a cogliere solo un aspetto e forse neanche quello centrale, di quanto disgraziatamente avviene.

Le morti in mare, ovvero la propria e vera strage che si verifica a singhiozzo nelle acque del Mediterraneo o altrove appaiono invero da un lato la conseguenza di eventi naturali ma dall'altro e soprattutto l'esito catastrofico finale di una vicenda interamente umana e sociale, costituita dalle migrazioni di massa. Umani sono certamente le motivazioni e la scelta, per molti versi obbligata, di mettersi in mare nel tentativo di raggiungere le coste europee dopo un viaggio che dura in media molti mesi attraversando lande inospitali. Umane sono d'altro canto anche le responsabilità da accertare, per un aspetto quelle delle situazioni che rendono le migrazioni l'unica alternativa e dall'altro, quelle della mancata predisposizione di mezzi idonei a salvare la vita di chi attraversa il mare nel disperato tentativo di dare a sé e alla propria famiglia una prospettiva di futuro. E il discorso non può fermarsi certo qui, come vedremo fra poco.

Dal primo punto di vista il discorso si presenta evidentemente lungo e complesso, dovendo esso identificare responsabilità di fondo attinenti all'esistenza di un modello di sottosviluppo indotto basato sullo sfruttamento selvaggio delle risorse che rende gran parte del Pianeta un mero serbatoio di ricchezza destinata ad essere utilizzata e valorizzata altrove, lasciando le popolazioni residenti nei territori colpiti in stato di abbandono e di miseria, aggravati in modo sempre più evidente e inarrestabile dal degrado ambientale.[4]

Data la complessità del discorso è anche più difficile identificare in modo sufficientemente preciso le responsabilità, specie se dall'ambito, di fondamentale importanza ma necessariamente generico, del giudizio storico, si vuole passare sul piano del diritto e della giustizia.

Diversamente stanno però le cose per il secondo dei due aspetti ora enunciati, attinente a un fenomeno molto più preciso e circoscritto, e cioè l'obbligo di soccorrere le persone che, in seguito a un tentativo di attraversare il mare nel corso di una migrazione, si trovino in pericolo di vita.

È infatti del tutto evidente come, in tal caso, la violazione di tale obbligo dia vita a una responsabilità giuridica vera e propria, fino al punto di imputare la responsabilità dell'eventuale morte o delle eventuali lesioni subite da persone che si trovino in una situazione di questo tipo, all'entità in capo alla quale esisteva l'obbligo del salvataggio. Ciò anche in forza del principio di carattere generale in forza del quale omettere di impedire il verificarsi di una situazione che si ha l'obbligo giuridico di impedire equivale a cagionarla. Nel caso in esame, poi, c'è qualcosa di più della mera omissione di soccorso, dato che gli Stati non si limitano ad astenersi dall'intervenire ma intervengono per impedire ad altri soggetti di farlo.[5]

Tornando al quesito iniziale, possiamo rispondere che in realtà l'evento si veri-

[4] Vedi, sul fenomeno dei cosiddetti rifugiati ambientali, M. Da Pra Pocchiesa, "Crisi climatica, il grande esodo degli invisibili", in *L'Extraterrestre (supplemento al manifesto)* del 25 febbraio 2021.

[5] Vedi A. Del Guercio, *Migrazioni via mare, luogo di sbarco sicuro e principio di* non refoulement, in questo Volume.

fica in conseguenza di una miscela di cause naturali e di scelte umane. Del tutto preponderanti appaiono tuttavia le seconde, e in particolare quella di chi nega il soccorso a chi si trova in pericolo di vita. Constatazione che diventa ancora più pregnante se si pone mente al fatto innegabile che chi agisce in tal modo lo fa in piena consapevolezza delle possibili conseguenze letali di tale rifiuto, trattandosi, anzi, di un comportamento chiaramente finalizzato a scoraggiare l'arrivo di migranti sulle coste europee, come parte di una politica di contenimento delle migrazioni.

Quest'ultimo aspetto pare invero determinante al fine di qualificare la condotta degli Stati e delle organizzazioni internazionali (tra le quali in prima fila la stessa Unione europea), che appaiono, nonostante vuote proclamazioni di segno apparentemente contrario, responsabili del mancato soccorso. L'esistenza di un disegno politico, a volte esplicito, a volte tacito, che consiste nello scoraggiare il flusso delle migrazioni verso l'Europa a costo di lasciare morire decine di migliaia di persone, costituisce infatti a ben vedere l'elemento decisivo. Tale disegno politico si trasforma quindi in una macchinazione criminale talmente sottile e perversa da potersi realizzare anche mediante mere omissioni. Omissioni di soccorso che, sia detto per il momento per inciso, costituiscono una figura abbastanza tipica di reato in molti ordinamenti giuridici contemporanei.

Abbiamo in tal modo stabilito due caratteri differenziali che valgono a distinguere le stragi di migranti che avvengono in mare da altri disastri marittimi che comportino la perdita di vite umane. Essi attengono da un lato alla sfera delle motivazioni che spingono i migranti ad attraversare il mare, spesso su battelli di fortuna e, dall'altro, al fatto che mediante di esse si realizza, in modo dissimulato ma non meno deliberato ed efficace, una scelta politica dei Paesi europei volta a scoraggiare o comunque contenere le migrazioni via mare. Le stragi in mare, quindi, come *instrumentum regni* e come armi di terrorismo psicologico di massa contro coloro che aspirano a migrare.

2. Il diritto di migrare

Incidentalmente possiamo a questo punto porci l'interrogativo se esista o meno un diritto di migrare che includa, come proprio aspetto o pertinenza, quello di attraversare il mare, o quantomeno di provarci, per riprendere il titolo di un interessante saggio scritto in argomento.[6]

Il diritto di migrare è affermato in termini abbastanza perentori dalla Dichiarazione universale dei diritti umani, la quale al suo art. 13, para. 2, recita come segue: "Ogni individuo ha diritto di lasciare qualsiasi paese, incluso il proprio, e di ritornare nel proprio paese".

È altresì noto come a tale diritto dell'individuo non corrisponda l'obbligo degli Stati di cui non è cittadino di permetterne l'accesso sul proprio territorio. Ne risulta

[6] F. De Vittor, "Il diritto di traversare il Mediterraneo… o quantomeno di provarci", in *Diritti umani e diritto internazionale*, 2014(1), pp. 63-82.

una situazione di oggettiva paralisi del diritto all'espatrio, dato che quest'ultimo non può ovviamente realizzarsi nel senso proprio e pieno del termine, se all'abbandono del territorio originario non si accompagna l'insediamento in un nuovo territorio.

Si tratta insomma di una norma dimezzata, incapace di dispiegare a fondo i suoi effetti nella realtà. Pur prendendo atto di questo vero e proprio paradosso, appare significativo il fatto che il diritto internazionale garantisca un diritto a migrare. Se pure gli Stati non sono obbligati ad aprire le proprie frontiere a coloro che lo esercitano, salvi beninteso gli obblighi di natura convenzionale o consuetudinaria relativi all'accoglienza dei richiedenti asilo, la sua affermazione impone loro quantomeno di garantire la vita e la sicurezza dei migranti, le quali peraltro sono già garantite da altre norme.

Il diritto alla vita e alla sicurezza è infatti garantito dal diritto internazionale in termini generali, a prescindere cioè dall'appartenenza di un individuo a una determinata cittadinanza statuale. Bisogna anzi ritenere che la protezione in tal modo garantita dall'ordinamento giuridico internazionale a beni essenziali e imprescindibili risulti addirittura rafforzata qualora l'individuo si trovi in situazioni di particolare vulnerabilità. Ovvero qualora gli eventi pericolosi o lesivi si verifichino in spazi sottratti alla sovranità di singoli Stati che non per questo motivo dovrebbero essere considerati sottratti all'impero del diritto, ma anzi luoghi nei quali la protezione dovrebbe essere attuata con efficacia ancora maggiore.

Nondimeno, qualche problema si pone riguardo alle modalità con le quali tali protezione possa o debba essere esercitata. Trattandosi infatti di spazi sottratti alla giurisdizione nazionale, sarebbero in astratto legittimati ad intervenire tutti gli Stati, come pure enti o al limite individui privati. E sarebbe altresì auspicabile che una collaborazione venisse all'uopo attuata a livello internazionale. Di fatto qualche passo è stato compiuto in questa direzione, coi vari accordi che hanno inteso concretizzare il dettato in materia della Convenzione delle Nazioni Unite sul diritto del mare, ma la realtà dei fatti mostra come in realtà si sia ancora ben lontani dal raggiungimento di una soddisfacente cooperazione che costituisca una garanzia effettiva per la salvaguardia della vita delle persone in pericolo. Proprio questa situazione di incompiutezza della collaborazione internazionale da costruire in materia rende peraltro quantomeno obbligatorio che gli Stati si astengano dal mettere i bastoni fra le ruote a coloro che intervengono, si tratti di organizzazioni non governative attive in questo senso o anche solo di pescatori che vengono a trovarsi in condizione di operare i soccorsi.

In altri termini abbiamo assistito negli ultimi anni, alla luce delle necessità per certi versi di tipo nuovo poste dal fenomeno della traversata di massa degli spazi marini per cercare asilo altrove, a un'evoluzione, o forse piuttosto a un'involuzione (o una perversione) dell'obbligo di salvataggio, che da molto tempo si è affermato sia in tempo di pace che in tempo di guerra.

3. L'obbligo di salvataggio

L'obbligo di salvataggio in mare poggia sia su solide radici consuetudinarie risalenti, sia su di un nutrito e articolato *corpus* di trattati stipulati in epoca abbastanza recente.

Alla base di tale norma possiamo rinvenire da un lato una prassi consuetudinaria antichissima e ben dotata dei requisiti classici della *diuturnitas* e dell'*opinio juris* e, dall'altro, obblighi fondamentali di carattere più generale attinenti alla salvaguardia della vita umana. A tale secondo proposito può anzi sostenersi come, se un qualche fondamento va riconosciuto alla controversa figura giuridica del cosiddetto *duty of protect*, essa si applica proprio a situazioni come quelle del salvataggio in mare, laddove ne va a chiare lettere esclusa la vigenza qualora esso entri in conflitto con la sfera riservata del dominio statale, con la sola discutibile eccezione delle cosiddette *mass violations*. Se quindi la motivazione di fondo che impone di guardare con grande cautela al *duty of protect*, se non di rigettarlo *tout-court*, è la possibile contraddizione fra di esso e la sovranità degli Stati, dimostrata del resto dai tentativi, alquanto maldestri peraltro, di affermarlo come ragione di interventi armati in territorio altrui, una motivazione di questo genere è invece palesemente assente qualora, come nel caso in esame, si tratti di interventi in spazi sottratti alla giurisdizione nazionale per salvare vite umane in pericolo.

Approfondendo il discorso riguardo alle radici consuetudinarie della norma è bene sottolineare come in molti ordinamenti, specie di *civil law*, esista un obbligo di soccorso formulato in caratteri generali, nei confronti di persone che si trovino in situazione di pericolo. La *ratio* di tale norme corrisponde d'altronde a un sentimento umano di importanza fondamentale che è la solidarietà di fronte a situazioni o fenomeni suscettibili di recare danno alle persone. Su tale base a carattere psicologico e antropologico si è sviluppata, nel corso dei secoli, una prassi specificamente riferibile agli spazi marini. Data la loro natura di spazi comuni o comunque sottratti all'imperio della giurisdizione statale, tali spazi, come altri per certi versi analoghi, quali quello extra-atmosferico o quelli polari, costituisce un ambiente particolarmente favorevole allo sviluppo di norme internazionali, alla cui graduale affermazione partecipano non solo gli Stati ma anche individui privati che entrano in relazioni di vario genere tra di loro. Non è quindi certamente casuale che, se da un lato in tali spazi si è enucleata la figura del pirata come *hostis humani generis*, dall'altro si è per converso dato luogo a una crescente attività di mutuo soccorso sul cui sviluppo di fatto poggiano le accennate norme di natura consuetudinaria.

All'inizio del Ventesimo secolo tale prassi è stata codificata da una serie di trattati multilaterali, il cui contenuto è stato poi trasfuso nelle Convenzioni sul diritto del mare. Da ultimo nell'art. 98 dell'*United Nations Convention on the Law of the Sea* (UNCLOS) del 1982, che consta dei due paragrafi seguenti:

> 1. Every State shall require the master of a ship flying its flag, in so far as he can do so without serious danger to the ship, the crew or the passengers: (a) to render assistance to any person found at sea in danger of being lost; (b) to proceed with all possible speed to

> the rescue of persons in distress, if informed of their need of assistance, in so far as such action may reasonably be expected of him; (c) after a collision, to render assistance to the other ship, its crew and its passengers and, where possible, to inform the other ship of the name of his own ship, its port of registry and the nearest port at which it will call.
> 2. Every coastal State shall promote the establishment, operation and maintenance of an adequate and effective search and rescue service regarding safety on and over the sea and, where circumstances so require, by way of mutual regional arrangements cooperate with neighbouring States for this purpose.[7]

L'obbligo incombe in via diretta sugli Stati e solo indirettamente sui natanti, ovvero su chi li dirige e guida. Gli Stati sono tenuti da un lato a far sì che costoro assistano le persone in pericolo di scomparire tra i flutti e ne procedano al salvataggio (la terza ipotesi è più specifica e prevede una collisione tra due o più imbarcazioni) e, dall'altro a mettere in piedi un efficace servizio di salvataggio marittimo nonché la necessaria collaborazione internazionale cogli Stati vicini.

Una serie di Trattati di portata più specifica affiancano la disposizione ora citata nell'intento, solo parzialmente riuscito, di darvi pratica ed efficace attuazione. Si tratta della Convenzione delle Nazioni Unite per la sicurezza della vita in mare (SOLAS) del 10 dicembre 1982, entrata in vigore il 16 novembre 1994, che stabilisce gli standard minimi che vanno osservati in materia di sicurezza nella costruzione, equipaggiamento e funzionamento delle navi. Occorre poi parlare della Convenzione internazionale per la ricerca e il salvataggio marittimi (SAR), firmata il 27 aprile 1979 ed entrata in vigore il 22 giugno 1985, che ha avuto minore fortuna delle altre ed è stata stipulata coll'intento di organizzare la cooperazione fra Stati vicini nello svolgimento delle operazioni di salvataggio in mare previste dal secondo comma del citato art. 98. Per nulla soddisfacente va giudicata l'attuazione di quest'ultima Convenzione, specie per quanto riguarda l'istituzione delle zone cosiddette SAR riservate ai singoli Stati[8] e l'obbligo di cooperazione tra di essi. Infine va citata la Convenzione internazionale sul salvataggio firmata il 28 aprile 1989 ed entrata in vigore il 14 luglio 1996, che stabilisce il premio che va corrisposto agli autori dei salvataggi, esteso, sia pure in modo non soddisfacente, ai cosiddetti salvataggi ambientali.

Si ritiene comunemente che la norma racchiusa nel citato art. 98, primo comma, dell'UNCLOS riproduca una norma di natura consuetudinaria.[9]

Il sostanziale fallimento della SAR ha segnato tuttavia un significativo arretramento sul cammino della concretizzazione della norma consuetudinaria, che può dirsi sia stata disattesa da vari governi che hanno attuato con crescente intensità un vero e proprio boicottaggio, spingendosi addirittura a prevedere odiose sanzioni anche di carattere penale o amministrativo nei confronti di chi intenda procedere al

[7] Convenzione delle Nazioni Unite sul diritto del mare, 10 dicembre 1982, entrata in vigore il 16 novembre 1994, art. 98.

[8] Un caso emblematico è quello della cosiddetta zona SAR libica sulla quale vedi il contributo di Fulvio Vassallo Paleologo, in questo Volume.

[9] I. Papanicolopu, *The duty to rescue in sea*, cit. *supra* nota 2, p. 494.

salvataggio di imbarcazioni in difficoltà, se cariche di migranti o richiedenti asilo. Tale sfregio intollerabile a principi di civiltà giuridica esistenti da tempo immemorabile è stato consumato nel contesto dell'accennata campagna politica contro le migrazioni, intrapresa da formazioni di stampo apertamente razzista ma di fatto avallata anche da numerosi governi e, al di là dell'inevitabile ipocrisia, dalla stessa Unione europea.

L'"obbligo giuridico di venire in aiuto dei migranti in mare" è stato bensì affermato dal Parlamento europeo nella sua risoluzione del 23 ottobre 2013. Non può peraltro davvero affermarsi che a tale astratta enunciazione corrisponda un concreto impegno volto a praticare il salvataggio. Anzi, può dirsi che l'Unione europea si sia sforzata sempre più a vanificare gli sforzi che taluni Stati membri, come l'Italia mediante il programma *Mare Nostrum*, avevano tentato di mettere in campo per salvare le vite umane a rischio nel Mediterraneo. Con una certa ipocrisia, a tale smobilitazione degli strumenti necessari a soccorrere le persone, è corrisposto piuttosto un impegno dichiarato a impedire che le stesse si mettano in viaggio per raggiungere l'Europa. L'evidente ipocrisia del discorso in questione consiste nel fatto che, per sradicare effettivamente alla base le partenze dei migranti e richiedenti asilo, occorrerebbe una vera e propria rivoluzione nei rapporti tra i loro Paesi d'origine e quelli più ricchi, che non risulta in nessun modo all'ordine del giorno. Anzi, proprio le recenti disgraziate vicende della pandemia mostrano come i Paesi ricchi, e fra essi in prima fila quelli europei, siano fermamente arroccati a difesa dei propri privilegi e soprattutto di quelli delle aziende multinazionali che ad essi fanno capo. Il diritto di queste ultime, se operanti nel settore chimico-farmaceutico, ad avvalersi dei privilegi di privativa industriale, sotto forma di brevetti od altro, viene agitato senza pietà a scapito di quello della grande maggioranza dell'umanità di difendersi dal virus mediante i vaccini. Prosegue d'altronde lo sfruttamento selvaggio delle risorse da parte delle imprese multinazionali che hanno i loro quartieri generali nei Paesi più ricchi, che producono devastazione ambientale e miseria economica, alimentando la fuga dei popoli verso lidi dove sperano di conseguire quantomeno la sopravvivenza, se non addirittura una vita migliore.

Vero è tuttavia anche che l'esito finale della rilevata ipocrisia consiste nel rendere del tutto inefficace anche la proclamazione astratta del rilevato obbligo di salvataggio, come dimostrato dal perdurare delle morti in mare fino a periodi recentissimi.

Ci troviamo quindi, chiacchiere a parte, a un evidente caso di violazione di una norma fondamentale, quella appunto relativa all'obbligo degli Stati e degli individui di soccorrere chi si trovi in condizioni di pericolo in mare aperto.

Giova peraltro rilevare come l'accennata smania di impedire a tutti i costi l'arrivo di migranti e richiedenti asilo sulle coste europee non si sia tradotta solo nella negazione dei soccorsi a persone in pericolo di vita, ma abbia assunto addirittura le sembianze dell'aggressione volta a provocare veri e propri naufragi. Un caso tristemente famoso è quello costituito dallo speronamento della nave albanese *Kater i Rades* da parte della corvetta Sibilla della Marina Militare italiana il 28 marzo, venerdì santo del 1997, all'epoca del governo di centrosinistra presieduto da Romano

Prodi. L'infame attacco provocò almeno 81 vittime tra le quali molti bambini. Pochi giorni dopo, il 1° aprile 1997, il ministro della difesa Andreatta dichiarava quanto segue dinanzi alle Commissioni Esteri e Difesa del Senato in seduta congiunta: "Le unità del nostro dispositivo hanno ricevuto direttive di adottare regole di pattugliamento volte a dissuadere il naviglio clandestino dal raggiungere il nostro Paese. (…) Le norme di comportamento prevedevano anche la possibilità, da parte delle nostre unità di manovrare in modo da scoraggiare il proseguimento della navigazione dei natanti verso le coste italiane".[10]

Più di recente lo stesso intento omicida, che si sostanzia per quanto detto in una flagrante violazione di norme consuetudinarie e forse anche, per quanto scriveremo tra poco, di *jus cogens*, ha assunto varie altre forme, dalla sostituzione di una missione come *Mare nostrum* con altre molto meno efficaci, alla costante opera di delegittimazione e screditamento delle organizzazioni non governative che si prefiggono di salvare le vite umane in mare, operando peraltro in sostituzione degli Stati inadempienti, per giungere addirittura, col famigerato ex ministro degli interni Salvini, a negare l'approdo a una nave che faceva parte della Guardia costiera.

4. Norma di *jus cogens*?

Al fine di qualificare ulteriormente il discorso di stampo giuridico svolto sulla norma relativa all'obbligo di salvataggio, occorre ora vagliarne la natura, verificando, in particolare se si tratti o meno di una norma di *jus cogens*.

Quella dello *jus cogens* è una categoria, per molti versi nuova o relativamente tale, di norme di diritto internazionale, la cui importanza indiscutibile è pari all'incertezza del loro contenuto.[11] La fonte normativa che si riferisce allo *jus cogens* in quanto tale è infatti com'è noto costituita dall'art. 53 della Convenzione di Vienna sul diritto dei trattati che si limita ad affermare, in modo del tutto tautologico che "a peremptory norm of general international law is a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character."[12]

Nessuna ulteriore specificazione viene in tal modo data riguardo al concreto contenuto delle norme di *jus cogens*. Il relativo compito viene pertanto delegato alla comunità internazionale degli Stati menzionata nella norma. Con molta e comprensibile cautela la Commissione di diritto internazionale delle Nazioni Unite si sta incamminando, per certi versi faticosamente, a definire meglio il concetto a partire dagli aspetti di ordine metodologico, da un'analisi dell'evoluzione storica del con-

[10] Citato da D. Gallo, "Non è un atto politico ma un crimine internazionale", I*l Manifesto,* 9 marzo 2021.

[11] Per un'introduzione all'argomento cfr. C. Tomuschat, J.-M. Thouvenin (eds.), The Fundamental Rules of International Legal Order, M. Nijhoff Publishers, 2006.

[12] Convenzione di Vienna sul diritto dei trattati, 23 maggio 1969, entrata in vigore il 27 gennaio 1980, art. 53.

cetto e dall'accertamento di alcuni aspetti fondamentali dello stesso dal punto di vista giuridico.[13] Il lavoro compiuto è ancora per molti versi allo stato embrionale. Esso comincia tuttavia ad esprimere dei contenuti interessanti e rilevanti per una ricerca più approfondita e concreta, specie laddove la Commissione afferma che "the values which are protected by jus cogens norms — those that constitute 'the fundamental values of the international law community' — are those that have been said to be 'toutes d'essence civilisatrice'. They are concerned with the basic considerations of humanity" e aggiunge come esempio calzante quello delle disposizioni della Convenzione per la prevenzione e repressione del crimine di genocidio, nell'interpretazione data dalla Corte internazionale di giustizia la quale nel parere dedicato a tale Convenzione ha sostenuto che "the Convention was manifestly adopted for a purely humanitarian and civilizing purpose … to safeguard the very existence of certain human groups and … to confirm and endorse the most elementary principles of morality."[14]

Ciò scritto però la Commissione si affretta a precisare che "While these are core characteristics, as opposed to requirements, of jus cogens, they do not tell us how jus cogens norms are to be identified in contemporary international law", rinviando la più puntuale definizione delle stesse a un futuro rapporto.

In attesa di tale rapporto può essere utile, o quantomeno dilettevole, dedicarsi alla relativa ricerca, con particolare riferimento a una situazione concreta, quale per l'appunto quella qui identificata della salvaguardia della vita umana in mare e dell'obbligo di soccorso che a tale salvaguardia è finalizzato. Bisogna in questo senso analizzare la prassi internazionale per ricavare le norme che possano aspirare a possedere tale carattere, identificando in particolare i valori supremi cui tale comunità intende ispirarsi.

Per giungere al relativo accertamento si possono percorrere, a ben vedere, cammini diversi, destinati peraltro ad intrecciarsi fra loro proprio nel momento della definizione della norma a partire dall'interesse essenziale da essa tutelato.

Il primo di tali sentieri punta sul diritto alla vita, che fra i diritti umani risulta per ovvi motivi il principale e il più irrinunciabile, data l'elementare considerazione che i cadaveri non possono in quanto tali godere di alcun diritto, se non quello al rispetto della loro memoria e della loro dignità di cose inanimate ma un tempo pertinenti a persone vive.

L'affermazione del diritto alla vita nasce com'è noto per reazione ai massacri e stermini di massa avvenuti nel corso del Ventesimo secolo, in particolare nella prima metà di esso ma purtroppo non cessati neanche in seguito, come dimostrato dai vari genocidi avvenuti in Bosnia, in Ruanda ed altrove. Si tratta di un diritto riconosciuto, senza condizioni, ad ogni essere umano. Del tutto categorica risulta quindi la formulazione dell'art. 3 della Dichiarazione universale dei diritti umani la quale

[13] Vedi Chapter V: Peremptory Norms of General International Law *(jus cogens)*, Report of the International Law Commission: Seventy-first session, 29 aprile, 7 giugno e 8 luglio, 9 agosto 2019.

[14] International Court of Justice, *Reservations to the Convention on the Prevention and Punishment of the Crime of Genocide*. Advisory Opinjon, of May 28th, 1951, p. 12.

unisce significativamente la proclamazione del diritto alla vita a quella della libertà e sicurezza della persona, affermando che: "Everyone has the right to life, liberty and security of person". D'altra parte l'Articolo 6(1) del nel Patto internazionale sui diritti civili e politici afferma che "Every human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life". I restanti paragrafi dell'articolo in questione sono dedicati alla pena di morte, assunta a suo tempo come unica ammissibile eccezione al godimento del diritto alla vita, e tuttora purtroppo praticata da numerosi Stati, tra i quali alcuni dei più importanti.

Il riferimento storico ai massacri e stermini di massa può in realtà estendersi anche alle decine di migliaia di morti per annegamento avvenute nel Mediterraneo o altrove in conseguenza dei movimenti migratori che si sono registrati negli ultimi decenni e dell'omissione di misure di soccorso volte a tutelare la vita dei migranti in tali perigliosi frangenti ovvero, come accennato, degli impedimenti dolosamente frapposti all'opera di quanti tentino invece di portare soccorso.

Il secondo possibile sentiero volto a valorizzare la potenziale natura di *jus cogens* delle norme a salvaguardia della vita umana in mare, nasce invece dal carattere solidale dell'obbligo di salvataggio, che trova vari riscontri, come accennato, in numerosi ordinamenti, soprattutto di *civil law*, *sub specie* del più generale obbligo di soccorso alle persone in difficoltà, ma viene particolarmente esaltato in situazioni naturalmente "ostili" come quelle dell'alto mare. La relativa prassi consuetudinaria è d'altronde riscontrabile da secoli nel comportamento sociale concretamente osservato non solo dagli Stati ma anche e soprattutto dalla gente di mare.

Anche in questo caso la natura di *jus cogens* della norma consuetudinaria ipotizzata deriva dal valore alla cui salvaguardia essa è finalizzata, che è anche qui la vita umana, non più solo in termini generici, come nel testo della Dichiarazione e del Patto menzionati, ma specificamente riferiti al contesto marino. Ci troviamo insomma di fronte a un combinato disposto di valore fortemente vincolante.

Ulteriore saldezza acquista questa costruzione normativa volta a conferire valore di *jus cogens* alle norme relative all'obbligo di salvataggio in contesto marino se si tiene in considerazione l'altro aspetto del problema sul quale ci siamo soffermati poco fa, e cioè il diritto a migrare. A maggior ragione, quindi, il diritto alla vita delle persone che si trovano in difficoltà e in pericolo mentre attraversano il mare va garantito, qualora si tratti di persone che esercitano il loro diritto a migrare, riconosciuto, nei limiti e colle forme ricordate, dal diritto internazionale.

Peraltro non si può sottacere come, per effetto della perversa volontà di taluni Stati e di organizzazioni internazionali come l'Unione europea di scoraggiare l'effettuazione dei movimenti migratori negando la possibilità di dare soccorso alle persone che si trovano in condizione in pericolo, sia proprio la condizione dei migranti e dei richiedenti asilo ad aumentare il pericolo stesso. Ciò conferma la natura antigiuridica delle politiche in questione.

Inutile aggiungere che tale antigiuridicità raggiunge livelli davvero intollerabili qualora all'omissione del compito, che incombe come abbiamo visto sugli Stati, di provvedere idonei mezzi di salvataggio ai migranti e richiedenti asilo che si trovino in pericoli durante la traversata del mare, si aggiunga l'intento di perseguitare le orga-

nizzazioni non governative che si dedicano con mezzi propri al relativo compito, supplendo in tal modo alle manchevolezze delle organizzazioni pubbliche e provvedendo a realizzare fondamentali previsioni normative che hanno per fine la salvaguardia della vita umana, valore giuridico e politico fondamentale per ogni ordinamento civile.

5. Possibili conseguenze della natura di *jus cogens* dell'obbligo di salvataggio

L'accertamento della natura di *jus cogens* dell'obbligo di salvataggio potrebbe portare con sé varie conseguenze. In primo luogo la nullità degli accordi coi quali due o più Stati mirino a impedirne o renderne più difficile l'adempimento, ovvero che contribuiscano al conseguimento di tale risultato anche indipendentemente da una volontà espressa e tacita degli Stati contraenti. Andrebbero pertanto attentamente valutati da tale punto di vista gli accordi, anche di natura meramente informale o solamente politica, raggiunti dagli Stati europei fra di loro o con Stati terzi, ad esempio la Libia, la Turchia od altri Stati delle sponde Sud ed Est del Mediterraneo.

In secondo luogo, tale natura di diritto cogente potrebbe avere effetti anche in ordine alla caratterizzazione di comportamenti che violino l'obbligo in questione, determinando il venire in essere di gravi violazioni dei diritti umani. Una prospettazione di tali comportamenti in termini di crimini contro l'umanità è stata effettuata dagli avvocati che sono ricorsi alla Corte penale internazionale un paio di anni fa e che hanno sottolineato fra l'altro come proprio l'accennata abolizione del programma *Mare Nostrum* abbia determinato un elevato innalzamento del numero di vittime che si sono registrate nel Mare Mediterraneo.[15] Specifici riferimenti alla giustizia penale internazionale sono d'altronde presenti nei Rapporti redatti per conto delle Nazioni Unite da Agnes Callamard, *Special Rapporteur* per le esecuzioni extragiudiziali, sommarie ed arbitrarie[16] e, in termini ancora più precisi e pertinenti dal Relatore speciale sulla tortura Nils Melzer, secondo il quale.

> States and the prosecutor from the International Criminal Court should examine whether investigations into crimes against humanity or war crimes are warranted in view of the scale, gravity and increasingly systematic nature of torture, ill-treatment and other serious human rights violations suffered by millions of migrants in all regions of the world as a consequence of corruption and crime, but also as a direct or indirect consequence of deliberate State policies and practices of deterrence, criminalization, arrival prevention, and refoulement.[17]

---

[15] Vedi "ICC Submission Calls for Prosecution of EU over Migrant Deaths", *The Guardian*, <https://www.theguardian.com/law/2019/jun/03/icc-submission-calls-for-prosecution-of-eu-over-migrant-deaths>.

[16] A/72/335 al punto 90: "The International Criminal Court should consider preliminary investigation into atrocity crimes against refugees and migrants where there are reasonable grounds that such crimes have taken place and the jurisdictional requirements of the Court have been met".

[17] A/HRC/37/50, al punto 80.

Una puntuale analisi dell'applicabilità delle norme dello Statuto della Corte penale internazionale e in particolare del suo art. 5 relativo ai crimini contro l'umanità esula dai limiti e propositi di questo scritto. È tuttavia intuibile come la natura di *jus cogens* delle normative che impongono l'obbligo di soccorso, che qui abbiamo sostenuto, non sia priva di conseguenze anche su questi aspetti, dato proprio il fatto che, assumendo come valida tale ipotesi, le norme in questione proteggerebbero valori fondamentali della comunità internazionale.

TOWARDS SUBJECTIVITY? THE CIVIL RESCUE FLEET AND ITS HUMANITARIAN AGENCY IN THE MEDITERRANEAN

Nassim Madjidian

1. Introduction

Maritime migration is not a new phenomenon. It has been a frequent occurrence in the history of humankind: Colonial settlers, Jews and political dissidents fleeing from Nazi Germany by boat, or the exodus of the so-called "Boat People" leaving Vietnam, are only a few historical instances of migration by sea.[1] In the aftermath of the Arab uprisings, migration across the Mediterranean has increased. The International Organization on Migration (IOM) estimates that since the beginning of 2014, at least 20,000 migrants have died[2] trying to reach European shores.[3] Although the Mediterranean has become one of the deadliest borders worldwide, European States are not actively engaged in systematic State-led rescue missions anymore. Italy was involved in systematic rescue operations in the past, but its naval operation "Mare Nostrum" ceased in October 2014. The EU military operation EUNAVFOR MED (Operation SOPHIA) ended *de facto* in 2019 after having resulted in the rescue of more than 49,000 migrants in distress.[4] The subsequent military operation "IRINI" does not continue the rescue mission of the preceding operation SOPHIA. Its naval vessels are placed expressly off the maritime routes of the Central Mediterranean.[5] Of the EU coastal States, Spain is conducting regular Search and Rescue (SAR) operations in its Search and Rescue Region (SRR) covering the Western Mediterranean route, which links the Canary Islands and Western African States.[6]

---

[1] E. Lindner, *Flucht übers Meer: von Troja bis Lampedusa/Flight Across the Sea*, E. S. Mittler & Sohn, Hamburg, 2019.

[2] Data on deaths during migration is highly incomplete, see K. Dearden et al., *Calculating 'Death Rates' In The Context Of Migration Journeys: Focus on the Central Mediterranean* (report Briefing series of IOM's Global Migration Data Analysis Centre), 2020, pp. 4-5, <https://gmdac.iom.int/calculating-death-rates-context-migration-journeys-focus-central-mediterranean> (06/21).

[3] Including the Eastern, the Central and the Western Mediterranean route, *Missing Migrants Project*, <https://missingmigrants.iom.int/> (06/21).

[4] *DW (Deutsche Welle)*, 23 January 2019, *Germany pulls out of Mediterranean migrant mission Sophia*, <https://www.dw.com/en/germany-pulls-out-of-mediterranean-migrant-mission-sophia/a-47189097> (06/21).

[5] M. Laux, "The evolution of the EU's naval operations in the Central Mediterranean: A gradual shift away from search and rescue", Report, *Heinrich Böll Stiftung Washington DC*, 16 April 2021, <https://us.boell.org/en/2021/04/16/evolution-eus-naval-operations-central-mediterranean-gradual-shift-away-search-and> (06/21).

[6] The Spanish "Sociedad de Salvamento y Seguridad Marítima" (SASEMAR or Salvamento Marítimo) is an example for (non-military) SAR operations led by a rescue organization that operates un-

Given the suspension of systematic State-led rescue missions on the Central Mediterranean route, which links North African States with Malta and Italy, the engagement of non-governmental Search and Rescue organizations (SAR NGOs) has become more significant. The presence of NGO vessels is often decisive for whether or not migrants are able to reach European shores and consequently, whether their right to life is upheld. Despite their limited rescue capacity, SAR NGOs are building a civil rescue fleet. This paper argues that the civil fleet has become an important humanitarian actor in the maritime space. Therefore, examining their concrete legal status under international law can contribute to the existing legal scholarship on non-State actors within the international legal system.

The article focuses on SAR operations conducted by NGOs and consists of two main parts. First, the article introduces the NGOs that have been present in the Mediterranean from 2014 until Spring 2021 (Section 2.1), arguing that a new type of humanitarian actor has emerged. Section 2.2 briefly describes how rescue operations are typically conducted. Section 3 frames NGO-led rescue operations as collective humanitarian agency under international law. It argues that rescue operations are capacitated and legitimatized, and thus *enabled* by several legal safeguards of the law of the sea, refugee law, and human rights law (Section 3.1). Section 3.2 offers a synthesized reading of the conceptualization as civil rescue fleet and the consequences of this concept when thinking about the legal status of SAR NGOs. The paper concludes that an open-ended and informal process of "subjectification" has begun (Section 4).

2. NGO-led Search and Rescue Operations in the Central Mediterranean

SAR NGOs have increased in number and rescue capacity within the last years. Most NGO vessels operate on the Central Mediterranean route. Today, these NGOs have become permanent actors in the Mediterranean even though State restrictions, including criminal proceedings and vessel detentions, prevent them from operating daily.[7] The following section conceptualizes SAR NGOs as a "civil rescue fleet". The fleet represents a new category of humanitarian actor that is worth studying, in particular against the background of the broader theoretical context of "non-State actors in international law". Understanding the role and position of SAR NGOs within the international legal system can extend the general debate on non-State entities being engaged in the realm of international law.[8]

---

der the auspices of the Spanish authorities. It is organized as a public company ("Entidad pública empresarial"). In 2019, SASEMAR rescued 17.683 migrants in distress, *Inform Annual 2019*, p. 23, <http://www.salvamentomaritimo.es/statics/multimedia/documents/2020/11/05/Memoria_salvamento_2019_ind.pdf> (06/21).

[7] On State restrictions see V. Keller, N. Madjidian, F. Schöler, "Hypocritical and Illegitimate. Maritime Safety Law and its Latest Use to Outlaw Humanitarian Missions in the Mediterranean", Blogpost, *Verfassungsblog*, 9 June 2020, <https://verfassungsblog.de/hypocritical-and-illegitimate/> (06/21).

[8] On the notion of the term "non-State actors" see J. d'Aspremont, "Non-state Actors and the Formation of International Customary Law: Unlearning Some Common Tropes", in Sufyan Droubi, Jean

2.1. Towards a Civil Rescue Fleet

The first NGO conducting maritime rescue in the Mediterranean was the German-French Association "Cap Anamur/Deutsche Not-Ärzte" in 2004. The association did not operate on a regular basis, their 2004 operation was subject to year-long criminal proceedings in Italy.[9] The steady presence of SAR NGOs in the Mediterranean began only in 2014, starting with the NGO "Migrant Offshore Aid Station" (MOAS).[10] More civil society actors followed in 2015 operating on the Central and Eastern Mediterranean routes. The initiative "The righteous of the Mediterranean Sea" gives an account of 60 organizations and individuals that have been involved in rescue operations since 2015. The list includes 34 organizations which have operated their own vessels, boats or floating rescue platforms and floating hospitals.[11]

About 30 different rescue *assets* (rescue vessels, monitoring vessels, aircrafts) have been deployed in the Mediterranean between 2016 and December 2020 by the following civil society organizations: Humanitarian Maritime Rescue Association, Jugend Rettet, LifeBoat, Mare Liberum, Médecins Sans Frontières, Mediterranea Saving Humans, Mission Lifeline, MOAS, M.V. Louise Michel, ProActiva Open Arms, Refugee Rescue, RESQSHIP, Save the Children, Sea-Eye, Sea-Watch, SOS Méditerranée (in alphabetical order).[12]

These organizations are all Europe-based humanitarian organizations mainly or exclusively funded by donations, and organized as private associations. By April 2021, not all organizations were operating at sea anymore. They have either stopped completely or their vessels have been detained. Pandemic restrictions (e.g. quarantining of the crew or closure of ports)[13] have rendered private SAR efforts even more difficult. However, the increased number of private associations in combination with the withdrawal of State-led SAR-operations confirm the trend of the "non-governmentalisation of SAR" as it is aptly described by Bevilacqua.[14]

---

d'Aspremont (eds.), International *Organisations, Non-state Actors, and the Formation of Customary International Law*, Manchester University Press, Manchester, 2020, pp. 166-188.

[9] For a summary of the criminal proceedings see <https://sherloc.unodc.org/cld/case-law-doc/migrantsmugglingcrimetype/ita/2009/case_n._326704_r.g.n.r..html> (06/21).

[10] E. Cusumano, "Emptying the Sea with a Spoon? Non-governmental Providers of Migrants' Search and Rescue in the Mediterranean", *Marine Policy,* 2017, pp. 91-98 (p. 96).

[11] *The Righteous List*, <http://www.nobel-righteous-mediterraneansea.info/the-righteous-of-the-mediterranean-sea/> (06/21).

[12] European Fundamental Rights Agency, *Table 1 – NGO ships involved in SAR operations*, <https://fra.europa.eu/en/publication/2020/december-2020-update-ngo-ships-involved-search-and-rescue-mediterranean-and-legal#TabPubTable1-NGOshipsinvolvedinSARoperations1> (06/21).

[13] A. Miron, "Port Denials and Restrictions in Times of Pandemic: Did International Law Lose its North Star?", Blogpost, *EJIL:Talk!*, 22 April 2020, <https://www.ejiltalk.org/port-denials-and-restrictions-in-times-of-pandemic-did-international-law-lose-its-north/> (06/21).

[14] G. Bevilacqua, "Italy Versus NGOS: The Controversial Interpretation and Implementation of Search and Rescue Obligations in the Context of Migration at Sea", *The Italian Yearbook of International Law Online,* 2019, pp. 11-27, p. 15.

NGO vessels regularly fly the flags of EU member States.[15] Consequently, the vessels need to comply with the legal requirements laid down in the flag State's domestic law. However, most of these domestic provisions stem from international environmental or ship safety law implemented by the flag State.[16] NGOs exchange information as well as staff and equipment.[17] Thus, the knowledge of the personnel, the equipment, and the technical standards of the vessels are widely comparable (although not identical).

Against this background, SAR NGOs can be understood as a "civil fleet". The term "civil fleet" is already used by some NGO activists who want to emphasize the solidarity among the NGOs and their commonalities.[18] In shipping vocabulary, a fleet is a (coordinated) formation of vessels generally assigned to a particular ocean or sea, commonly in the context of naval or commercial shipping. Despite the lack of operations under unified control, SAR NGOs are united in their purpose of saving lives at sea. The group of SAR NGOs consists of several civil society organizations, all based in Europe, that use vessels to prevent migrants from drowning and consequently dying in the maritime space. The vessels thus form a fleet, which is operated and managed by human rights activists belonging to different organizations. Despite the organizations having their own resources and purchase their own vessels, there is a strong link between all the SAR NGOs engaged in the Mediterranean. The purpose of their missions is the same. Their operational models are widely comparable, as the next section will show. And ultimately, the rescue operations conducted by NGOs present a clear contrast to "conventional" shipping activities and purposes – indicating that a new type of non-State humanitarian actor has emerged in the context of maritime migration.

2.2. The Fleet's Life-Saving Procedures

One of the reasons to argue that, together, SAR NGOs form a "civil rescue fleet" is the emergence of a common rescue pattern within the last years. As a consequence, all SAR NGOs involved apply similar and comparable standards for rescue situations on the high seas of the Mediterranean. This section details the typical course of a rescue operation. For this purpose, I will draw on interviews I have conducted with current and former SAR NGO staff.[19]

One has to acknowledge that each rescue operation is unique. Still, since SAR

[15] The vessels of the NGOs, e.g., Sea-Watch and Sea-Eye currently fly the German flag, the Ocean Viking belonging to SOS Méditerranée flies the Norwegian flag. Aita Mari, belonging to the Spanish NGO Salvamento Marítimo Humanitario, flies the Spanish flag.

[16] E.g. the International Convention for the Prevention of Pollution from Ships (MARPOL), 17 February 1973, modified by the Protocol of 1978, entered into force 2 October 1983 or International Convention for the Safety of Life at Sea (SOLAS), 1 November 1974, entered into force 25 May 1980.

[17] E. Cusumano, "United to rescue? Humanitarian role conceptions and NGO-NGO interactions in the Mediterranean Sea", *European Security*, 2021, pp. 1-22 (pp. 6-7).

[18] In Germany, a private German association is called "Civilfleet-Support".

[19] I have conducted ten semi-structured interviews in 2021 with NGO members having assisted in rescue missions of four different NGOs.

NGOs began their operations in late 2014, a certain procedure and rescue pattern has been developed. Although each NGO follows its own Standards of Procedure (SOPs), the rescue pattern introduced below is widely comparable.

A typical rescue operation is conducted in the following way: the vessel leaves the (often Italian) port and heads towards the Central Mediterranean route. NGO vessels generally do not enter Libyan territorial waters.[20] The rescue operations typically take place on the high seas within the Libyan, the Maltese, or the Italian SRR. In the early years of rescue operations, the Maritime Rescue Coordination Centres (MRCCs) were often indicating coordinates to NGO vessels. By now, NGO vessels generally do not receive coordinates of distress cases by authorities such as coast guards, MRCCs or Frontex surveillance assets. Rather, NGO vessels spot unseaworthy vessels on their own, in cooperation with aircrafts operated by volunteers, or are made aware of coordinates of boats in distress shared by the NGO Alarm Phone.[21] In some cases, commercial vessels might share coordinates via radio with MRCCs and NGO vessels nearby.

SAR NGOs generally prepare their volunteers and crew members through training and with the help of SOPs.[22] The crew members assigned to the rescue operation generally approach migrants' boats on rigid-hulled inflatable boats (RHIBs). The crew members manoeuvering the RHIBs have to prevent people from panicking or jumping into the water. If possible, life-vests are distributed before the crew members help the rescuees embark safely on the main vessel.

Once the rescuees have been taken on board the vessel, first aid is provided by medical personnel. Many rescuees suffer from chemical burns caused by fuel, salt water, and/or urine. Pregnant women require special medical attention. Often, rescuees suffer from dehydration or undernourishment. The master of the vessel, assisted by the head of mission, typically initiates communication with the MRCC in whose SRR the vessel is situated as soon as the vessel has reached the SRR. When rescue is about to happen, SAR NGO vessels declare themselves as "on-scene coordinators" in case no other vessel has taken this responsibility, typically by communication via email with the MRCC in whose region the rescue is taken place. According to the SOLAS[23] and to the SAR Convention[24], MRCCs must swiftly assign

[20] NGO vessels generally neither search nor rescue within Libyan territorial waters although the law of the sea grants the right of innocent passage through the territorial sea (Art. 17 UNCLOS) which, according to Art. 18(2) UNCLOS, includes 'rendering assistance' within the definition of innocent passage. See D. Guilfoyle, "Art. 98 UNCLOS", in Alexander Proelß et al. (eds.), *United Nations Convention on the Law of the Sea: a commentary*, C.H. Beck/Hart/Nomos, Munich, Oxford and Baden-Baden, 2017, para. 3.

[21] The organization Alarm Phone provides a telephone which migrants can reach when they are at sea. Alarm Phone shares the GPS and more information with European MRCCs and on social media. See for instance the tweet of 7 April 2021, *Alarm Phone on twitter*, <https://twitter.com/alarm_phone/status/1379900450879770626?s=20>. <https://alarmphone.org/en/faq_en/> (06/21).

[22] Standards of Procedures of two different SAR NGOs are on file with the author.

[23] International Convention for the Safety of Life at Sea (SOLAS Convention), 1 November 1974, entered into force 25 May 1980 (SOLAS), Ch. V, Reg.33(1-1).

a "place of safety" where the rescuees can disembark. [25] During the past years, Malta and Italy have often refrained from assigning a "place of safety" immediately, leading to long standoffs (up to 38 days in the case of migrants on board a Danish tanker in 2020).[26] In contrast to the clear rule that disembarkation has to take place as soon as possible, a so-called ship-to-ship approach has emerged, by which European member States negotiate a relocation quota for the persons rescued before disembarkation is allowed.[27]

In general, two distinct operational models of rescue operations can be distinguished: Either SAR NGOs perform "fully-fledged" SAR operations with large vessels that can take migrants on board and disembark them at a "place of safety", or SAR NGOs refrain from taking migrants on board and only provide life-saving appliances.[28] The operational model of SAR NGOs is determined by the size and the rescue capacities of the vessel. NGOs equipped with smaller vessels or mere monitoring NGOs generally act as "first responders" that only provide first aid, whereas larger vessels may then take the rescuees on board.

3. Collective Humanitarian Agency and International Law

SAR NGOs operate within a legal framework which consists of public international law (hard and soft law), European law, and domestic law.[29] Section 3.1 explicates why SAR operations take place on the intersection of different international legal regimes – concluding that NGO-led SAR operations are capacitated and legitimatized, and thus *enabled* by several legal safeguards of the law of the sea, refugee law, and human rights law. Section 3.2 intends to synthesize these findings together with the conceptualization of SAR NGOs as a civil rescue fleet – asking whether SAR NGOs can reach or have reached a particular legal status under international law.

---

[24] International Convention on Maritime Search and Rescue (SAR Convention), 27 April 1979, entered into force 22 June 1985, Annex, Reg. 3.1.9.

[25] Malta has not ratified these provisions introduced by amendments in 2004, see A. Farahat and N. Markard, *Places of Safety in the Mediterranean: The EU's Policy of Outsourcing Responsibility*, Report of the Heinrich-Böll-Stiftung Brussels European Union, Brussels, 2020, (p. 16).

[26] L. Tondo, "Migrants land in Sicily after 'longest standoff in European maritime history'", *The Guardian*, 13 September 2020, <https://www.theguardian.com/world/2020/sep/13/migrants-land-in-sicily-after-longest-standoff-in-european-maritime-history> (06/21).

[27] L. Rasche, "Far from a fresh start on migration: What to make of the solidarity mechanism for the Mediterranean", *Policy Brief of the Jacques Delors Institute Berlin*, online publication, 15 October 2019, <https://www.delorscentre.eu/de/publikationen/detail/publication/der-malta-mechanismus-neustart-fuer-die-eu-migrationspolitik> (06/21).

[28] Cusumano, "Emptying the Sea with a Spoon?", *cit. supra* note 10, p. 96.

[29] At the international level, the law of the sea, human rights law, and refugee law have to be considered. At the European level, immigration and asylum policies belong to the policy field related to the "Area of Freedom, Security, and Justice", (see Title V of the Treaty on the Functioning of the European Union, Arts. 67 to 89). Regarding the domestic level, one has to consider that international and European law has typically been adopted by national legislations. Also, the admission of NGO vessels by the flag State is subject to domestic provisions and procedures.

3.1. International Law's Receptiveness towards NGO-led SAR Operations

Understanding the role and the position of SAR NGOs in the international realm requires considering the legal framework they operate in. From a legal point of view, it is important to acknowledge that NGO-led SAR operations are highly regulated by different legal levels and issue areas, whose legal provisions form, when put and read together, the legal framework for NGO-led rescue operations. This section argues that SAR NGOs can trigger the application of (at least) three different issue areas of public international law, namely the law of the sea, human rights law, and refugee law. It is beyond the scope of this paper to offer an in-depth doctrinal analysis of the legal framework applicable. Rather, this section intends to highlight that different issue areas of international law allow, protect, and thus *enable* NGO-led SAR operations. Against this background, I argue that SAR NGOs can draw upon the receptiveness of international law towards their actions. Consequently, SAR NGO rescue operations profit from international law's inherent claim to legitimacy.[30]

In the following paragraphs, I will briefly unpack this idea of receptiveness and legitimacy by giving examples of legal provisions stemming from the issue areas of the law of the sea, human rights law, and refugee law that enable SAR operations.

The most significant legal provision in relation to rescue operations is the duty to render assistance at sea.[31] This duty is established under treaty law[32] but also acknowledged as being customary international law.[33] Art. 98(1) UNCLOS[34] is often depicted as the "key" obligation stemming from the law of the sea which addresses States party to the UNCLOS:

> Every State shall require the master of a ship flying its flag, in so far as he can do so without serious danger to the ship, the crew or the passengers: (a) to render assistance to any person found at sea in danger of being lost; (b) to proceed with all possible speed to the rescue of persons in distress, if informed of their need of assistance, in so far as such action may reasonably be expected of him (…).

The UNCLOS provision addresses the State, which, in turn, has to provide for

---

[30] On international law's inherent claim to legitimacy see S. Besson, "The Authority of International Law – Lifting the State Veil", *Sydney Law Review*, 2009, pp. 343-380 (p. 345).

[31] See in particular F. Attard, *The duty of the shipmaster to render assistance at sea under international law*, Brill Nijhoff, Leiden/Boston, 2020; I. Papanicolopulu, "The duty to rescue at sea, in peacetime and in war: A general overview", *International Review of the Red Cross*, 2016, pp. 491-514.

[32] See Art. 98(1) UNCLOS; SOLAS Convention, Ch. V/Reg. 33(1); SAR Convention Annex, Ch. 2, reg. 2.1.10 and 2.1.1; Art. 10(1) Salvage Convention (International Convention on Salvage, 28 April 1989, entered into force 14 July 1996).

[33] F. Attard, *The duty of the shipmaster, cit. supra* note 31, pp. 92-126; D. Guilfoyle, "Art. 98 UNCLOS", in Alexander Proelß et al. (eds.), *United Nations Convention on the Law of the Sea: a commentary*, München, 2017, paras. 1, 5.

[34] United Nations Convention on the Law of the Sea (UNCLOS), 10 December 1982, entered into force 16 November 1994.

the realization of this international legal duty to render assistance by means of domestic law. Thus, the master of the vessel is bound by the duty stemming from Art. 98(1) UNCLOS only via mediation through the flag State. In contrast to the UNCLOS provision, the SOLAS Convention[35] terminologically directly addresses the "master of a vessel" (Ch. V, Reg. 33)[36] – allowing for discussion on whether the convention is stipulating a directly binding provision for the master.[37] The different wording, therefore, establishes a margin of interpretation regarding the addressee (and thus the subject) of the provision.

In the Central Mediterranean, migrants in distress can generally be located within the Libyan SRR[38], the Maltese SRR, or the Italian SRR. According to the SAR Convention[39], the coastal State in whose SRR the assistance is rendered, shall exercise primary responsibility for ensuring that coordination of the rescue case and cooperation between States involved occur and, importantly, that survivors are disembarked from the assisting ship and delivered to a place of safety (see regulation 3.1.9). The wording of regulation 3.1.9 is of particular importance in many ways. It does not only require the disembarkation of persons rescued in a "place of safety"[40] but also acknowledges a primary responsibility of the coastal State in whose SRR the assistance has taken place. By the wording and the use of the term "primary responsibility", the SAR Convention assigns *secondary* responsibility to other, neighbouring coastal States to render assistance (*argumentum e contrario*). Importantly, parties to the SAR Convention must ensure that assistance is provided to *any* person in distress at sea (regulation 2.1.10). These legal requirements address the coastal State but SAR NGOs profit indirectly from these regulations as the SAR Convention confers the responsibility to coordinate the NGO-led rescue operation to the coastal State(s).

The legality of SAR operations conducted by NGO vessels in the high seas or in the exclusive economic zone of a coastal State as such is beyond doubt.[41] The law of the sea, primarily, requires States (and subsequently also masters) to prevent

---

[35] SOLAS Convention, *cit. supra* note 23.

[36] See i.a. SOLAS Convention Ch. V/Reg. 33(1): "The master of a ship at sea which is in a position to be able to provide assistance on receiving information from any source that persons are in distress at sea, is bound to proceed with all speed to their assistance (…)".

[37] See M. Ratcovich, *International Law and the Rescue of Refugees at Sea*, Stockholm University, Stockholm, 2019, pp. 88-89.

[38] The Libyan SRR was only established in December 2017. It was re-established in June 2018, see T. Calandrino, "Wie Libyen zum sicheren Hafen wurde. Die Zuweisung einer libyschen „Search and Rescue Zone" als europäisches Migrationsmanagement", *borderline-europe*, 2019, pp. 1-8, <https://www.borderline-europe.de/eigene-publikationen/wie-libyen-zum-sicheren-hafen-wurde-die-zuweisung-einer-libyschen-%E2%80%9Esearch-and> (6/21).

[39] International Convention on Maritime Search and Rescue (SAR), 27 April 1979, entered into force 22 June 1985.

[40] On 'Places of Safety', see in particular the contribution of A. Del Guercio to this volume and A. Farahat and N. Markard, "Places of Safety in the Mediterranean", *cit. supra* note 25.

[41] V. J. Schatz/M. Fantinato, "Post-rescue Innocent Passage by Non-governmental Search and Rescue Vessels in the Mediterranean", *The International Journal of Marine and Coastal Law*, 2020, pp. 740-771 (p. 744).

the loss of life at sea by establishing legal obligations, but also offers legal safeguards that enable SAR operations – allowing the question whether SAR NGOs are assigned with rights stemming directly from international law. A second provision of the law of the sea that enables private rescue operations, is the freedom of navigation as it is included in the list of the freedoms of the high seas (Arts. 87(1)(a) UNCLOS) and by means of own codification in Art. 90 UNCLOS (termed the "right of navigation). In a nutshell, the freedom of navigation includes "[t]he right to enter upon the oceans and to pass them unhindered by efforts of other States or entities (…)".[42] Every State has the right to sail ships flying its flag on the high seas. [43] In this sense, SAR NGOs have the right to sail by virtue of flying the flag of the respective flag State. Mediated by the flag State's right, they exercise the freedom of navigation when conducting search and rescue operations.

A second issue area of international law that enables private rescue operations is international human rights law. From a human rights perspective, the right to life of migrants facing death by drowning is probably the most important legal guarantee within the context of maritime migration.[44] However, as States are often absent, instances that might establish a jurisdictional link between a coastal State and a migrant facing death by drowning (as a trigger for the application of human rights obligations) are difficult to establish.[45] As States may not be (de jure) responsible for the violations of the human right to life, it is worth thinking about private rescue operations not only as humanitarian action but also as a legal practice that prevents the loss of life at sea. In this sense, SAR NGOs protect the right to life of migrants at sea. Thus, the protection of human rights takes place by a non-State entity. Two further assumptions can be drawn here. First, SAR NGOs have factually taken over responsibility for the protection of the right to life in extraterritorial maritime settings. And second, as SAR NGOs are closely linked to the (universal) human right to life, every restriction on SAR NGO operations, e.g., the seizures of vessels by the coastal or the flag State, can touch upon the scope of the human right to life, at least in an indirect way.

A different approach towards human rights law is put forward by Mann emphasizing the human rights of NGO crew members. He draws on the civil and political rights of the rescuers, in particular the freedom of expression and the rights to as-

---

[42] M. McDougal/ W. T. Burke, *The Public Order of the Oceans*, Yale University Press, New Haven, 1987, p. 763.

[43] D. Guilfoyle, "Art. 90 UNCLOS", in Alexander Proelß et al. (eds.), *United Nations Convention on the Law of the Sea: a commentary*, cit. *supra* note 20, para. 1.

[44] The Human Rights Committee acknowledges situations of distress within its Comment No. 36 on the right to life, Ibid, 3 September 2019, CCPR/C/CG//36, para. 63.

[45] The UN Human Rights Committee has rendered a "milestone" decision when qualifying the "non"/late reaction of Italy in a case of migrants' distress at sea as a breach of the human right to life, see N. Madjidian, "Mediterranean Responsibilities, Extra-territorial Jurisdiction of Coastal States in the Context of Maritime Migration", Blogpost, *Verfassungsblog*, 29 January 2021, <https://verfassungsblog.de/mediterranean-responsibilities/> (6/21); On the lacking of migrants' rights, see I. Mann, "Maritime Legal Black Holes: Migration and Rightlessness in International Law", *European Journal of International Law*, pp. 347–372.

sembly and association.[46] Mann argues that the State has the duty to respect and to protect its citizens' freedom of expression whether they act territorially or extraterritorially[47] – referring also to the ECtHR's case *Women on Waves v. Portugal*,[48] in which the court acknowledged the relevant association's right of expression (Art. 10 ECHR) and the freedom of assembly and association (Art. 11 ECHR) at sea.[49] When protected by civil human rights, one can claim that human rights law also provides safeguards for SAR operations in relation to crew members and thus also enables private rescue operations legally.

A third issue area of international law that needs to be considered in the case of SAR NGOs is refugee law and in particular the prohibition of refoulement.[50] This section cannot introduce the non-refoulement principle in depth.[51] Nevertheless, the argument here is to draw attention to the fact that SAR NGO vessels can fall within the scope of application of this provision, namely when coastal States violate the principle by pushing back or not allowing the entry of NGO vessels with refugees and asylum-seekers on board.

This brief overview has shown that SAR NGOs operate within a densely regulated legal field whose provisions stem from different issue areas of international law. The provisions introduced above, relate to the different subjects involved (the flag State, the coastal State, the NGOs, the shipmasters and crew members, the refugees and asylum-seekers). SAR NGOs have manoeuvered themselves into the scope of different international legal provisions that regulate but also enable rescue operations. As a result, rescue operations can draw both their legality and their legitimacy from different issue areas of international law. As rescue operations take place at the intersection of (at least) three different issue areas of international law, SAR NGOs profit from the receptiveness of distinct legal regimes.

---

[46] I. Mann, "The Right to Perform Rescue at Sea: Jurisprudence and Drowning", *German Law Journal*, 2020, pp. 598-619, p. 611.

[47] Ibid. 613.

[48] ECtHR, *Women on Waves and Others v. Portugal*, Application No. 31276/05, Judgment of 2 March 2009.

[49] I. Mann, "The Right to Perform Rescue at Sea", *cit. supra* note 47, p. 612.

[50] Art. 33(1) of the 1951 Refugee Conventions States that: "No Contracting State shall expel or return ('refouler') a refugee in any manner whatsoever to the frontiers of territories where his life or freedom would be threatened on account of his race, religion, nationality, membership of a particular social group or political opinion.", Convention Relating to the Status of Refugees, 28 July 1951, entered into force 22 April 1954.

[51] On non-refoulement, see the contribution of A. Del Guercio to this Volume and S. Trevisanut, "The Principle of Non-Refoulement at Sea and the Effectiveness of Asylum Protection", *Max Planck Yearbook of United Nations Law*, 2008(12), pp. 205-246; M. Giuffré, "Access to Asylum at Sea? Non-refoulement and a Comprehensive Approach to Extraterritorial Human Rights Obligations", in Violeta Moreno Lax and Efthymios Papastavridis, *"Boat refugees" and migrants at sea. A comprehensive approach: integrating maritime security with human rights*, Brill Nijhoff, Leiden, 2017; G. Goodwin-Gill, "The Right to Seek Asylum: Interception at Sea and the Principle of Non-Refoulement", *International Journal of Refugee Law*, 2011, pp. 443-457.

3.2. Humanitarian Agency Resulting in Legal Status

How does the conceptualization of SAR NGOs as a civil rescue fleet speak to the findings that SAR NGOs operate within a legal framework consisting of different (sub)fields of international law? And that this international legal framework is receptive towards NGO-led SAR operations by not only requiring but also enabling these non-State rescue missions?

From an international legal perspective, the conceptualization of SAR NGOs as a – more or less – uniform group of humanitarian actors whose rescue practices fall within the scope of legal provisions stemming inter alia from the international legal order raises the question of the legal status of these NGOs. SAR NGOs can be seen as "*de facto* international actors"[52] as they operate within an international migratory context. Still, acknowledging SAR NGOs as "*de facto* international actors" does not describe their concrete legal status sufficiently.

International legal doctrine offers only very limited tools for the understanding of non-State actors' agencies and their roles and positions within the international legal system. From a doctrinal legal perspective, the criterion of international legal personality is often used as the main analytical lens for the assessment of the legal status of non-State entities' participation in the international realm.[53] International legal personality is, in a nutshell, often understood as the fact that an entity is capable of possessing international rights and/or duties.[54] Still, legal theory has not agreed upon a uniform understanding and definition of international legal personality.[55] Despite these existing controversialities, one intellectual option to understand the agency of SAR NGOs can be the assessment of whether or not SAR NGOs are equipped with international legal personality by means of a doctrinal analysis of the rights and duties stemming from international law. Here, the duty to render assistance at sea, the freedom of navigation, and also human rights of NGO crew members can be discussed – bearing in mind that legal rights and duties might not be directly addressed towards SAR NGOs but mediated by State actors being parties to human rights or law of the sea conventions.

If one would assume that SAR NGOs (or the master or the crew of the NGO vessels) are directly addressed by international legal provisions (either by rights or by duties), and consequently affirm that they possess (partial) international legal personality, what would follow? Accepting that SAR NGOs enjoy partial international legal personality, leads to follow-up questions regarding their potentially existing capacity to conclude treaties, to be responsible for international unlawful acts,

---

[52] I. Rossi uses this term in: *Legal Status of Non-Governmental Organizations in International Law*, Intersentia, Antwerp. 2010, p. 51 (italics not added).

[53] See R. Ben-Ari, *The Normative Position of International Non-Governmental Organisations under International Law: An Analytical Framework*, Leiden 2010, pp. 7-10.

[54] C. Walter, "Subjects of International Law", *Max Planck Encyclopedia of Public International Law*, online publication, May 2007, para. 21.

[55] A. Peters, *Beyond Human Rights. The Legal Status of the Individual in International Law*, Cambridge University Press, Cambridge, 2016, pp. 35-41.

and ultimately, their official membership to the "club" of subjects of international law. Nevertheless, answering whether a non-State actor enjoys international legal personality would not explicate the concrete legal outcome or contribution stemming from the actor's agency. Against this background, the mere focus on international legal rights and duties appears to restrict a differentiated and further thinking on non-State actors' potential roles, positions, and agencies under or within international law.[56] Acknowledging that particular legal rights and duties are expressly addressed towards SAR NGOs can, therefore, be one (important) way of determining the legal status of SAR NGOs. In contrast, this section offers a distinct assessment of the legal status of SAR NGOs by drawing on two different aspects stemming from an empirical perspective: First, one can ask whether a legal status has been granted by other subjects of international law (States, IOs, the EU) by an implicit or explicit act of recognition.[57] And second, one can draw on the conceptualization offered here of SAR NGOs as a civil rescue fleet in a combined reading with the finding that the legal framework enables NGO-led SAR operations (sections 2.1 and 3.1).

Have States or other subjects of international law recognized SAR NGOs as legitimate actors of international law, and have they conferred any kind of legal status to SAR NGOs? SAR NGOs are typically registered as non-profit organizations under domestic law. However, one can ask whether a certain degree of international legal status has been acknowledged by subjects of international law either by implicit or explicit recognition. The European Commission has addressed rescue operations by NGOs explicitly in their 2020 recommendations on migration and asylum.[58] In this set of recommendations, the EU Commission calls for an intensified coordination of EU Member States by establishing a contact group and calling for exchange between the owners of the NGO vessels in order to identify procedures that allow to "increase security at sea" but also compliance with safety-related provisions (recommendation N° 2). The EU Commission indicates that "several non-governmental organizations (NGOs) have also been operating private vessels, mostly in the Central Mediterranean area, significantly contributing to the rescue of persons at sea, who are then brought to EU territory for safe disembarkation (…)".[59] Hence, one can argue that the EU Commission has already accepted the emergence of SAR NGOs as a phenomenon of interest that needs regulation.

Another example can be drawn from the reactions of coastal States such as Italy and Malta. Both States had declared their ports "unsafe" in 2020 during the first month of the Covid-19 pandemic leading to the initial closure of their ports for

[56] See the discussion summarized by I. Rossi, *Legal Status of Non-Governmental Organizations in International Law*, Intersentia, Antwerp. 2010, pp. 48-52.

[57] Ibid. 53.

[58] Commission Recommendation (EU) 2020/1365 of 23 September 2020 on "Cooperation among Member States Concerning Operations Carried out by Vessels Owned or Operated by Private Entities for the Purpose of Search and Rescue Activities", 1.10.2020, L 317/23.

[59] Ibid. at para. 5.

NGO vessels.[60] A further example can be drawn from the reactions of Italy towards SAR NGOs. In 2017, Italian authorities prepared a code of conduct for SAR NGOs consisting of 13 provisions agreeing on SAR procedures.[61]

These different examples show that State and supra-State actors acknowledge and react towards SAR NGOs. Their intentions to regulate or restrict NGO-led SAR operations go hand in hand with an implicit recognition of SAR NGOs' existence and agency.

A second empirical perspective stems from the observations of SAR NGO procedures as they were briefly depicted in section 2.1. SAR NGOs have managed to establish a "standard procedure" for conducting rescue operations. Their operational models have converged although slight differences remain. Consequently, NGOs have expanded their individual agency[62] towards a common, simultaneously existing, agency of all SAR NGOs. Expanding the standing and the agency of the single NGO towards a common agency of a group of SAR NGOs leads to an important conceptual difference. When addressing NGO-led SAR operations legally and politically, the focus shifts from the particular case to the general case, and ultimately, the particular rescue operation loses importance. What becomes more important is the more general conduct of rescue operations, or to put it differently: the more general picture of rescue operations led by civil society actors comes to the fore. In this sense, the formation of a civil rescue fleet has resulted in a collective and joint agency of SAR NGOs. Still, SAR NGOs do not speak with one voice, they are formally not organized as one actor but as several individual actors. Nevertheless, they have reached an informal group status due to the emergence of a "civil rescue fleet".

This empirical reading of NGO operations can help to understand and to identify the legal contributions, and ultimately, the legal status stemming from NGO rescue practices. As argued in section 3.1, SAR NGOs have prevented the death of thousands of people.[63] In addition, SAR NGOs perform rescue operations as they are prescribed by the law of the sea –for States and for the masters of vessels. They

---

[60] A. Pelliconi, "Covid-19: Italy is not a "place of safety" anymore. Is the decision to close Italian ports compliant with human rights obligations?", *EJIL:Talk!*, 23 April 2020, <https://www.ejiltalk.org/covid-19-italy-is-not-a-place-of-safety-anymore-is-the-decision-to-close-italian-ports-compliant-with-human-rights-obligations/> (06/21); Times of Malta, <https://timesofmalta.com/articles/view/malta-says-it-cannot-guarantee-migrant-rescues.784571> (06/21).

[61] For a detailed analysis, see E. Cusumano, "Straightjacketing migrant rescuers? The code of conduct on maritime NGOs", *Mediterranean Politics*, pp. 106-114.

[62] Agency is understood broadly here, in the sense of the "capacity to act". See the definition of Braun, Benjamin; Schindler, Sebastian; Wille, Tobias, "Rethinking agency in International Relations: performativity, performances and actor-networks", *Journal of International Relations and Development*, 2019, pp. 787–807 (p.788).

[63] Still, it is difficult to calculate as no exact numbers of persons rescued by NGOs exist. Also, one does not know whether persons rescued from unseaworthy vessels would have died without the intervention of the SAR NGO or whether they would have reached European shores autonomously or with the help of other actors such as coast guards or fishing vessels, etc.

can relate to the freedom of navigation and to the duty to render assistance at sea, and they can claim that coastal States have to assign a place of safety. In this sense, SAR NGOs relate to already existing legal provisions. Mégret understands NGO practices on the high seas (not limited to NGO rescue operations) as a way of "taking international law in one's own hands" and seeking to implement it from below.[64] In the case of SAR NGOs, it might not only be the implementation or the enforcement of laws (e.g., the duty to render assistance). Rather, SAR NGOs have contributed to the construction of a – still incomplete and incomprehensive – legal framework stemming from different issue areas of international law with the civil rescue fleet as the main actor involved.

To summarize, coastal States such as Italy or Malta, but also the EU Commission have already recognized the group of SAR NGOs as a group of actors on the international plane. In this sense, SAR NGOs have received leverage regarding their legal status by being recognized as a common group of actors. Due to their harmonized and standardized procedures, it is apt to understand SAR NGOs as a uniform humanitarian actor, consisting of various single NGOs. Their formal legal status might derive from the registration as a private association under domestic law and the doctrinal analysis of their international legal rights and duties. Their (still) informal legal status under international law, however, does not derive from the recognition by other subjects of international law. The recognition is rather an indicator of factually existing relevance and leverage. The legal status results ultimately from the interpretation of the actions undertaken by these NGOs and the contribution to the functioning of the international legal system. In this sense, SAR NGOs can be seen as non-State entities that protect human rights on the high seas due to their humanitarian mandate. They implement States' duties, such as the duty to render assistance, and contribute to the development of a – still incomplete and incomprehensive – legal framework emanating from different issue areas of international law, with the civil rescue fleet currently being the main actor involved.

4. Conclusion

Rescue at sea is an undisputed legal duty. However, in the context of maritime migration, it is heavily contested and delegitimized. This paper has sought to explicate that NGO-led rescue operations are required and regulated by international law. As argued in section 3.1, the applicable legal framework capacitates and legitimatizes, and thus also *enables* rescue operations by offering several legal safeguards of the law of the sea, refugee law, and human rights law.

Scholarly attention has already been paid to the legal framework of non-State rescue operations whereas the concrete legal status of SAR NGOs remains unexplored. This paper has therefore sought to offer a first assessment of the role, agen-

[64] F. Mégret, "Activists on the High Seas: Reinventing International Law from the Mare Liberum?" *International Community Law Review*, online publication, January 2021, pp.1-36.

cy, and ultimately of the legal status of SAR NGOs. A doctrinal perspective would have put its focus on the determination of legal rights and duties stemming directly from the international legal order. The paper, in contrast, has offered a broader assessment of the legal status of SAR NGOs by including aspects related to recognition and factual legal contributions stemming from such collective humanitarian agency. As a result, SAR NGOs must not only be regarded as "de facto" international actors. They have found their ways and strategies to become "de jure" international actors. Even if these NGOs might not have reached the threshold of international legal personality yet, an open-ended informal process of "subjectification" has been initiated.

HUMANITARIAN ENGAGEMENT IN MARITIME RESCUE AND MIGRANTS' RELOCATION

Sara Bellezza - Haidi Sadik

1. Introduction

The Central Mediterranean Sea constitutes a maritime space where border surveillance, merchant seafarers, people on the move to Europe and humanitarian actors encounter each other. Increased attempts of EU border enforcement have contributed to turning this space into a highly surveilled zone where an uncountable number of people continue to lose their lives. With the criminalization of civil Search and Rescue (SAR) NGOs, as well as fishermen and merchant vessels, the rescue of people at sea became a political issue not only at sea, but brought ashore with so-called EU ad hoc relocation agreements for disembarkation. In September 2019, five EU Member States (MS) decided on a common agreement for the distribution of people rescued from distress at sea to various EU countries. The so-called Malta agreement,[1] a temporary policy approach, was established in response to the Italian and Maltese refusal to let civil SAR boats arrive in their ports. Along with the increased criminalization of SAR operations in the Central Mediterranean Sea, the question of distribution of protection-seekers in the EU re-gained broader media attention during former Italian Minister of Interior Matteo Salvini's term of office, when the scandalization of SAR operations was actively pursued.

In a context of ever stronger attempts to deter migration and stop movement to and within the EU, in this paper we offer on-the-ground perspectives on the *modus operandi* of actors involved in the EU's border management. Mobilizing firsthand experience from a Sea-Watch mission in June 2019 and testimonies from people who survived one of the most dangerous routes to Europe, we aim to criticize the supposed 'humanitarian' practices of EU institutions. Namely Frontex, the European Border Guard Agency, the European Asylum and Support Office (EASO), as well as two German institutions that are relevant for an analysis of current relocation procedures: the German Domestic Intelligence service and the German Federal Office for Migration and Refugees (BAMF).

We will discuss two separate legal issues; Haidi Sadik will first deal with the freedom of humanitarian actors to operate in the Mediterranean. Additionally she looks at violations of international and maritime law and the human impact of 'closed port' policies through the lens of personal impressions from a particularly

[1] *Joint Declaration of Intent on a Controlled Emergency Procedure. Voluntary Commitments by Member States for Predictable Temporary Solidarity Mechanism*. La Valletta, Malta. 23 September 2019. <https://download.repubblica.it/pdf/2019/politica/joint-declaration.pdf> (11/2020).

poignant Sea-Watch 3 rescue led by Captain Carola Rackete, who was recently acquitted of all charges brought against her for entering the Italian port of Lampedusa in July 2019.[2] Sara Bellezza addresses the rights of people on the move within the framework of relocation between European MS. She analytically connects the closed-port policies with the hotspot-approach and relocation procedures forming part of the EU's Dublin regulation. Through qualitative interviews with survivors of distress at sea, she re-narrates the experiences protection-seekers must go through when arriving in Europe. Both authors of this paper will argue, from the perspective of the respective legal angle addressed, that the security and protection of people on the move along this border, one of the deadliest in the world, is subordinated to the EU's border enforcement attempts.

2. EU-Libya Cooperation in Violent Border Control

Since the EU intensified funding and training for the so-called Libyan Coast Guard (LCG), whose legitimacy is drawn into question by human rights observers,[3] thousands have drowned or been intercepted and illegally returned to Libya in the Central Mediterranean Sea.[4] Still, true numbers of crossings, shipwrecks and deaths remain unknown.

In 2018, the UN's International Maritime Organisation (IMO) formally acknowledged Libya's so-called SAR region (SARR).[5] Previously, this region fell under the responsibility of the Italian Maritime Rescue Coordination Centre (IMRCC), whose SARR extended to Libyan waters. Each NGO rescue ship in this area received instruction, coordination and support for trans-shipment and disembarkation from the IMRCC.

In my personal experience in rescue missions since 2017, I caught a glimpse of Italian cooperation while it lasted, not only in the IMRCC's daily coordination, but also in hearing stories of citizens hailed as heroes of rescue; fishermen and merchant ship crews, but also dedicated Italian Coast Guard vessels, stepping in to rescue thousands of people off their shores.

Throughout 2017 and 2018, a noticeable shift happened in state commitments to rescue. Failed naval Operation Sophia, mostly focused on wider efforts to disrupt the business model of human smuggling and trafficking networks' but also, ironi-

[2] Z. Freudenberg et. al.: The Island of Hope in a Sea of Misery. The Italian Court of Cassation's Unequivocal Stance on the Right to Disembark. <https://verfassungsblog.de/the-island-of-hope-in-a-sea-of-misery/ > (07/21)

[3] "Amnesty Challenges French Government's 'Reckless' Donation to Libyan Coast Guard." Amnesty International, 25 Apr. 2019, <www.amnesty.org.uk/press-releases/amnesty-challenges-french-governments-reckless-donation-libyan-coast-guard> (06/21).

[4] "Missing Migrants Project", *International Organisation for Migration*, <missingmigrants.iom.int/region/Mediterranean> (06/ 2021).

[5] "EU/Italy/Libya: Disputes over Rescues Put Lives at Risk." *Human Rights Watch*, 25 July 2018, <www.hrw.org/news/2018/07/25/eu/italy/libya-disputes-over-rescues-put-lives-risk.> (06/21).

cally, preventing 'the further loss of life at sea,'[6] withdrew its ships in March 2019.[7] With power change in Italy came policy change costing people their lives. Now a distress alert is sent by the IMRCC 'on behalf of 'LCG,'' which has been observed to violently intercept boats and rescues, as in the deadly interception of a Sea-Watch rescue on 6 November 2017,[8] and conducts illegal refoulement to Libya; a phenomenon widely recorded by civil society observing from both sea and air, including Sea-Watch. European military vessels have redirected their resources to support a new border surveillance approach termed 'refoulement by proxy', directly coordinating push- and pullbacks to Libya, physically carried out by the 'LCG' or commercial vessels.[9] UNHCR acknowledges that Libya does not "meet the criteria for being designated as a place of safety for the purpose of disembarkation following rescue at sea."[10]

Individuals attempting the sea crossing often describe seeing aircraft fly overhead or ships sailing past but not rescuing. Such unlawful acts of non-assistance, carried out with impunity, are symptoms of a cruel border regime. Civil society is far from able to fill the vacuum in SAR created by states; thousands still go missing at sea in an emergency that could be prevented entirely if there was intention to do so. This is not a 'migration crisis,' but a crisis of European responsibility towards displaced people, and which has post-colonial and racist undercurrents.

3. Legitimacy of Humanitarian Response and Humanitarian Coordination

In contrast to strong military coordination with Libyan counterparts by Europe, there is a marked lack of supranational coordination on the civil/humanitarian side

---

[6] Mission, Operation Sophia, EUNAVFOR MED <https://www.operationsophia.eu/about-us/> (06/21).

[7] "EU: Diminished 'Operation Sophia' Abandons Refugees and Migrants to Reckless Libyan Coast Guard." *Amnesty International*, 27 March 2019, <https://www.amnesty.org/en/latest/news/2019/03/eu-diminished-operation-sophia-abandons-refugees-and-migrants-to-reckless-libyan-coast-guard/> (06/21).

[8] "Legal Action against Italy over Its Coordination of Libyan Coast Guard Pull-Backs Resulting in Migrant Deaths and Abuse." *Sea-Watch e.V.*, May 8, 2018, <https://sea-watch.org/en/legal-action-against-italy-over-its-coordination-of-libyan-coast-guard/> (06/21). C. Heller et. al, "Opinion | 'It's an Act of Murder': How Europe Outsources Suffering as Migrants Drown." *The New York Times*, December 26, 2018, <https://www.nytimes.com/interactive/2018/12/26/opinion/europe-migrant-crisis-mediterranean-libya.html.> (06/21).

[9] C. Heller and L. Pezzani. "Mare Clausum", *Forensic Architecture*, May 2018, <https://content.forensic-architecture.org/wp-content/uploads/2019/05/2018-05-07-FO-Mare-Clausum-ExEN.pdf>.(06/21).

D. Howden, A. Fotiadis, and Z. Campbell. "Revealed: The Great European Refugee Scandal." *The Guardian*, 12 March 2020. <https://www.theguardian.com/world/2020/mar/12/revealed-the-great-european-refugee-scandal> (06/21).

[10] UN High Commissioner for Refugees (UNHCR), *Position on the Designations of Libya as a Safe Third Country and as Place of Safety for the Purpose of Disembarkation Following Rescue at Sea*, September 2020. < https://www.refworld.org/docid/5f1edee24.html> (06/21).

of the equation. It lacks legitimisation as a 'worthy' emergency by the institutions mandated with improving the delivery of humanitarian aid worldwide. Assistance largely takes place outside of the formal humanitarian response architecture; including recognition by UNOCHA, which assesses whether crises warrant international response and ensures efforts are well organised. Emergency response in the Mediterranean lies in limbo between humanitarian coordination in Libya and in Italy, where UN bodies like UNHCR and IOM, as well as INGOs adhering to the international cluster approach under IASC,[11] are present. Naturally, well-coordinated response is unwanted by the very states creating the humanitarian need.

Bridging gaps in assistance at sea falls entirely on civil actors at sea, whom to an extent have self-organised informal coordination mechanisms. One example is the referral of people with specific vulnerabilities to partner NGOs and UN bodies on shore, for a smoother transition in service delivery and onward care after disembarkation.

The coordination gap is amplified by the fallout of the IMRCC's role, which in this context provided at least limited ways of improving 'assistance' by avoiding duplication of efforts and deploying resources according to emerging needs. Intended or not, this coordination held an element of 'humanitarian coordination', for the simple fact that those rescued at sea may be seeking international protection and require, by law, special consideration by those rendering assistance. SAR operations must include explicit efforts to ensure the right to seek asylum, enshrined in the UDHR[12] and the EU's Charter of Fundamental Rights.[13] This includes disembarkation in a Port of Safety (PoS) where people face no 'rejection at frontiers and have access to fair and effective procedures for determining status and protection needs.'[14] This effort was easier when rescue was legitimized by coastal state institutions' coordination.

The intersection between SAR as a maritime and as a humanitarian practice has long been recognised. According to UNHCR, "state responsibility under international refugee law, and in particular the 1951 Convention relating to the Status of Refugees, is activated once it becomes clear that there are asylum-seekers among those rescued."[15] This connection between maritime and refugee law underpins each rescue ship stand-off.

---

[11] "The Inter-Agency Standing Committee", *IASC*. <interagencystandingcommittee.org/the-inter-agency-standing-committee> (06/21).

[12] United Nations. 1998. *The Universal Declaration of Human Rights, 1948-1998*. [New York]: [United Nations Dept. of Public Information].

[13] European Union: Council of the European Union, *Charter of Fundamental Rights of the European Union (2007/C 303/01)*, <https://www.refworld.org/docid/50ed4f582.html> (06/21)

[14] UN High Commissioner for Refugees (UNHCR), *Background Note on the Protection of Asylum-Seekers and Refugees Rescued at Sea (Final, including Annexes)*, 18 March 2002, <https://www.refworld.org/docid/3cd14bc24.html> (06/21).

[15] Ibid.

4. The failure of Deterrence Policies

Civil humanitarian actors face constant threats to the freedoms required to occupy this maritime space. EU policies of deterrence take up increasingly hostile forms, despite being proven unsuccessful. A recurring argument in EU deterrence discourse is the so-called 'pull-factor' argument. It has long been evidenced that there is no causal link between attempted crossings and the presence of NGO rescue (or any other) ships.[16] More rescue ships present does not equal more boat launches from Libya. Conversely, the removal of rescue ships also does not act as a deterrent for smugglers launching boats;[17] a point made painfully clear by many mass drownings on record, including a 2015 shipwreck that accelerated the start of Operation Sophia.[18] Often, as in 2018, a decline in dedicated rescue ships (along with rises in non-assistance by private ships) in the area, actually coincides with higher death rates.[19]

5. Strategies in Limiting the Freedom to Navigate Humanitarian Space

Non-governmental humanitarian actors working in the Mediterranean Sea certainly do not enjoy a free humanitarian space;[20] movement is restricted and legal or administrative obstacles, such as technical ship inspections, crew arrests and prosecution, and confiscation of organisational assets including ships, are a constant threat looming over NGO operations. Rather than enjoying overall access permission, each single departure from port may be an NGO's last for weeks, months, or even years, as in the case of the permanent confiscation of the Iuventa ship, whose crew have been under criminal investigation and facing trial in Italy for almost four years.[21]

---

[16] E. Steinhilper and R. Gruijters. "Border Deaths in the Mediterranean: What We Can Learn from the Latest Data." *University of Oxford, Faculty of Law, Border Criminologies Blog*, 8 Mar. 2017 <www.law.ox.ac.uk/research-subject-groups/centre-criminology/centreborder-criminologies/blog/2017/03/border-deaths> (06/21).

[17] C. Heller and L. Pezzani. "Blaming the Rescuers." *Forensic Architecture*, June 2017, <blamingtherescuers.org/> (06/21).

[18] N. Nováky. "The Road to Sophia: Explaining the EU's Naval Operation in the Mediterranean." *European View*,
Oct. 2018, pp. 197–209, <https://doi.org/10.1177/1781685818810359> (06/21).

[19] "Six People Died Each Day Attempting to Cross Mediterranean in 2018, UNHCR Report Shows." *UNHCR*, 30 Jan. 2019, <www.unhcr.org/ph/15103-six-people-died-each-day-attempting-to-cross-mediterranean-in-2018-unhcr-report-shows.html> (06/21). "Over 1,600 Died in Mediterranean This Year: UN." *Al Jazeera,* September 3, 2018, <https://www.aljazeera.com/news/2018/9/3/mediterranean-refugee-numbers-drop-but-crossing-is-deadlier-un> (06/21).

[20] 'Humanitarian space' is the symbolic space within which NGOs enjoy freedom of movement, to establish dialogue with the people they serve and stakeholders in their intervention; to assess needs; and to monitor the provision of assistance. It is based on the notion that the ability to deliver humanitarian relief according to the established principles is contingent upon equal access to victims, resources, and the abilities to maintain proportionality and to complement existing services in response to disaster or emergency.

[21] "Italy: Crew of Rescue Ship Face 20 Years in Jail on Third Anniversary of Smuggling Investiga-

The right to seek protection is enshrined in international law,[22] and rescue has been a centuries-long code among seafarers long before it became law.[23] Yet, it appears that Europe cannot unite to guarantee even the right to life itself, but does agree on strengthening external borders. This is not only an Italian problem; EU-wide response to the influx of asylum-seekers is the militarisation of borders[24] and a disproportionate emphasis on deterrence and anti-smuggling agendas as opposed to on the facilitation of protecting human life. MS (be they coastal, transit or flag states) have stretched or even made-up new laws to criminalise (the rescue of) asylum-seekers.

6. Blockades: Sea-Watch 3

The mission described below happened after a prolonged season of (administrative and physical) blockades imposed by EU MS. In February 2019, Sea-Watch 3 was held in Catania after extensive Ialian port and Dutch flag-state controls, used as a political tool to keep it, at the time the last active NGO rescue ship, from sailing. The ship docked in Catania to bring 47 people to shore (only permitted after six MS agreed on an ad hoc relocation); a lawful act which prompted a police investigation by the Criminal Prosecutor of Catania, the result of which later cleared Sea-Watch of any criminal conduct.[25]

That same year the Dutch Minister of Infrastructure and Water Management Van Nieuwenhuizen introduced a new policy on ship safety, targeted at Sea-Watch. Under the Dutch Freedom of Information Act, Sea-Watch gained insight into the historical process behind this swift policy change, which confirmed that safety was not the concern, but that the Dutch government was looking to restrict disembarkations by NGO ships at the Ministry of Foreign Affairs' request. Emails showed the Cabinet calling an urgent consultation a week before the Migration Summit in June, asking for new ways to regulate NGO ships in the context of migration policy.

Under the veil of safety concerns for shipwrecked persons, the new rules in effect were an administrative blockade. The Netherlands was known for having an

---

tion.", *Amnesty International,* 31 July 2020, <www.amnesty.org/en/latest/news/2020/07/italy-crew-of-rescue-ship-face-20-years-in-jail-on-third-anniversary-of-smuggling-investigation/> (06/21).

[22] UN High Commissioner for Refugees (UNHCR), *The 1951 Convention Relating to the Status of Refugees and its 1967 Protocol*, September 2011.

[23] UN General Assembly, *Convention on the Law of the Sea*, 10 December 1982. International Maritime Organization (IMO), *International Convention for the Safety of Life at Sea*, 1 November 1974, 1184 UNTS 3. International Maritime Organization (IMO), *International Convention on Maritime Search and Rescue*, 27 April 1979, 1403 UNTS.

[24] J. Jolly. "Airbus to Operate Drones Searching for Migrants Crossing the Mediterranean." *The Guardian*, 20 Oct. 2020, <www.theguardian.com/business/2020/oct/20/airbus-to-operate-drones-searching-for-migrants-crossing-the-mediterranean> (06/21).

[25] "Sea Watch 3 Still Held in Catania Port after Being Cleared of Criminal Charges", *European Council on Refugees and Exiles (ECRE)*, 8 February 2019, <www.ecre.org/sea-watch-3-still-held-in-catania-port-after-being-cleared-of-criminal-charges/> (06/21)

'open arms policy' for ship registration, providing a so-called 'flag of convenience' including for activists and NGOs operating ships.[26]

The political nature of the policy was confirmed by the fact that each proposal for new regulations was shared with the Directorate of Migration Policy at the Ministries of Justice and Foreign Affairs for approval, which clearly has no mandate on questions of ship safety, but does on matters of migration.

Sea-Watch called into question the legitimacy of the process, took this case to court and won it.[27] Two Dutch courts stated that the Minister had violated the rules of good governance and that the policy did not justify the consequences; people drowning in the Mediterranean Sea. In practice however, the policy took its intended toll (several months of being stuck in port). Sea-Watch decided to undo its original flag of choice and instead now sails under the German flag.

7. Minister Salvini's Decree and Its Human Impact

On 12 June 2019, the Sea-Watch 3 performed a rescue of a rubber dinghy in distress, bringing all 53 shipwrecked persons safely on board. The unseaworthy rubber boat was located in international waters, about 47 nautical miles north of Zawiya, Libya.

During the rescue, an unmarked vessel associated with the 'LCG' approached the scene at high speed; the fear was palpable among the final group remaining on the dinghy. A common sentence heard, familiar to any activist involved in civil SAR is: 'I would rather die than go back to Libya'. Yet, the first official response to the rescue was an email assigning us Tripoli as PoS, effectively asking the ship to conduct refoulement, neatly in line with EU values and policy. Then Italian Minister of Interior Matteo Salvini demanded that Sea-Watch follow Libyan instructions, which of course we declined.

Two days post-rescue, a new decree introduced by Minister Salvini was passed in the Senate, effectively banning the entry of rescue NGOs into Italian waters and criminalising civil ships' disembarkation of rescued people in Italy.[28] The new law targeted NGO rescue ships, the sensational topic around which Minister Salvini's campaign was built, and contradicted international law in that it hindered lawful free passage of vessels into territorial waters, as well as the prompt provision of a PoS for shipwrecked persons.

Sea-Watch found itself in another stand-off with Italy, an unnecessary escala-

---

[26] E. Wallis, "Sea-Watch 3 to Sail under German Flag.", *InfoMigrants*, 5 December 2019, <https://www.infomigrants.net/en/post/21353/sea-watch-3-to-sail-under-german-flag > (06/21).

[27] "Sea-Watch Wins Court Case in The Hague: Sea-Watch 3 Wrongly Prevented from Sailing since Early April", *Sea-Watch e.V.*, 7 May 2019, <sea-watch.org/en/sea-watch-wins-court-case-in-the-hague-sea-watch-3-wrongly-prevented-from-sailing-since-early-april/> (06/21).

[28] L. Tondo, "Italy Plans to Fine NGO Boats up to €5,500 per Rescued Migrant.", The Guardian, 13 May 2019, <www.theguardian.com/world/2019/may/13/italy-fine-ngo-boats-migrants-salvini> (06/21).

tion in an otherwise lawful act. In one of the daily meetings with rescued people and crew, in which political developments were openly discussed, there was a startling realisation that we were at the heart of something historical; new laws were being written in Italy, and people on board were ready to risk prosecution. While the world was watching, we joked about politicians drafting new decrees just for us; and just how impactful 40 travelers and 22 activists on one ship can be.

In over two weeks at sea without acknowledgement of the urgent specific needs of people on board, the morale fluctuated with brief moments of hope of a political solution, followed by the reality of being stuck on a ship with pressing protection, physical and mental health needs waiting to be properly addressed on shore. Despite the ship being well-equipped above standard, there is only so much transitory humanitarian assistance can achieve.

Several medical evacuations occurred under Italian Coast Guard coordination. This ostensible act of good will was a crowd management risk, and indeed distinguished between urgencies: a necessary medical evacuation does not negate the urgent needs of those remaining, including unaccompanied minors and those suffering mental health emergencies. In each of what we called 'partial disembarkations', there was a palpable dip in morale. Those remaining asked things such as: 'Must we also be dying on this ship for Europe to recognise our need?' In fact, our crew had identified at least five people with suicidal intentions, after which we expanded our 24/7 watches on the deck to include a 'suicide watch'. This ultimately became one of the breaking points in the decision to dock in Lampedusa, as we could no longer guarantee the safety of all on board.

Another moment of crushed hope was the European Court of Human Rights' decision on the case filed on behalf of those rescued. The Court failed to order Italy to allow their disembarkation. In a press release stating its position on the urgent filing, the Court said: "In his reasoning the president of the court noted, inter alia, that the vulnerable individuals, children and pregnant women on board had been disembarked on 15 June and that Sea-Watch 3 had not indicated that other individuals from vulnerable categories were on the ship. In consequence, he considered that there were no exceptionally serious and urgent reasons justifying the application of the urgent measures".[29]

This demonstrates the problem in the portrayal of this emergency; lacking recognition of the urgency to disembark *any* person rescued, and fueling the misperception that it is only those identified as most severely in medical need who can lawfully be given a PoS without delay. By law, shipwrecked persons do not need to 'compete' for protection.

Italy's hostile 'closed ports' policy unnecessarily prolonged the emergency for people rescued. However, past the façade of Minister Salvini's smear campaign, of

[29] European Court of Human Rights, Rackete and Others vs. Italy, Application No. 32969/19, Registrar of the Court, 'Request for interim measure refused in the case of Sea Watch 3', Press Release – Interim Measures of 25 June 2019, <https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-6443361-8477507%22]}> (06/21).

which rescued people partially became the target, Italy's ports were actually as open as ever. A day after Sea-Watch docked in Lampedusa, an independent arrival of a wooden boat happened before our eyes, and hours later, the same number of people rescued (closer to Italian coast) by NGO ship Open Arms were escorted to Lampedusa by Italy's Coast Guard. This poignantly illustrates that this decree was mostly aimed at civil rescue ships, and to the hypocrisy of the political discourse in Italy at the time. It demonstrates the arbitrary application of closed port policies; this particular civil mission was chosen to create a border spectacle surrounding the arrival of only 40 people. When the 'LCG' are not close enough to conduct a pullback, Italian vessels faced with distress cases in their own SARR have no choice but to uphold international laws relating to PoS; laws which Minister Salvini chose to violate in at least 24 stand-offs in the period of one year, and which the EU consistently violates in every standoff where arrival becomes conditional upon ad hoc MS negotiations.

In the world media there was little depth beyond the sensationalist imagery of a stand-off between a captain and an Italian Minister. One need not look further than this illustrative mission to understand what civil action in the Mediterranean stands for. Every decision on board was underpinned by the dignity and right of every person on the ship, especially of those who, even throughout the viral media frenzy covering this mission, largely remain unnamed and unheard themselves. However, on board, their voice was more important than the propaganda of political 'leaders'. We refer to people by their names, Nadege, Salma, James, Mohammed, rather than by the number drawn on their shirts by a smuggler or by the statistic they become as another batch of arrivals to Europe.

8. Closed-port-policies and EU *ad hoc* Relocation

Since 2018, the closed port policies were, as Haidi Sadik outlined, targeting the arrival of civil SAR ships. Entry into a safe port in Italy or Malta was not allowed until the EU came to a relocation agreement for the distribution of the passengers to other EU Member States (MS). Alongside racist remarks against the arrival of protection seeking persons in the EU, the closed port-policies were deployed to emphasize a critique on the Dublin regulation, which decrees that protection seeking persons need to apply for asylum in the first country of arrival.[30] Mobilizing a decade old dispute among EU MS around the question of distribution of asylum-seeking persons within the EU, Salvini was not asking for the abolishment of the Dublin regulation. Instead, he was asking for relocation agreements. Relocation is an inte-

[30] European Communities Convention 97/C254/01 of 19.08.97 Determining the State Responsible for Examining Applications for Asylum Lodged in one of the Member States of the European Communities. The Dublin III convention Regulation No. 604/2013 is the most recent valid EU convention concerning the responsibility for the examination of an asylum application inside the EU Regulation (EU) No. 604/2013 <https://eur-lex.europa.eu/LexUriServ/LexUri-Serv.do?uri=OJ:L:2013:180:0031:0059:en:PDF> (12/2020).

gral part of the Dublin regime and it continues to take place from Italian and Greek hotspots. Italy and Malta's refusal to let people arrive in a safe port was violating the rules of international human rights and maritime law. However, as often in EU border management, the political tug war around the arrival of such a small number of people turned out to be a successful strategy, as a result of which disembarkations were subjected to prior negotiations of EU MS on relocation. Between July 2018 and June 2019 alone, 24 stand-offs were enforced on SAR NGO ships and merchant vessels, as well as on Italian Coast Guard vessels.[31] The former Italian Minister Salvini was in fact accused of deprivation of liberty for keeping the crew and 131 survivors of a distress case on the Coast Guard ship Gregoretti from disembarking in an Italian port.[32]

A strong civil society movement in Europe, including sea rescue NGOs, the rescued people and those who stand in solidarity with both, called for safe harbors in Europe and the distribution of asylum seekers from the hotspots.[33] Various EU governments felt compelled to act. The German government and other EU MS were able to position themselves in this game as players on both sides. While introducing themselves as humanitarian actors willing to accept shipwreck survivors as asylum seekers in their countries, they would also bargain around the numbers of people they would accept from each boat. Following the demand for reception and a safe harbor, this strategy allowed EU MS to maintain the status quo in Italy, Malta and Greece by not abolishing neither the Dublin regime, nor the hotspot approach. The agreed relocation from the hotspots however only concerned a very small number of people. Persons arriving autonomously in Italy, Malta or Greece or who are rescued by non-civil SAR ships are not included in the EU ad hoc relocation mechanism that was temporarily formalized in September 2019. How do relocation politics play out on the ground? In the following, I will approach this question through a positioned research, attending to the voices of the people targeted by these politics. I will draw data from the relocation research project conducted in a collective effort by borderline-europe, Borderline Sicilia, Equal Rights Beyond Borders, Refugee Council Berlin and Sea-Watch. This project was meant to shed light on relocation by interviewing over 45 persons after arrival in Italy, Malta, Germany, and in single cases, France and Portugal.[34] Those people were rescued by different search and rescue NGO ships and relocated from either Malta or Italy to Germany (or respectively France and Portugal). For over a year, we followed their trajectories and engaged in producing an extensive report on the EU ad relocation mechanism. In

[31] < https://eu-relocation-watch.info/#closed-ports> (06/21).

[32] *Matteo Salvini trial for kidnapping authorised by Italian senate*, <https://www.theguardian.com/world/2020/feb/12/matteo-salvini-trial-for-kidnapping-authorised-by-italian-senate> (03/21). Italy's premier testifies in Salvini migrant case, <https://www.aa.com.tr/en/europe/italys-premier-testifies-in-salvini-migrant-case/2126756> (03/21).

[33] The Greek hotspot Moria on the island Lesvos gained painful notoriety when it burned down in September 2020, though the conditions in the camp have been inhuman ever since its opening.

[34] *EU Ad Hoc Relocation- A Lottery from the Sea to the Hotspots and back to Unsafety*. <eu-relocation-watch.info> (06/21).

addition to the qualitative interviews, which are the most extensive source, as it is the firsthand experience that gives testimony to the consequences, the chaos and arbitrary procedures created by EU institutions, we relied on parliamentary inquiries, official EU documents and academic research in relation to relocation to be able to draw an encompassing picture on ad-hoc relocation in relation to the closed port policies. We are grateful for their trust in sharing their stories with us, especially after having gone through so many interview processes, as described below. From this extensive study, I will share the stories of two persons I met in Germany after their relocation procedure took place and whom I have been accompanying through their fight for papers ever since.

9. From Libya to Italy, then to Germany

The experiences of Baqer and Justine include their trajectory from Libya to Italy, from where they were relocated to Germany. Baqer and Justine left their home countries in 2016. Starting from two different countries, both had to endure long voyages through the desert, numerous countries and cities and suffered imprisonment in Libya with all its dire consequences. They were rescued from a distress case from the rescue ship Ocean Viking on September 9, 2019, and assigned a safe harbor in Lampedusa, which allowed for disembarkation on September 15, after "only" 6 days of stand-off. After arrival, the group of 82 people was fingerprinted and interviewed by Frontex officers in Lampedusa. The Frontex interview, according to Baqer and Justine, was relatively short and the officers were mostly interested in the route they had taken to come to Libya.

Two weeks later, they were transferred from Lampedusa to Messina, where the relocation procedure began. In Messina, the reception center is divided into two spaces: one so-called hotspot facility, where, according to EU law, people are not allowed to be kept longer than four weeks, and on the same premises, the reception center that is supposed to "host" people for an unlimited time. The hotspot in Messina serves as an experimental space, where the EASO develops and puts into practice the hotspot approach.[35] Frontex, the EU's Border and Coast Guard Agency, EASO, the European Asylum and Support Office, Europol, the EU's Law Enforcement Agency and Eurojust, the EU's Agency for Criminal Justice Operations send officers and staff to register, interview and return persons in- and from the so-called hotspots.[36] As Martina Tazzioli and Glenda Garelli[37] underline, the hotspot system does not mean detention without exit, but rather is intended to slow down migration and to contain further movement within the EU. Occasionally, a media scandal aris-

[35] EASO/ED/2019/403 Note on the 'Messina Model' applied in the context of ad hoc relocation arrangements following disembarkation, 10.09.2019.

[36] Ibid.

[37] M. Tazzioli and G. Garelli (2020) Containment beyond detention: The hotspot system and disrupted migration movements across Europe. *Environment and Planning D: Society and Space*, 2020, pp. 1009-1027.

es over the horrific conditions that persons who are stuck in the hotspots are confronted with. From Lampedusa to Lesvos, from detention centers in Malta to the so-called Ankerzentren in Germany, camp structures in Europe are beyond human rights, and instead constitute spaces of various forms of violence and abuse. Detention in hotspot facilities constitutes, among others, a breach of Article 9 of the Universal Declaration of Human Rights which states that "No one shall be subjected to arbitrary arrest, detention or exile."[38]

According to Baqer and Justine, the conditions in Messina were untenable. The people who were rescued from distress at sea were situated in a different building than those who had managed to arrive independently to Lampedusa or were rescued by merchant vessels or the Italian Coast Guard. Both described that they were not provided with fresh clothes, which meant that they stayed with the same clothing for months. A quick medical check-up was done after arrival, however, no access to any further needed medical care was provided, nor did they have the possibility to speak with a lawyer. None of the survivors received any money to buy food or clothing, nor were they allowed to move freely in Sicily, even after they left the hotspot facilities in Messina.

In Messina, as foreseen by the Messina Model, the European Asylum and Support Office (EASO) is supposed to conduct pre-selection interviews in Italy and Malta, after which each Member State is invited to send delegations to the respective hotspots, interview the selected persons again and then organize for transport to the other EU states.[39] Every Member State is invited to voluntarily accept people rescued from distress at sea. As pre-selection at the external borders is not provided for by EU law (at least so far, which the new pact on migration wants to formalize), the EASO is not supposed to make final decisions on the asylum claims of the respective person. Asylum decisions thus should take place after relocation, not before.[40]

There are some guidelines that should organize the EASO selection procedure. They include considering the potentiality of the respective person to receive international protection. Also, cultural links and family ties should play a pivotal role during the selection process.

As Bareq and Justine recall, the interview lasted for about one hour, during which the EASO staff let them tell their story rather freely, in presence of a translator in respectively French and Arabic. After the interview, EASO staff members showed them a transcript of their interview and let them sign. However, neither of them received a copy of their testimony. Still in Messina, the group was informed by a letter that was openly hung on the wall in the camp, informing the people about who was selected to be relocated to which EU country. Baqer and Justine found

[38] *Fact Sheet No. 26, The Working Group on Arbitrary Detention*, <https://www.ohchr.org/Documents/Publications/FactSheet26en.pdf >(06/21).

[39] Ibid.

[40] Answer to parliamentary inquiry 19/9703 Aufnahme und Verteilung aus Seenot geretteter Schutzsuchender (translation by author: Reception and relocation of protection seeking persons rescued from distress at sea), 26.04.2019, p. 4 f.

their names on the list for the German delegation, though as they underlined during our conversation, they had no idea why they were selected to go to Germany.

The interview with the German delegation was the longest. It lasted for two hours, and they asked more questions than during all the other interviews before. On the following day, Baqer and Justine were called for a second interview with other migration officers for another half hour. The German delegation presented themselves as being responsible for Baqer's asylum procedure but did not mention their affiliation to the German Domestic Intelligence Service, whose practice of conducting security check-ups outside of German territory is legally controversial.[41] During the interviews, Baqer recalls having been asked the following questions: Was he part of the army, did he participate in any action of rebel groups, what was his religion? They also asked discriminatory questions such as "what was he going to do if his kid came out as homosexual?" Or: When you go to Germany and a Christian person comes with a drawing from his prophet, what would he do? Again, neither Baqer, nor Justine were provided with any documentation or copy of the interview conducted by the German delegation. Three months later, they were called through loudspeakers in the camp: Those who hear their names, will be transferred to Germany. Some people were rejected without explanation. Others waited for nine months before being transferred.

Baqer and Justine were especially surprised that they had to give their fingerprints a third time, when they had already been fingerprinted in Lampedusa by Frontex, the Italian Police in Messina and the third time by the German delegation. After one month in Messina, a group of people was transferred to Crotone, where they stayed until their relocation flight from Rome to Germany took place in December 2019. When asked about Italy, both Justine and Baqer turn silent. Italy was not good. No money for food, no medical care, no chance of moving around, nobody wants to stay there, they said.

What their narrations show are the manifold ways in which people on the move are criminalized, placed under general suspicion and treated as if they had committed a crime. From the numerous interrogations to the fingerprinting, the lack of information provided to them and the lack of possibilities of choosing where to go, where to stay and for how long.

This policing of persons contradicts the allegedly humanitarian approach to survivors of sea distress cases, that the EU is trying to sell to the public. Relocation does not provide a solution to the badly crowded Italian hotspots, nor the immigration detention centers in Malta. In fact, as the stories of Justine and Baqer painfully illustrate, in practice the Messina Model with its involvement of numerous EU agencies and local police authorities does not actually translate to humane treatment. Having to walk around in the same clothes for months, being confronted with a deprivation of liberty in closed facilities, and not being able to access legal or medical assistance constitutes several human rights violations. The relocation ap-

[41] EU ad hoc relocation- a lottery from the sea to the hotspots and back to unsafety, <https://eu-relocation-watch.info/#dubious-selection-criteria> (06/21).

proach does not help to restore survivors of distress cases as the sovereigns for their lives and movements. Instead, it puts them through various hardships which include immense precarity, strain and indefinite times of insecurity. The extent to which time, temporality, hope, future and space are taken from people seeking protection and security is striking.

10. The German Delegation and Controversial Security Check-ups

Germany was one of the 5 countries who agreed in La Valetta, Malta on the 19th of September 2019, to formalize the ad-hoc- relocation mechanism. For every disembarkation, Germany would accept a specific quota of people for transfer to Germany from a Maltese or Italian hotspot.

The German government declares that they have no pre-established selection criteria for the people they will transfer, but the delegation will try to consider family ties, cultural links and the prospects of staying long-term in Germany etc. for the selection.[42] Also, the German delegation sends representatives of the Bundespolizei (federal police) and staff from the German Domestic Intelligence Service for conducting security check-ups with the respective people.[43] Apart from the criminalizing nature of those security check-ups, the deployment of the German Domestic Intelligence Service abroad is legally controversial. German federal law does not foresee, ever since the experiences of the Nazi regime, any activity of the German domestic intelligence abroad.[44] Also, it is questionable on which legal grounds people can be subject to interviewing by any intelligence service without any assumption of illegal activity that would suggest such interviewing was necessary. During the interview process, neither the German federal police, nor the intelligence service identify themselves as such to the people being interviewed. As mentioned before, when people are rejected on security grounds, those people are not informed about the reason for their non-acceptance and remain in the country of first arrival to conduct their asylum process there.

Between 2018 and 2020, Germany agreed to transfer 1291 people from Italy and Malta. However, transfer was only organized for 624 people.[45] Also, contrary to the declared intention, among the people relocated to Germany, which should consider the prospect of potentially staying in Germany after relocation, 82 percent of the relocated people received a rejection on their asylum claim.[46]

---

[42] Answer to parliamentary inquiry 19/7209, Aufnahme aus Seenot geretteter Flüchtlinge (translation by author: Reception of refugees rescued from distress at sea), 21.01.2019, p. 2.

[43] Answer to parliamentary inquiry 19/14638, Sicherheitsüberprüfung Schutzssuchender (translation by author: Security check-ups on protection seeking persons), 30.10.2019.

[44] *EU ad hoc relocation-a lottery from the sea to the hotspots and back to unsafety* <https://eu-relocation-watch.info/#dubious-selection-criteria> (06/21).

[45] Answer to Parliamentary inquiry BT-Drucksache 19/21657 Aktuelle Fragen zur Aufnahme aus Seenot geretteter Asylsuchender (translation by author: Current questions concerning the reception of asylum seeking persons rescued from distress at sea), 11.11.2020, p. 3 f.

[46] Ibid. p. 12.

11. How Did Baqer's and Justine's Story Continue?

Both arrived together on a transfer flight from Rome to Germany on the 21st of December 2019. Four buses were waiting for the group of 132 people, who were served a lunch-package and then divided to different first reception centers in Germany. There was no information given to the people where they would go.

Baqer and Justine arrived in two different regions. They stayed in touch over the phone. Baqer stayed in the first reception center only for 11 days, after which he was transferred to another reception center. There, he spent another month, before he arrived in the camp where we finally met in August 2020. Justine on the other side, spent the first two months in one reception center that gained notoriety during the beginning of the Corona pandemic for not providing enough food to its inhabitants. For her, the transfer to the second reception center was very troublesome, as she happened to be the only woman in the premises. She spent 6 months in the second shelter and finally received a small apartment on her own, after accessing several social assistance centers who supported her claim to the local authorities for a safe living space. While she was recognized as 'vulnerable' and thus could improve her living situation, this recognition had no influence on her asylum process.

Both Justine and Baqer had yet another asylum interview in Germany in the first month after arrival. Without any prior legal counseling or any information about the German Asylum system, both went to their interviews unprepared.

This is relevant, as the German Federal Office for Migration and Asylum (BAMF) issues negative asylum decisions quick-handed, when court revision often reveals that the respective person was indeed eligible for international protection.[47] The asylum interview in Germany, as Baqer and Justine recall, lasted for over 5 hours. A second interview with another official followed the day after, which lasted for three hours. They were asked the same questions they had already answered in Italy and additional new questions. What was most surprising to them, was the question from the BAMF official how they managed to arrive in Germany. Apparently, the staff did not know that they had come with an official relocation flight. However, they had the impression that the BAMF officials seemed to be in possession of the interview that was taken in Italy and seemed to compare their answers.

In August 2020, when we met for the first time, Baqer had not received his decision yet. He was worried, because Justine and all the other people, who he had stayed in touch with from the same relocation flight, had received a negative decision. So far, he did not have a lawyer or any legal counsel. Justine and I met in October 2020. She had already received her rejection in February 2020 and appealed

[47] Negative decisions on asylum claims are responded with a 75 percent appeal rate, of which at least 30 percent of appeals were successful in front of German administrative courts. Additionally, more than 270.000 cases of negative BAMF decisions were pending lawsuits in 2019, which suggests that the actual acceptance rate might be even higher when the court dates are finally there. Answer to parliamentary inquiry 19/18498, Ergänzende Informationen zur Asylstatistik für das Jahr 2019 (translation by author: additional information on Asylum Statistics for 2019), 02.04.2020; *Asyl in Zahlen 2019* https://www.proasyl.de/hintergrund/asyl-in-zahlen-2019/ (06/21).

in front of an administrative court. In June 2021, both Baqer and Justine's asylum claims were conclusively rejected. Neither the BAMF, nor the court was willing to grant a humanitarian permit to stay on the basis of the trauma and violence they had experienced during their journey to Europe.

Justine and Baqer, as well as all the other people we met and talked to in Germany, and those who continue to contact us, are disillusioned and do not understand the relocation procedure. Why would Germany accept them, relocate them and then reject them? Why did many of the people they had met in Lampedusa, who went to France, receive a residence permit for the next 10 years, while 82 percent of the people that were relocated to Germany did receive a negative decision? Baqer feels like they were tricked by Germany. First, they were relieved when they were accepted by Germany, but did not know that they were going to be confronted with so many other interviews, and then receive a negative decision. Baqer underlines several times that first creating that hope and then this disillusion was what troubled him most.

12. Conclusion

Ironically, it is under the veil of 'humanitarianism' that the EU carries out deadly and often unlawful policies of deterrence, including the criminalisation of civil humanitarian action. The breach of international law by EU-wide anti-immigration and deterrence policies ranges from limiting navigable spaces and creating norms of non-assistance, pull- and push backs and refoulement, to the undignified treatment and rights violations experienced by asylum-seekers within European relocation schemes.

Those who are still dedicated to sea rescue, including fishermen, captains of merchant vessels willing to render assistance, and the few remaining operational NGO rescue ships, are vehemently upholding international law in the Mediterranean, and exposing the contemporary crimes of Europe. While safe and legal passage for all is yet to be achieved, border policy must not render the protection of human life negotiable.

The relocation lottery, as it was called by interview partners, presents itself as a humanitarian approach committed to upholding the rights of persons seeking protection in Europe. Yet rather than alleviating human suffering, it feeds into the inhumane logic of EU border management and migration deterrence, causing immense suffering in the process. Current relocation procedures consist of constant policing, discrimination, and an absolute lack of information for the people concerned, and neglect of their wishes and needs. Neither the EASO, nor the German delegation and government deliver what they promise in their "guidelines." Instead, the system produces chaos and operates in a presumed state of "emergency," when in fact the current number of people arriving at the European borders diminished to such small numbers that it is incomprehensible how such powerful states should not be able to handle or allow those people to arrive and to stay, where they want and for how long they want it.

Elected European leaders must listen to their civil societies holding them to account. This includes demands that any person forced to come to Europe on illegalized routes, is granted permission to stay. The promise to receive people needs to be accomplished and accompanied by the right to stay, without putting survivors through more interviewing processes and prolonging the insecurities concerning their futures. We demand that disembarkations are not subordinated to prior relocation agreements and that Europe puts an end to their racist deterrence practices, both at the external borders and within the EU.

THE CHALLENGES FACED BY PRIVATE SHIPS IN LARGE-SCALE RESCUE OPERATIONS AT SEA

Kiara Neri

1. Introduction

"Ships are now shutting off their radio in strategic locations to avoid being called in to help migrants in the Mediterranean".[1] These very serious allegations, formulated by Danish shipping following the *Maersk Etienne* saga in 2020, highlight the difficulties and challenges faced by the private sector when rescuing migrants at sea. At the request of the Maltese SAR services, on 4 August 2020, the Danish Flag Oil-tanker *Maersk Etienne* rescued 27 people on a small fishing vessel in distress off the coast of Tunisia. The tanker, its crew and the 27 persons rescued were stuck for 38 days at sea with no place to disembark the survivors. Eventually, on 11 September 2020 the *Maersk Etienne* was able to transfer them on the *Mare Jonio,* an NGO operated vessel. They reached Pozzallo (Sicily) on 13 September. This incident dramatically shows the difficulties faced by the private ships and the shipping industry when involved in a rescue operation in the context of migration.[2] The lack of political will of States to accept the disembarkation of migrants in their ports has serious practical, legal, and commercial consequences for the shipmasters their crews. Besides, most of the time, commercial ships are not equipped nor trained for conducting search and rescue missions making them both significantly expensive[3] and dangerous.

Nevertheless, the recourse to private ships in the framework of search and res-

[1] T. Kristiansen, "Migrant crisis has ships going off radio and rerouting near Malta", *Shippingwatch*, 9.9.2020, <https://shippingwatch.com/carriers/Tanker/article12401608.ece > (06/21).

[2] See L. Iussich and L. Maglic, "Search and rescue operations of Immigrants at sea: challenges for the crew of Merchant ships", *Journal of Maritime & Transportation Science*, 2019, pp. 45-58; R. L. Kilpatrick, Jr, "Why Evolving European SAR Policies threaten Merchant Shipping", *MarSafeLaw Journal* – Special Issue on the EU and Maritime Security, 2019, pp. 39-61; R. L. Kilpatrick Jr and A. Smith, "The International Legal Obligation to Rescue During Periods of Mass Migration at Sea: Navigating the Sovereign and Commercial Dimensions of a Mediterranean Crisis", *University of San Francisco Maritime Law Journal*, 2018, pp. 142-195; R. L. Kilpatrick Jr., "The "Refugee Clause" for Commercial Shipping Contracts: Why Allocation of Rescue Costs is Critical During Periods of Mass Migration at Sea", *Georgia Journal of International and Comparative Law*, 2018, pp. 403-446; K. S. Goddard, "Rescuing Refugees and Migrants at Sea: Some Commercial Shipping Implications", *International Journal of Maritime Law,* 2015, pp. 352-367; Robert D. Peltz, "Adrift at Sea – The duty of Passing Ships to rescue Standed Seafarers", *Tulane Maritime Law Journal*, 2014, pp. 363-388; F. G. Attard and R. L. Kilpatrick, Jr., "Reflections on the Maersk Etienne Standoff and its Ramifications for the Duty to Render Assistance at Sea", *EJIL Talks !*, 2020; F. G. Attard, *The Duty of the Shipmaster to Render Assistance at Sea under International Law*, Brill, Series: Queen Mary Studies in International Law, 2020.

[3] R. L. Kilpatrick Jr., "The "Refugee Clause" for Commercial Shipping Contracts", cit. *supra* note 2.

cue (SAR) operations is essential. As pointed out by the IMO itself, "SAR services throughout the world depend on ships at sea to assist persons in distress. It is impossible to arrange SAR services that depend totally upon dedicated shore-based rescue units to provide timely assistance to all persons in distress at sea."[4] As a result, the SAR services rely upon private ships to ensure the effectivity of their actions and save human lives.[5] For example, the Agreement between the United states of America and Mexico on Maritime Search and Rescue provides for the use of "other units":

> the United States Coast Guard makes use of available non-United States Coast Guard units in lieu of, or in addition to, United States Coast Guard units, in responding to existing or potential maritime distress situations. Such units may include, but are not limited to, […] *available merchant vessels*. Similarly, the Mexican Navy may use non-Navy resources for search and rescue. The United States Coast Guard and the Mexican Navy undertake, for purposes of this Agreement, to treat such units as falling under the terms of this agreement.[6]

Therefore, a significant number of private ships are involved in rescue operations every year. It is difficult to have clear reliable figures,[7] but the IMO estimates that a private ship is involved in one to ten SAR operations in the Mediterranean Sea between 2015 and 2017.[8] For instance, in 2016, almost 400 ships were diverted from their routes and around 120 were involved in the rescue of nearly 14,000 people.[9] The participation of the shipping industry and private shipping in general to the global objective of rescuing people in distress at sea is an old and well-implanted practice. International law is providing a well-established legal framework and contains an obligation, for the shipmasters to rescue persons in distress at sea. Most of the time, these operations are conducted without any problems, especially when the persons rescued are fellow seafarers, fishermen or tourists.

However, the legal framework organizing their participation is challenged during massive waves of migration at sea. The situation in the Mediterranean Sea since 2014 is, of course, significant, but it is not unprecedented. It had already been the case in the 1970s, during the Indochinese crisis when the establishment of com-

---

[4] IMO, MSC.167(78) - Guidelines on the Treatment of Persons Rescued at Sea, 5.1.

[5] See also International Convention on Maritime Search and Rescue (SAR), 27 April 1979, entered into force 22 June 1985, Annex, 2.1.9 "Parties having accepted responsibility to provide search and rescue services for a specified area shall use search and rescue units and *other available facilities* for providing assistance to a person who is, or appears to be, in distress at sea."

[6] Agreement between USA and Mexico on Maritime Search and Rescue, August 7, 1989, art. VII.

[7] "In general, it is estimated that different merchant ships are conducting rescue operations alone or in cooperation with public or navy ships in one third of all rescue operations at sea", L. Iussich and L. Maglic, "Search and rescue operations of Immigrants at sea", cit. *supra*, note 2, p. 49.

[8] IMO website: <https://www.imo.org/en/MediaCentre/PressBriefings/Pages/29-mixedmigration.aspx> (04/21).

[9] IMO website: <https://www.imo.org/en/MediaCentre/PressBriefings/Pages/29-mixedmigration.aspx > (04/21).

munist regimes in Vietnam, Laos and Cambodia led to an important wave of migration by sea to neighboring States. At the time, thousands of migrants were rescued by merchant ships, sometimes with no place to go as the neighboring States refused, one after the other, to allow disembarkation of survivors in their ports.[10] Since then, important instruments were adopted to prevent this situation from happening again, especially the 1979 Convention on search and rescue at sea (SAR Convention). Despite the undeniable enhancement of the legal framework, the issue of finding a place for disembarkation remains and is at the very center of the current challenges faced by the international merchant fleet.[11]

As a result, since 2015, the shipping industry has tried to raise the issue in the relevant international *fora* (IMO, ICS, etc.) advocating that the reliance on commercial shipping for SAR operations, especially in the framework of a migration crisis was not sustainable.[12] In the early years of the migration wave, private vessels performed approximately 25% of all maritime rescues in the Mediterranean Sea.[13] In the period from January 2014 to December 2015 in the Mediterranean Sea alone, "over 1,350 merchant vessels diverted from their intended voyage to rescue over 57,000 mixed migrants in danger of being lost at sea."[14] This proportion had decreased in the following years because of the increase of states and NGOs resources and the modification of the migration routes.[15] However, due to the seizure of most of the NGO vessels in European ports, the part of merchant ships is expected to rise again.[16]

It is clear -and undisputed- that private ships have obligations under the law of the sea in the framework of search and rescue operations (Section 21). But it is equally clear that the solicitation of the private fleet raises a significant number of

---

[10] UNGA, Report of the Secretary-General on Oceans and the Law of the Sea, 7 November 1979, UN Doc A/34/627. See also F. G. Attard, *The Duty of the Shipmaster to Render Assistance at Sea under International Law*, cit. *supra* note 2, p. 6 ; W. C. Robinson, "The Comprehensive Plan of Action for Indochinese Refugees, 1989–1997: Sharing the Burden and Passing the Buck", *Journal of Refugee Studies*, 2004, pp. 319–332; B. Wain, "The Indochina Refugee Crisis", *Foreign Affairs*, 1979, pp. 160–180.

[11] F. G. Attard and R. L. Kilpatrick, Jr., "Reflections on the Maersk Etienne Standoff and its Ramifications for the Duty to Render Assistance at Sea", cit. *supra* note 2.

[12] S. Trevisanut, "Search and rescue operations in the Mediterranean: Factor of cooperation or conflict". *International Journal of Marine and Coastal Law*, 2010, pp. 523-542.

[13] Strategic Note, "Irregular Migration via the Central Mediterranean", European Commission European Political Strategy Center, 22, 2 February 2017, <https://ec.europa.eu/epsc/sites/epsc/files/strategic_ note issue_22_0.pdf >(04/21), at 4, cited by Seline Trevisanut, "Search and rescue operations in the Mediterranean", cit. *supra* note 10.

[14] IMO, Assembly, Resolution A. 1093(29), Special recognition for merchant vessels and their crew involved in the rescue of mixed migrants at sea.

[15] Strategic Note, "Irregular Migration via the Central Mediterranean", putting forward that reliance on merchant ships has decreased since 2014 because SAR operations have moved closer to Libya and away from the main commercial routes. cited by Trevisanut, "Search and rescue operations in the Mediterranean", cit. *supra* note 12. See also Kilpatrick, Jr, "Why Evolving European SAR Policies threaten Merchant shipping", cit. *supra* note 2.

[16] See N. Madjidian, *Towards Subjectivity? The Civil Rescue Fleet and its Humanitarian Agency in the Mediterranean*, in this Volume.

challenges (Section 3) which are not properly addressed by the coastal States leading to detrimental consequences on the implementation of the obligation to render assistance at sea.

2. The Obligations of the Private Ships Under International Law of the Sea

Under the law of the sea private ships have the obligation to render assistance (Section 2.1). However, the implementation of this obligation is far from easy. Therefore, the IMO issued instructions, guidelines and manuals in order to assist private ships (Section 2.1).

2.1. Relevant Law of the Sea

The obligation to render assistance at sea. Under customary international law and law of the sea conventions,[17] every State has the obligation to require the master of a ship flying its flag whether private or public, to render assistance at sea to any person in distress or in danger of being lost. This obligation is a longstanding maritime tradition, provided for by art. 98 para.1 of UNCLOS, Regulation V33.1 of the SOLAS Convention and art. 2.1.10 of the Annex to the SAR Convention.

Content of the obligation. The obligation to render assistance at sea contains the obligation to rescue, namely "to retrieve persons in distress, provide for their initial medical or other needs, and deliver them to a place of safety."[18] It goes beyond the strict recovery of people. Under the SOLAS Convention, the SAR services of the coastal State as well as the Master of the ship in distress, have the right to requisition one or more private ships to render assistance.[19] The *requisition is mandatory* for the shipmaster of the private ship.

Therefore, at the request of the competent SAR services or the Master of the ship in distress, the Master of the private ship has the obligation to *proceed with all possible speed*[20] to the rescue of persons in distress and to inform, if possible and as soon as possible the ship in distress and the competent SAR services.

In addition, the SAR Convention[21] contains a *prohibition of discrimination* in the SAR operations. The obligation to render assistance has to be applied regardless

[17] Art. 11 of the Convention for the Unification of Certain Rules of Law Relating to Assistance and Salvage at Sea, 23 September 1910 ; art. 12para.1 of the Geneva Convention on the High Seas, 29 April 1958 ; art. 98, para.1 of the United Nations convention on the Law of the Sea (UNCLOS), 10 December 1982 ; art. 2.1.10 of the International Convention on Maritime Search and Rescue (SAR), 27 April 1979, entered into force 22 June 1985; International Convention for the Safety of Life at Sea (SOLAS), 1 November 1974, entered into force 25 May 1980, Regulation V33.2.

[18] IMO and ICAO International Aeronautical and Maritime Search and Rescue Manual (IAMSAR Manual), November 1999, Volume III, definition of « rescue », p. xviii.

[19] SOLAS Convention, Regulation V33.2.

[20] Art. 98 para.1b) UNCLOS and Regulation V33.1 SOLAS Convention.

[21] Art. 2.1.10 of the Annex. See also IMO, Resolution A.920(22) - Review of Safety Measures and Procedures for the Treatment of Persons Rescued at Sea.

of the nationality of the persons in distress, their status or the circumstances in which the persons are found. Therefore, international law expressly prohibits any distinction between the rescue of migrants and the operations concerning fellow seafarers or tourists. The obligation to render assistance also contains the obligation for the private retrieving ship to *treat the survivors humanely* while on board, i.e. meet their immediate needs and act consistently with the relevant IMO instruments, international agreements and long-standing humanitarian maritime traditions.[22]

Lastly, the retrieving ship shall *deliver the survivors to a place of safety*.[23] This obligation cannot be fulfilled by the private ships without the cooperation of neighboring coastal States and is very often at the very heart of the difficulties faced by the ships which have retrieved persons in distress at sea.

Exceptions. International law provides for two exceptions to the obligation to render assistance. The shipmaster is relieved from its obligation either if the rescue operation could cause serious danger to the ship, the crew or the passengers[24] or if another ship has been requested to proceed with the rescue or has already conducted it.[25] The first exception can be difficult to apply in practice, especially when security issues are at stake (see *infra*). In any case, if the shipmaster of the ship receiving the distress alert is unable to proceed with the assistance or finds it too dangerous for the ship or its crew, "the master must enter in the log-book the reason for failing to proceed to the assistance of the persons in distress, taking into account the recommendation of the Organization to inform the appropriate search and rescue service accordingly."[26]

As a result, the obligation to render assistance at sea applies to private ships. However, the implementation of this obligation is challenging for the shipmasters and the crews. To address these concerns and difficulties, the IMO produced a significant number of instruments containing guidance for the shipmasters of private ships involved in SAR operations.

2.2. Specific Instruments and Guidelines

The IMO issued an important number of resolutions and circulars containing guidelines[27] as well as a Manual[28] to assist shipmasters in the conduct of delicate

---

[22] IMO, MSC.167(78) - Guidelines on the Treatment of Persons Rescued at Sea and resolution A.920(22) - Review of Safety Measures and Procedures for the Treatment of Persons Rescued at Sea.

[23] Ibid.

[24] Art. 98 para.1 UNCLOS.

[25] Regulation V33.3 and 4 SOLAS Convention.

[26] Regulation V33.1 SOLAS Convention.

[27] *IMO Resolutions*: MSC.167(78) - Guidelines on the Treatment of Persons Rescued at Sea; MSC.346(91): Application of SOLAS Regulation III/17-1 to Ships to Which SOLAS Chapter III Does not Apply See Circular MSC.1/Circ.1447; A.919(22) - Acceptance and Implementation of the International Convention on Maritime Search and Rescue, 1979, as Amended; A.920(22) - Review of Safety Measures and Procedures for the Treatment of Persons Rescued at Sea; A.949(23) - Guidelines on Places of Refuge for Ships in Need of Assistance; A.1093(29) - Special recognition for merchant vessels involved in the rescue of mixed migrants at sea.

rescue operations. Following the *Tampa*[29] incident, the IMO Maritime Safety Committee (MSC) adopted amendments to chapter V of the SOLAS Convention and to chapters 2, 3 and 4 of the Annex to the SAR Convention. At the same time, the MSC adopted new guidelines on the treatment of the persons rescued at sea, especially Resolution MSC.167(78).[30] This Resolution provides for specific guidelines for shipmasters of retrieving ships. The first set of guidelines[31] is merely general and specifies that the shipmaster has to understand its obligation under international law (see above). The second set of guidelines is linked to the IMASAR Manual and asks for its correct implementation[32] and urges for the use of reporting systems established for the purpose of facilitating SAR operations.[33] Finally, the third set of guidelines is specifically dedicated to the coordination with the SAR services in charge of the location where the survivors were found. The Resolution MSC.167(78) asks the shipmasters to keep the competent SAR services informed of their actions in relation to the rescue[34] and to comply with the instructions of the State in charge of the SAR region where the survivors were recovered.[35] However,

---

IMO Circulars: COMSAR/Circ.22 - Guidance on Data Fields for SAR Databases; COMSAR/Circ.23 - Guidance for Central Alerting Posts (CAPs); COMSAR/Circ.31 - Guidance for Mass Rescue Operations; MSC/Circ.1073 - Directives for Maritime Rescue Co-ordination Centres (MRCCs) on Acts of Violence Against Ships; MSC/Circ.1079 - Guidelines for Preparing Plans for Co-operation Between SAR Services and Passenger Ships - Revision 1; MSC.1/Circ.1182 - Guide to Recovery Techniques - Revision 1; MSC.1/Circ.1183 - Guidelines on the Provision of External Support as an Aid to Incident Containment for SAR Authorities and Others Concerned; MSC.1/Circ.1186 - Guidelines on the Training of SAR Service Personnel Working in Major Incidents; MSC.1/Circ.1338 - Guidance to SAR Services in Relation to Requesting and Receiving Long-Range Identification and Tracking (LRIT) Information - Revision 1; MSC.1/Circ.1447 - Guidelines for the Development of Plans and Procedures for Recovery of Persons from the Water; MSC.5-Circ.13-Rev.3 - Information on Maritime Assistance Services (MAS).

[28] IMO and ICAO International Aeronautical and Maritime Search and Rescue Manual (IAMSAR Manual), November 1999.

[29] "On 24 August 2001 the *Palapa*, a small Indonesian fishing boat overloaded with 433 asylum-seekers from Afghanistan, became stranded in international waters about 140 kilometers north of Christmas Island.

The asylum-seekers were rescued by the Norwegian container ship, the *MV Tampa*, under direction by the Australian Maritime Safety Authority. […] Over 48 hours Rinnan made repeated requests to Australian authorities for assistance. These requests were acknowledged but not acted on, so Rinnan decided to enter Australian waters. The ship crossed the Australian maritime boundary on 29 August, shortly before midday. Australian authorities advised Rinnan that he was in 'flagrant breach' of the law, and the Government dispatched 45 Special Air Service (SAS) troops to board the ship and prevent it from sailing any closer to Christmas Island […]" Australian National Museum, <https://www.nma.gov.au/defining-moments/resources/tampa-affair#:~:text=In%20August%202001%20Australian%20troops,to%20bring%20them%20to%20Australia > (04/21). See also Jessica E. Tauman, "Rescued at Sea, but Nowhere to Go: the Cloudy Legal Waters of the Tampa Crisis", *Pacific Rim Law & Policy Journal*, 2002 p. 461.

[30] MSC.167(78) - Guidelines on the Treatment of Persons Rescued at Sea; MSC.346(91), 20 May 2004.

[31] Points 5.1.1 and 5.1.2 of Resolution MSC.167(78).

[32] Ibid., point 5.1.3.

[33] Ibid., point 5.2.

[34] Ibid., point 5.1.5.

[35] Ibid., point 5.1.7.

two difficulties may arise and are addressed by the guidelines: first, the situation where the area is not covered by a designated SAR service or where they are not reachable. In that case, the IMO recommends the shipmaster to contact another RCC or any other Government that may be able to assist.[36] Second, and this is a crucial point, the shipmaster should "seek to ensure that survivors are not disembarked to a place where their safety would be further jeopardized."[37] The Resolution is, however, silent on how to articulate the obligation to obey the instructions of the State responsible for the SAR zone and the prohibition to disembark the survivors in an "unsafe" place. These conflicting obligations have generated difficult situations in the past, especially for NGOs when asked to disembark survivors in Libya.[38]

Besides, the IAMSAR Manual, was adopted in 1999 by the IMO, to replace both the 1971 Merchant Ship Search and Rescue Manual (MERSAR) and the 1978 Search and Rescue Manual (IMOSAR). The 3-volume Manual is a common aviation and maritime approach to organizing and providing search and rescue (SAR) services. The purpose of the Manual is to provide guidance to the master of any ship that might be called upon to participate in search and rescue operations, whether public or private. Although applicable to private ships, the Manual is mainly oriented towards SAR units. However, volume III (Mobile Facilities - SAR units, civil aircraft and vessels) contains relevant guidelines for private, including procedures to prepare for a SAR mission, but also on-scene coordination, on board organization, and security and safety requirements. The Manual also calls upon private ships to adopt a reporting system and to send regular reports to the authority operating a ship reporting system for SAR and other safety-related services. These reporting systems, such as *Amver* are essential to identify vessels in the vicinity of a distress situation, to contact the vessels, to reduce the response time and avoid calling numerous ships for help, but also to get information about the vessel such as the presence of a doctor on board.[39]

The procedures for responding to emergencies, including rescue operations at sea can also be found in the International Safety Management (ISM) Code,[40] the International Ship and Port Facility (ISPS) Code,[41] the International Medical Guide

[36] Ibid., point 5.1.4.

[37] Ibid., point 5.1.6.

[38] See the decision of the Italian Tribunal of Ragusa, 16 April 2018, RG n. 1182/2018: the rescuing NGO (Open Arms) is not only responsible for the search and rescue operations but has a say in the assessment of the safety of disembarkation in line with the principle of non-refoulement. The Tribunal ordered the immediate release of the Open Arms ship considering that it conducted a reasonable assessment of the situation given that Libya could not be considered a place of safety and that Italy had already communicated an available one. For a short comment, see V. Passalacqua, "The 'Open Arms' case: Reconciling the notion of 'place of safety' with the human rights of migrants", *Ejil Talks!* May 21, 2018 or C. Focarelli, *International Law*, Edward Elgar Publishing 2019, 138.6.

[39] IAMSAR Manual, Volume III Section 1, 1-3 and 1-4.

[40] The International Safety Management (ISM) Code was adopted by IMO's MSC in 1993 by resolution A.741(18) and entered into force, on 1 July 1998.

[41] The International Ship and Port Facility (ISPS) Code is part of the SOLAS Convention (chapter XI-2). It entered into force on 1 July 2004.

for Ships[42] and the Guide to Ship Sanitation.[43] These instruments require the Company and the ship to have a specific plan in case of an emergency: the company's Safety Management System (SMS) and the Ship Security Plan (SSP).

Taken together, these IMO instruments, give practical instructions and recall the legal and operational framework applicable SAR operations at sea. However, the number of instruments, their complexity, and their lack of relevance to large-scale rescue missions have led the international shipping industry to issue its own guidelines, both trying to identify, in all these instruments, the principles applicable in the specific situation of a rescue of a large number of migrants and to take into account and address the issues and challenges faced by the shipping industry.[44] The ICS *Large-Scale Rescue Operations at Sea Guidance on Ensuring the Safety and Security of Seafarers and Rescued Persons* gives guidance on how to best prepare the ship and the crew for a possible large-scale rescue operation (plans and procedures, training, life-saving equipment, food and water supplies, etc.). It also contains guidelines on how to conduct the rescue operation itself (answering the distress call, assessing and monitoring the situation, embarkation of rescued persons) and on how to manage the survivors once onboard (security of the crew and the ship, accommodation, infectious diseases, sanitation and hygiene, medical care). Lastly, the ICS guidance addresses the issue of disembarkation of survivors, recalling that the responsibility of finding a safe location lies with the authorities in charge of the SAR zone in which the rescue took place. But the ICS guidance goes beyond legal issues and gives practical advice on the management of personal effects, post disembarkation actions (search for stowaways, effective cleaning) or crew welfare considerations (stress, fatigue, psychological impact, etc.).

Despite all these instruments and guidelines, conducting a SAR operation remains very challenging for a private vessel.

3. The Challenges Faced by the Private Sector

The main – but not only- challenges faced by the shipmaster of a private vessel and its crew when conducting a large-scale rescue operation are the lack of preparedness (2.1), the lack of coordination for disembarkation (2.2), and the management of security, safety and sanitary risks (2.3).

---

[42] The International Medical Guide for Ships was published by the World Health Organization in 1967 <https://apps.who.int/iris/bitstream/handle/10665/43814/9789240682313_eng.pdf;jsessionid=D6291EC5BAFFC7E3FC562BFBAB272648?sequence=1> (04/21 – Third edition).

[43] The Guide to Ship Sanitation was published by the World Health Organization in 1967 <https://apps.who.int/iris/bitstream/handle/10665/43193/9789241546690_eng.pdf?sequence=1> (04/21- Third edition).

[44] ICS, *Large Scale Rescue Operations at Sea Guidance on Ensuring the Safety and Security of Seafarers and Rescued Persons*, second Edition 2015, <https://www.ics-shipping.org/wp-content/uploads/2015/01/large-scale-rescue-at-sea-min.pdf.>

3.1. The lack of preparedness

The first challenge faced by private ships is the lack of preparedness, including the lack of training of the crew, but also the lack of preparedness of the ship itself in terms of equipment and procedures.

Lack of training. The IMSAR Manual recalls the need for Masters and officers of merchant ships to be properly trained.[45] The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STWC)[46] states that every seafarer must receive basic safety training (Regulation A-VI/1, chapter 2 of STWC), including communications; control of fatigue; teamwork; and marine environmental issues. The basic knowledge on how to conduct a rescue operation is thus not included in the requirements for the crew. As a result, very few crew members,[47] - if any - are trained for this particular mission. Section A-VI/2 of the Convention is dedicated to mandatory minimum requirements for the issue of certificates of proficiency in survival craft, rescue boats and fast rescue boats. It is mainly dedicated to the security of the ship itself and the ways of escaping it if needed, however, being trained with towing procedures using a rescue boat is essential to conduct a large-scale rescue operation.[48] In the framework of the STWC Convention, the model courses 1.23 and 1.24 do recommend one hour of training, which is generally not performed.[49]

Lack of equipment and precise security procedures on board the ship. The applicable procedures are supposed to be planned by the Ships Security plans.[50] However, a large number of small private ships do not have such a Plan on board. Besides, the equipment of the ship, regardless of its size is often not sufficient to conduct a large scale SAR operation, especially in terms of security, sanitation, food and water supplies. The International Chamber of Shipping's guide on *Large-Scale rescue operation at sea* can provide for practical solutions on these particular issues.

3.2. The lack of coordination for disembarkation

"The obligation of the master to render assistance should complement the corresponding obligation of IMO Member Governments to co-ordinate and co-operate

---

[45] IAMSAR Manual, Volume III, 2.63.

[46] International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STWC), 7 July 1978, entered into force 28 April 1984.

[47] Shipmasters, Security officers, and every person designated to provide medical first aid on board a vessel are supposed to receive appropriate training (STWC Convention).

[48] See *infra*.

[49] L. Iussich and L. Maglic, "Search and rescue operations of Immigrants at sea", cit. *supra* note 2, p. 55.

[50] Such a Plan is mandatory for the ships in international trade according to the ISPS Code.

in relieving the master of the responsibility to provide follow-up care of survivors and to deliver the persons retrieved at sea to a place of safety."[51] Resolution MSC.167(78) could not be clearer: in order for the SAR system to work properly and fulfill its mission of saving human lives at sea, both shipmasters and States need to comply with their obligations, especially in terms of disembarkation.

The SAR Convention is based on a network of search and rescue regions, for which each Party is responsible. In terms of disembarkation, the Convention obliges the State responsible for the SAR zone to find a safe location as soon as reasonably possible. Indeed, the 2004 amendments provide:

> The Party responsible for the search and rescue region in which such assistance is rendered shall exercise primary responsibility for ensuring such co-ordination and co-operation occurs, so that survivors assisted are disembarked from the assisting ship and delivered to a place of safety, taking into account the particular circumstances of the case and guidelines developed by the Organization. In these cases, the relevant Parties shall arrange for such disembarkation to be effected as soon as reasonably practicable.[52]

In addition, the Convention aims at ensuring that masters of ships providing assistance by embarking persons in distress at sea are released from their obligations with minimum further deviation from the vessel's initial route. This provision is extremely important if a merchant ship is involved in the rescue mission.

As a result, the State responsible for the SAR zone has the primary responsibility to find a safe location, with minimum further deviation for the merchant ship.[53] However, the SAR Convention does not require that this location be its own territory or port. Besides, this obligation does not exist either for the flag State or for the rescuing ships. In 2009 the IMO Facilitation Committee promulgated a document entitled 'Principles Relating to Administrative Procedures for Disembarking Persons Rescued at Sea' providing further guidance on the issue.

> If disembarkation from the rescuing ship cannot be arranged swiftly elsewhere, the Government responsible for the SAR area should accept the disembarkation of the persons rescued in accordance with immigration laws and regulations of each Member State into a place of safety under its control in which the persons rescued can have timely access to post rescue support.[54]

---

[51] Resolution MSC.167(78), cit. note 27.

[52] Resolution MSC.155(78), Amendments to the international convention on maritime search and rescue, 1979, 20 May 2004. Malta has not accepted these amendments.

[53] See for instance K. Gombeer and M. Fink, "Non-Governmental Organisations and Search and Rescue at Sea", *Marsafelaw Journal*, 4/2018, p. 1-25; J. van Berckel Smit, "Taking Onboard the Issue of Disembarkation. The Mediterranean Need for Responsibility-Sharing after the Malta Declaration", *European Journal of Migration and Law*, 2020, pp. 492-517 or K. Neri, "The Missing Obligation to Disembark Persons Rescued at Sea", *Italian Yearbook of International Law*, 2018, pp. 47-62.

[54] IMO, Principles Relating to Administrative Procedures for Disembarking Persons Rescued at Sea FAL.3/Circ.194 (22 January 2009).

This is only a recommendation. Therefore, situations in which people rescued at sea have had to wait off the coasts of Australia, Italy or Malta for several days or weeks before being told where to disembark is certainly a violation of the obligation to provide a safe location "as soon as reasonably possible" but not a violation of the "missing" obligation to grant access to rescued persons in a State's ports.[55]

To prevent these issues, Resolution MSC.167(78) calls upon Flag and coastal States to "have effective arrangements in place for timely assistance to shipmasters in relieving them of persons recovered by ships at sea".[56] Indeed, the lack of coordination between the Mediterranean States has severe consequences on both the private ship participating to a SAR mission and the survivors, as highlighted dramatically by the *CapAnamur*,[57] *Pinar*[58] or *Maersk Etienne* incidents. In the *Pinar* case for instance, a Turkish merchant vessel rescued 153 persons off the Coast of Lampedusa, in the Maltese SAR zone. Both Italy and Malta then denied the *Pinar* access to their territorial waters and their ports.[59]

European States are still unable to adopt a clear common strategy for disembarkation. Yet, it is precisely to find a solution to disembarkation issues that the SAR Convention itself and its 2004 amendments were adopted, following respectively the South-East Asia crisis and the *Tampa* incident off the coast of Australia. As a reminder, when the neighboring countries of former Indochina decided, in the late 1970s to close their frontiers and not accept disembarkation of migrants anymore, merchant ships consequently failed to perform rescue operations leading to a massive humanitarian crisis.[60] In the 1979 the UNHCR was already raising the issue of disembarkation in the first port of call or resettlement guarantees by flag States.[61]

---

[55] K. Neri, "The Missing Obligation to Disembark Persons Rescued at Sea", cit. *supra* note 53.

[56] Resolution MSC.167(78), cit. *supra* note 27.

[57] S. Trevisanut, « Le Cap Anamur. Profiles de droit international et de droit de la mer », *Annuaire du Droit de la Mer*, 2004, pp. 49-64.

[58] See "Pinar. Alta tensione con Malta, Larmatore: "Situazione tragica"," *La Repubblica*, 18 April 2009; "I migranti del Pinar in Sicilia," in *Corriere della Sera*, 19 April 2009; "Maroni Claims Malta Sent 40,000 Migrants to Italy," *Times of Malta*, 21 April 2009.

[59] S. Trevisanut, "Search and rescue operations in the Mediterranean", cit. supra note 12. See also R. L. Kilpatrick "Why Evolving European SAR Policies threaten Merchant Shipping", cit. *supra*, note 2, p. 53: "On the one hand, they are morally and legally obliged to respond to requests for assistance at sea and to coordinate with state RCCs to deliver survivors to a place of safety. If they fail to comply with these obligations, people in need of assistance could die, and the shipmaster could also face criminal prosecution. But on the other hand, if merchant ship operators do honour their legal obligations, they depend on states to quickly determine a safe place for disembarkation. If states abrogate these responsibilities, private shipmasters cannot fulfil their own duties without putting lives at risk and suffering substantial economic harm."

[60] UN General Assembly, Meeting on Refugees and Displaced Persons in South-East Asia, convened by the Secretary-General of the United Nations at Geneva, on 20 and 21 July 1979, and subsequent developments: Report of the Secretary-General, 7 November 1979, A/34/627 and *Opening Statement by Mr. Poul Hartling, United Nations High Commissioner for Refugees, at the Consultative Meeting with Interested Governments on Refugees and Displaced Persons in South-East Asia, Geneva,* 11 December 1978, <https://www.unhcr.org/admin/hcspeeches/3ae68fce4c/opening-statement-mr-poul-hartling-united-nations-high-commissioner-refugees.html >

[61] Report of the Secretary-General, 7 November 1979, A/34/627 para. 35.

The plan of action suggested by the Secretary General included the following calls to both private ships and governments:

> (q) Many thousands of boat cases have perished at sea. Those in distress *must be rescued* before they die and *masters of vessels in the area must scrupulously observe the law of the sea in this regard.* […]
> (r) Within the framework of the over-all solutions envisaged, *Governments of the first port of call must allow the disembarkation* of all those rescued. […][62]

More than 40 years later, and despite the adoption of the SAR Convention and its amendments, the issue is still unresolved.

3.3. Security, safety and sanitary issues

A modern merchant vessel is unsuited to perform SAR operation in general, especially when they involve a large number of persons at the same time, significantly more numerous than the crew. For instance, in October 2016, the *Okyroe*, an oil-tanker with a crew of 21 seafarers rescued over 1500 people from rubber dinghies.[63] They offer inadequate shelter, medical care or sanitation, and have limited food and water supplies on board.

But beyond living conditions onboard, a SAR operation is also a great challenge for the crew in terms of security and safety.

The risks linked to the recovery. The recovery operation in itself is very dangerous, both because of technical issues and because of human risks. For instance, in April 2015 a Portuguese-flagged container vessel, the *M/V King Jacob* responded to a distress call of a migrant vessel carrying more than 800 people. During the rescue operation, the migrant vessel collided with the *M/V King Jacob* causing the death of hundreds of people.[64]

Two main methods can be used for the recovery, both delicate. The *ship to ship* method: berthing the vessel in distress alongside the merchant ship and use the ships gangway. This method is only possible with good weather conditions. If the first method is not practicable, the crew will use the *rescue boat* method: either use a rescue boat to tow the distress vessel (or life raft) or transfer people in smaller groups to the rescue boat. Both techniques imply serious risks and are delicate, but the use of a rescue boat is especially tricky because it is -in general- significantly smaller and lighter that the vessel in distress and therefore vulnerable in case of panic reactions of desperate people jumping to the rescue boat.

The risks onboard. Security issues can also arise if criminals are present among

---

[62] Ibid., para. 37q) and r)

[63] IMO Media Center: <https://www.imo.org/en/MediaCentre/PressBriefings/Pages/29-mixedmigration.aspx> (04/21).

[64] M. Mesco, "How Migrants' Ordeal Turned Into Tragedy at Sea", *The Wall Street Journal*, 21 April 2015, <https://www.wsj.com/articles/captain-error-caused-migrant-ship-to-capsize-investigators-say-1429614614> (04/21).

the persons in distress. This possibility is often put forward by the shipping industry[65] or some scholars.[66] However, it is so seldom that the practice is close to zero. To address this risk, some are advocating for the information of the persons before boarding the ship that weapons or drugs are not allowed onboard, for a rough personal search when entering the ship and for a systematic use of hand metal detectors to search the survivors for weapons.[67]

In practice, security issues and acts of violence arise from the despair of the survivors, for instance when no place for disembarkation can be found quickly or when they realize that they are being returned to the country of departure. For instance, when the survivors on board the *Elhiblu 1* realized that the vessel which just had rescued them was heading back to Libya, they used violence to force the shipmaster and the crew to change their route and to take them to Malta. On 28 March 2019, the Maltese forces stopped the vessel before entering the Maltese waters and took control of the ship. Three young men were arrested and are prosecuted in Malta. Similarly, in July 2018, it was reported that the migrants rescued by an Italian-fagged platform supply vessel, the *Vos Thalassa*, threatened the crew when they discovered that they were being returned to Libya.[68] The Italian coast guard intervened and transferred the migrants onto a coast guard vessel at sea.[69]

Sanitary issues. The Master of the rescuing vessel also need to take into consideration the risks for the crew in terms of health, both physiological and psychological. The more direct risk arises when one of the survivors suffers from an infectious disease. The Covid-19 crisis has aggravated the situation. After a year of pandemic, the International Maritime rescue Federation issued guidelines[70] on how to proceed with a rescue operation in this context. The key priorities are to minimize the risk of infection for the crew, while continue to provide effective SAR and lifesaving services. The Guidelines are intended to SAR services and not private ships, but they contain relevant general principles to be applied in any SAR operation during a

---

[65] A. Adamopoulos, "Shipowners Worried for Crew After Vessel Hijacked by Migrants", *Lloyd's List*, 28 March 2019 (04/21); L. Tondo and J. Rankin, "Rescued Migrants Hijack Merchant Ship Off Libya", *The Guardian*, 27 March 2019 (04/21).

[66] L. Iussich and L. Maglic, "Search and rescue operations of Immigrants at sea", cit. supra note 2, p. 55.

[67] Ibid., p. 55.

[68] T. Kington and D. Charter, "Mutinous migrants threaten to kill Italian crew after rescue", *The Times*, 11 July 2018 (04/21). Two men were prosecuted for violent and intimidating actions against the crew of the *Vos Thalassa*. However, the Tribunal of Trapani acquitted both defendants on the grounds of self-defence (well-founded fear of return to Libya). Tribunal of Trapani, Office of the Judge for Preliminary Investigations (Piero Grillo), 23-05-2019. To read a summary of the decision: <https://www.asylumlawdatabase.eu/en/case-law/italy-tribunal-trapani-office-judge-preliminary-investigations-piero-grillo#content>.

[69] Similarly, in November 2018, 77 survivors refused to leave a Panamanian-flagged cargo ship, the *Nivin*, when arriving in Misrata (Libya) after being rescued off the Libyan coast: "Rescued migrants refuse to leave ship taking them to Libya", BBC, 18 November 2018 (accessed April 2021).

[70] International Maritime Rescue Federation, Pandemic Response Guidance for Maritime Search and Rescue Organisations February 2021. <https://www.international-maritime-rescue.org/Handlers/Download.ashx?IDMF=7fee8ef0-5c28-4fc7-b365-6312000dec1f >(04/21).

pandemic. For instance, drafting a response plan for suspected infection containing the identification of a room/area where the person can be safely isolated and monitored, the requirement to deep clean any areas which the infected person has been in, and indications on who should be contacted for assistance and how to call for help.

4. Conclusions

European policies on migration by sea, especially the lack of a clear rule regarding disembarkation are putting the shipping industry in an inextricable situation and threatening the life-saving mission of SAR. It is doubtless that most of the shipmasters continue to take their part in the implementation of the obligation to render assistance, sometimes even with bravery.[71] However, NGOs and seafarers have also pointed out a rare but growing tendency for merchant vessels to avoid getting involved in rescues altogether.[72]

[71] IMO, Assembly, resolution A.1093(29) Special recognition for merchant vessels and their crew involved in the rescue of mixed migrants at sea. the IMO Assembly delivers certificates for the bravery, professionalism and compassion displayed by crews of merchant vessels in the rescue of migrants at sea. For instance, the IMO awarded the Captain and the crew of the *Okyroe*, who rescued 1,536 people from rubber dinghies in 2016.

[72] R. L. Kilpatrick, Jr, "Why Evolving European SAR Policies threaten Merchant Shipping", cit. *supra* note 2. See also: F. D'Emilio, "Aid Groups: Ships Not Willing to Save Mediterranean Migrants", *Associated Press*, 12 August 2018 (04/21); T. Kington, "Captains 'Hide Ship Locations in Med to Avoid Migrant Rescues", *The Times*, 1 August 2018 (04/21).

IL RUOLO DEGLI ATTORI NON STATALI NELLA MACEDONIA DEL NORD NELLA PROMOZIONE DELLA SICUREZZA UMANA DURANTE LA CRISI MIGRATORIA DEL 2015/2016

Ana Nikodinovska Krstevska

1. La crisi migratoria del 2015-2016 e le minacce alla sicurezza umana dei migranti e rifugiati nella Macedonia del Nord

I flussi migratori del 2015-2016, [1] che hanno interessato l'Unione Europea e i paesi lungo la rotta balcanica, hanno trovato impreparati gli Stati coinvolti. Ciò ha determinato una crisi nei sistemi di asilo e di gestione dei flussi migratori nei vari Stati,[2] i quali hanno iniziato ad adottare azioni e politiche migratorie molto spesso in violazione dei diritti umani di migranti e richiedenti asilo.[3]

Con specifico riferimento alla Macedonia del Nord, il quadro legislativo allora vigente non riconosceva ai migranti il diritto di transitare sul territorio macedone.[4] In materia di asilo e migrazione,[5] ai migranti irregolari era consentito solamente presentare richiesta di asilo nel paese. Di conseguenza, coloro che venivano fermati nel territorio nazionale privi della documentazione richiesta venivano considerati

[1] I dati statistici dell'IOM riportano che solo durante il 2015 il numero dei migranti che è entrato nell'Europa ammonta a 1.046,599 migranti. *International Organization of Migration, Mixed Migration Flows in the Mediterranean and Beyond, Compilation of available data and information (reporting period 2015)* <https://www.iom.int/sites/default/files/situation_reports/file/Mixed-Flows-Mediterranean-and-Beyond-Compilation-Overview-2015.pdf>, (03/21).

[2] *European Commission*, Towards a reform of the Common European Asylum System and Enhancing Legal Avenues to Europe Brussels, COM(2016) 197 final, 6.4.2016,<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex%3A52016DC0197>, (03/21).

[3] S. Grigonis, "EU in the face of migrant crisis: Reasons for ineffective human rights protection", *International Comparative Jurisprudence*, December 2016, pp. 93-98, <https://doi.org/10.1016/j.icj.-2017.01.003>, (04/21).

[4] S. Selo Sabić and S. Borić, "At the Gate of Europe: A Report on Refugees on the Western Balkan Route", Fridrich Ebert Stiftug, Zagreb, January 2016, p. 6 <https://www.researchgate.net/publication/320452040_At_the_Gate_of_Europe-_A_Report_on_Refugees_on_the_Western_Balkan_Route >, (03/21).

[5] Si riferisce all'art. 17 della Legge sull'asilo e protezione temporanea (LAPT) che regola l'ingresso e il soggiorno irregolare nella Repubblica di Macedonia (Gazzetta Ufficiale della Repubblica di Macedonia N. 49/2003 ed emendamenti consecutivi N.66/2007, 142/2008, 146/2009, 166/2012 e 27/2013); art. 100 e 101 della Legge sugli stranieri che riguardano il soggiorno irregolare nella Repubblica di Macedonia e l'espulsione e deportazione forzata di stranieri dal territorio nazionale (Gazzetta Ufficiale della Repubblica di Macedonia N. 35/2006 e emendamenti seguenti N. 66/2007, 117/2008, 92/2009, 156/2010, 158/2011, 84/2012 e 147/2013); nonché le regole previste dall' art. 5 par. 2 dell'Acquis di Schengen sulle condizioni di ingresso nel territorio delle parti contraenti della Convenzione di Schengen, riguardo i quali la Macedonia del Nord si adegua nel processo di integrazione europea.

illegali e dunque soggetti a deportazione.[6] La legislazione nazionale vigente, pertanto, non teneva minimamente conto del fatto che i migranti transitavano sul territorio macedone al solo fine di chiedere asilo in altri paesi europei. Tale situazione sfavorevole costringeva i migranti a intraprendere varie vie illegali per attraversare il paese, appoggiandosi spesso ai trafficanti, proseguendo il tragitto da soli.[7] Se decidevano di rivolgersi ai trafficanti, spesso venivano derubati, violentati anche sessualmente o rapiti per estorcere denaro ai familiari; se, invece, proseguivano da soli lungo la linea ferroviaria rischiavano di rimanere feriti o di perdere la vita in incidenti ferroviari. In alcuni casi, i migranti venivano catturati dalla polizia insieme ai loro trafficanti e detenuti arbitrariamente in un centro di detenzione statale, sovraffollato, con scarse condizioni igieniche e libertà di movimento ridotte a minimo. Spesso accadeva che ufficiali di polizia praticassero violenza sui detenuti.[8] Comunque sia, qualsiasi strada scegliessero, i migranti finivano per essere deprivati dei loro diritti di base ivi compresi accesso ad aiuti umanitari, assistenza medica e altro. Quindi la loro sicurezza umana, rappresentata dal diritto delle persone a vivere in libertà e dignità, libere dalla povertà e dalla disperazione, è stata minacciata, nonostante si trattasse di migranti e rifugiati. Tutti gli individui, in particolare le persone vulnerabili, hanno diritto alla libertà dal bisogno, con pari opportunità di godere di tutti i loro diritti e sviluppare pienamente il loro potenziale umano, in base a quanto previsto dall'art. 3 par. a della Risoluzione 66-290 dell'Assemblea Generale delle Nazioni Unite.

In questo scenario, gli unici attori ad essersi messi dalla parte dei migranti e rifugiati e ad aver prestato soccorso e aiuto, proponendo cambiamenti sia nel campo legislativo sia nelle pratiche di dare assistenza ai migranti al confine e anche all'interno dello stato, sono state le organizzazioni non governative sia nazionali che internazionali.[9] Infatti, le ONG nazionali come LEGIS, Macedonian Young Lawyers Association, La Strada e altri insieme ad UNHCR e Amnesty International, sono state le prime a prestare soccorso e aiuto a migranti e rifugiati, nonché ad avanzare proposte concrete circa la modifica della Legge sull'asilo e sulla protezione temporanea che avrebbero consentito il diritto di transito nella Macedonia del Nord. Inoltre, l'ONG LEGIS insieme a Human Rights Watch sono state le prime a

[6] Z. Drangovski, "Analytical report Lessons learned from the 2015-2016 migration situation in the Western Balkan region", *'Prague Process: Dialogue, Analyses and Training in Action' Initiative, International Center for Migration Policy Development*, May 2019, <https://www.pragueprocess.eu/en/migration-observatory/publications/document?id=180>, (04/21).

[7] M. Smailovikj, "The Humanitarian aspect of the refugee crisis" in A. Nikodinovska Krstevska and B. Tushevska Gavrilovikj, *Migration at sea: International Legal Perspectives and Regional Approaches*, Giannini Editore, Napoli, 2015, pp. 79-96, <http://www.isgi.cnr.it/wp-content/uploads/2017/10/Migration-at-sea.-International-Law-Perspectives-and-Regional-Approaches.pdf>, (04/21).

[8] C. Veigel, O. Koshevaliska, B. Tushevska Gavrilovikj and A.Nikodinovska Krstevska, "The 'Gazi Baba' Reception Center for Foreigners in Macedonia: migrants caught at the crossroad between hypocrisy and complying with the rule of law", *The International Journal of Human Rights*, December 21, 2016, pp. 103-119, < https://doi.org/10.1080/13642987.2016.1257987>, (04/21)

[9] Smailovikj, *The Humanitarian aspect of the refugee crisis*, cit. *supra* nota 7, pp. 77 – 82.

denunciare la detenzione arbitraria dei migranti e rifugiati nel Centro di accoglienza per stranieri 'Gazi Baba' a Skopje.

2. Le migrazioni e lo spazio marittimo

Prima di entrare nel vivo dell'argomentazione, è doveroso, allo scopo di questa ricerca, tracciare il collegamento tra le migrazioni e lo spazio marittimo per avere idee più chiare sul collegamento tra le migrazioni e la sicurezza umana nello spazio marittimo. Nella parte introduttiva, Giorgia Bevilacqua asserisce che nell'antichità i mari e gli oceani erano considerati spazi completamente aperti e liberi, regolati dal principio della libertà dei mari e che l'unico limite a questo principio legale era rappresentato dal rispetto per la libertà degli altri. Il collegamento tra la predetta asserzione con la libertà di movimento e la libertà di navigare sui mari, riconduce al principio che viene sancito nella Convenzione sul diritto del mare (1982),[10] cioè quello del passaggio inoffensivo, definito come la possibilità delle navi di tutti gli Stati, costieri o privi di litorale, di godere del diritto di passaggio inoffensivo attraverso il mare territoriale (art. 17, 18 e 19). Anche se la Convenzione sul diritto del mare restringe il diritto di navigare liberamente con l'introduzione della sovranità nazionale nei mari,[11] comunque esso rimane garantito nelle zone di alto mare e tenendo conto anche dell'universalità della Convenzione, esso ormai ha assunto un carattere imperativo. Di conseguenza, se lo scopo di applicazione del principio viene spostato dallo spazio marittimo allo spazio terrestre, esso si identifica con la libertà di movimento e di migrazione, e quindi come tale lo troviamo sancito nell'art. 13 della Dichiarazione Universale dei diritti umani (1948),[12] come diritto di movimento e residenza all'interno dei confini dello stato (par. 1) e anche come diritto di lasciare qualsiasi paese, incluso il proprio, e di ritornare nel proprio paese (par. 2). Similmente allo spazio marittimo dove vengono imposti dei limiti di sovranità nazionale sui mari, lo stesso accade anche nello spazio terrestre dove gli Stati hanno introdotto dei confini entro i quali esercitano la loro potestà sovrana, e di conseguenza anche qui il diritto di spostarsi liberamente viene circoscritto con regimi di visto, controlli statali, politiche protezionistiche e tant'altro. Un'eccezione a queste restrizioni proviene proprio dalla norma sancita nella Convenzione relativa allo status dei rifugiati (1951)[13] e dal Protocollo aggiuntivo (1967)[14] relativi al principio di *non-refoulement* noto anche come divieto di espulsione e di rinvio al confine (art.

[10] Convenzione delle Nazioni Unite sul diritto del mare, 10 dicembre 1982, entrata in vigore 16 novembre 1994.

[11] Vedi parte II della Convenzione sul diritto del mare relativa al mare territoriale e zona contigua.

[12] Dichiarazione universale dei diritti umani, 10 dicembre 1948, Assemblea Generale delle Nazioni Unite.

[13] Convenzione relativa allo status dei rifugiati, 28 luglio 1951, Ginevra, entrata in vigore 22 aprile 1954.

[14] Protocollo relativo allo status dei rifugiati, 31 gennaio 1967, New York, entrato in vigore 4 ottobre 1967.

33 dalla suddetta Convenzione). Visto come un principio ormai di carattere ius cogens, il *non-refoulement* prevede che nessuno possa espellere o rimpatriare ('refouler') un rifugiato contro la sua volontà, in qualsiasi modo, in un territorio dove l'individuo teme minacce alla vita o alla libertà.

Quindi, se prendiamo in considerazione la definizione che viene data al concetto di libertà, vista come capacità del soggetto di agire (o di non agire) senza costrizioni o impedimenti esterni e di autodeterminarsi scegliendo autonomamente i fini e i mezzi atti a conseguirli,[15] e la mettiamo in connessione con il diritto di movimento come libertà assoluta, considerando il suo carattere imperativo, ne consegue che il diritto di movimento previsto sia dall'art. 13 della Dichiarazione universale dei diritti umani sia dalla Convenzione sui rifugiati, è privo di limitazioni sia temporali sia spaziali. In altre parole, l'idea di migrare o di spostarsi verso altri paesi è un diritto che non conosce confini e che dipende soltanto dalla volontà della persona. Trasferito questo concetto nel terreno delle migrazioni, ne consegue che la libertà di movimento dei migranti e rifugiati, garantita dalle norme internazionali e consuetudinarie, dovrà essere assicurata fino alla destinazione prescelta dell'individuo, cioè fino al paese prescelto dove l'individuo vuole chiedere asilo. Ciò significa che tutto lo spazio sia marittimo che terrestre, in questo specifico contesto di migrazioni, dovrà essere interpretato come uno spazio unico, illimitato. Questo in virtù della libertà di movimento sancita nella Dichiarazione universale dei diritti umani e della libertà sui mari e cioè il diritto di passaggio inoffensivo sancito nella Convenzione sul diritto del mare. Di conseguenza, i migranti e rifugiati che abbiano intrapreso il loro viaggio dall' Africa o dall'Asia e tramite il mare siano arrivati nella Macedonia del Nord o in altri paesi vicini, tenendo presente però che la loro destinazione finale non era la Macedonia del Nord bensì altri paesi dell'Occidente Europeo, allora si presuppone che il loro diritto di movimento e di spostarsi non fosse esaurito interamente nella Macedonia del Nord, ma rimane in vigore finché non arrivino alla destinazione prescelta. In linea con questo ragionamento, tratteremo il percorso migratorio come passaggio tramite un unico spazio che comprende sia lo spazio marittimo sia quello terrestre.

3. Sul concetto della sicurezza umana, delle migrazioni e dello spazio marittimo

Riguardo al concetto di sicurezza umana, nel Rapporto sullo sviluppo umano delle Nazioni Unite[16] così come lo ricorda nell'introduzione Giorgia Bevilacqua, viene stabilito che le nuove minacce alla sicurezza non provengono più dagli Stati e non sono più diretti verso di essi, ma ad esempio da una guerra civile, da malattie

[15] Treccani, < https://www.treccani.it/enciclopedia/liberta_%28Dizionario-di-filosofia%29/ > (04/21).

[16] United Nations Development Programme (UNDP), *Human Development Report*, Oxford University Press, New York-Oxford, 1994, <http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf> (04/21).

infettive, da catastrofi naturali, da atti terroristici o altre forme di crimini transnazionali, i quali possono originare sia da attori statali sia da attori non statali, e possono essere diretti sia a Stati sia ad attori non statali. In questo senso, ciò riconduce alla concezione che tutte le sfide e le minacce alla sopravvivenza, alla sussistenza e alla dignità umana possono essere definite come minacce alla sicurezza umana. Per Axworthy[17] la sicurezza umana significa proteggere gli individui contro le minacce, indifferentemente se accompagnate o meno da atti di violenza. L'autore specifica che si tratta di una situazione, oppure di uno stato, caratterizzato dall'assenza di violenza sui diritti fondamentali alle persone, alla loro sicurezza, alla loro vita. Quindi la sicurezza umana implicherebbe l'adozione di misure preventive per diminuire la vulnerabilità e ridurre a minimo i rischi, oppure semplicemente intraprendere misure per rimediare a tali situazioni.

Nel contesto delle migrazioni, le minacce alla sicurezza umana vanno oltre i confini nazionali degli Stati, e quindi molte di esse hanno carattere transnazionale. Infatti, è proprio in tale contesto che mettiamo in connessione le migrazioni, lo spazio marittimo e la sicurezza umana, tenendo sempre presente il sopraccitato collegamento relativo allo spazio marittimo e spazio terrestre. In questa categoria vi rientrano diversi tipi di minacce, iniziando da quelle tradizionalmente associate alle guerre civili e al degrado ambientale sui confini, a quelle emergenti, associate al crimine organizzato e al terrorismo.[18] Oltre a queste, ci sono quelle che riguardano strettamente le migrazioni illegali, come il traffico di esseri umani e migranti, i vari tipi di violenza e abuso di diritti umani di base, la persecuzione, la prostituzione,[19] oppure il diniego di accesso ai servizi sanitari, le malattie infettive, l'incarcerazione e detenzione arbitraria in paesi di transito o in paesi di destinazione, la chiusura dei confini, le restrizioni riguardo alla libertà di movimento, le restrizione al diritto di lavoro e tant'altro.[20]

In questo senso, dall'analisi dei risultati dei questionari relativi allo spazio marittimo, che sono stati condotti all'interno delle attività di ricerca del progetto Humarcyspase[21], emerge che una delle minacce più grandi per la sicurezza umana nel-

---

[17] L. Axworthy, "La sécurité humaine : la sécurité des individus dans un monde en mutation", *Politique étrangère* n°2, 1999, pp. 333-342, p. 337.

[18] S. Michael, "The Role of NGOs in Human Security" Working paper n. 12, *The Hauser Center for Nonprofit Organizations and the Kennedy school of Government*, Harvard University, 2002, pp. 1-30, <https://cpl.hks.harvard.edu/files/cpl/files/workingpaper_12.pdf?m=1440169193> (04/21), p. 16.

[19] S. Vucetic, "Illegal Migration in the Balkans: Whose Security Concerns?", *Annual Balkan security conference,* Centre for the Democratic Control of Armed Forces, Geneva, October 27-30, 2004, <https://srdjanvucetic.files.wordpress.com/2015/03/vucetic-whose_security-2004.pdf>.

[20] *Human security course, e-learning*, <http://humansecuritycourse.info/module-4-human-security-in-diverse-contexts/issue-5-migration/ > (05/21)

[21] Il progetto HUMARCYSPASE (Protecting HUman SEcurity with non-state-actors in the MARitime and CYber SPAce) è un progetto nel campo del diritto internazionale condotto dal Dipartimento di Giurisprudenza dell'Università degli Studi della Campania 'Luigi Vanvitelli' di Caserta, sotto la tutela della prof. Giorgia Bevilacqua come coordinatrice scientifica, e in collaborazione con la Facoltà di legge dell'Università Goce Delchev di Shtip, sotto la tutela delle prof. Ana Nikodinovska Krstevska e Olga Koshevaliska, <https://eprints.ugd.edu.mk/24422/> (04/21).

lo spazio marittimo è la pirateria (54% delle risposte), la quale sullo spazio terrestre corrisponde agli atti criminali eseguiti nei confronti dei migranti e rifugiati ; seguita dalla violazione dell'obbligo di soccorso in mare (27% delle risposte), che trova riscontro nelle politiche di chiusura dei confini, violazione del principio di *non-refoulment*, omissione di prestazione di aiuti e simile (questi ultimi, nel presente volume sono stati elaborati da Adele del Guercio relativamente al principio di non-refoulment). Altre minacce rilevanti per lo scopo di questo saggio sono quelle riscontrate nel questionario riguardante il traffico di esseri umani (18% delle risposte) presente sia nello spazio marittimo sia nello spazio terrestre, e la mancanza di norme adeguate a livello nazionale. Invece, circa la domanda su quali siano le minacce più ricorrenti in cui è possibile incorrere, sono state identificate: la pirateria, il sequestro di persona, l'immigrazione clandestina nonché l'estorsione da parte dei trafficanti e i respingimenti. Quindi, alla luce di quanto detto sopra, si riscontra la stessa tipologia di minacce verificatasi durante la crisi migratoria del 2015-2016 nella Macedonia del Nord.

4. Il ruolo degli attori non governativi in relazione all'inadeguatezza delle norme legislative a livello nazionale

Le prime minacce alla sicurezza umana dei rifugiati e migranti erano generate dalla legislazione nazionale inadatta in materia di asilo e migrazione. Infatti, l'art. 17 della Legge sull'asilo e protezione temporanea (LAPT),[22] prevedeva la possibilità per i migranti e rifugiati entrati illegalmente nel paese, di presentare domanda di asilo immediatamente al loro ingresso nel paese; in caso contrario in base all'art. 100 e 101 della Legge sugli stranieri,[23] e in accordo con l' Articolo 5 paragrafo 2 dell' *acquis* di Schengen in materia di controllo sulle frontiere esterne, sarebbero stati considerati come persone senza soggiorno regolato e soggetto a espulsione dal paese. Però, visto che la destinazione finale dei migranti e rifugiati erano i paesi dell'Unione Europea, essi non si avvalevano del diritto di chiedere asilo in Macedonia del Nord e quindi si limitavano solo a entrare nel paese con lo scopo di transitare. Di conseguenza, il diritto interno li considerava soggetti con soggiorno irregolare. Quindi la legislazione nazionale non prevedeva la possibilità di transitare tramite il paese senza la richiesta di asilo, la quale ipoteticamente, seguendo il ragionamento precedente riguardo la libertà di movimento, dovrebbe essere assicurata come nello spazio marittimo così anche sullo spazio terrestre. Per evitare di trovarsi in tale situazione, essi entravano illegalmente nel paese e viaggiavano clandestinamente, da soli o accompagnati da trafficanti. Quando viaggiavano accompagnati da trafficanti, venivano spesso sottoposti ad atti di violenza oppure di rapimento, per-

[22] Gazzetta Ufficiale della Repubblica di Macedonia N. 49/2003 ed emendamenti consecutivi N.66/2007, 142/2008, 146/2009, 166/2012 e 27/2013.

[23] Gazzetta Ufficiale della Repubblica di Macedonia N. 35/2006 e emendamenti seguenti N. 66/2007, 117/2008, 92/2009, 156/2010, 158/2011, 84/2012 e 147/2013.

ché i trafficanti estorcevano denaro alle loro famiglie.[24] Quando invece procedevano da soli, erano esposti ad altri tipi di pericoli. Ad esempio, in un incidente ferroviario, accaduto vicino alla città di Veles,[25] persero la vita 14 migranti i quali, diretti verso il confine con la Serbia, percorrevano la strada lungo i binari della ferrovia. Questa grave tragedia ha attirato l'attenzione dei media e fu allora che le ONG locali ed internazionali hanno iniziato le loro attività che possiamo definire come attività rivolta alla protezione della sicurezza umana dei migranti e rifugiati in Macedonia del Nord.[26]

In questo senso, le ONG Legis, Macedonian Young Lawyers Association, La Strada, UNHCR, Amnesty International, Human Rights Watch e altre, hanno proposto degli emendamenti sulla Legge sull'asilo e protezione temporanea che successivamente avrebbero consentito di transitare sul territorio macedone.[27] Le proposte prevedevano la legalizzazione del transito attraverso il paese, senza che i migranti chiedessero asilo nella Macedonia del Nord.[28] Questa soluzione, già in vigore nella Serbia, prevedeva nello specifico che tutti i migranti entrati illegalmente nella Macedonia del Nord potevano, al confine oppure nei Centri di transito vicino al confine, manifestare 'l'intenzione di chiedere asilo', in base alla quale avrebbero ottenuto un permesso di 72 ore che gli avrebbe consentito di transitare per il paese. Alla scadenza del termine i migranti erano costretti o a lasciare il paese oppure a presentare richiesta di asilo. Nel caso in cui non si fossero avvalsi di nessuna delle due opzioni allora il loro soggiorno sarebbe stato considerato illegale e quindi sarebbero stati deportati nel paese della loro entrata nella Macedonia del Nord. Il lasso di tempo di 72 ore era anticipato come tempo sufficiente per effettuare il transito attraverso il paese tenendo conto anche delle varie necessità come riposo nei centri di transito, ricevere aiuti, assistenza medica e altro. Quindi, l'introduzione di queste manovre legislative ha posto temporaneamente fine al problema delle migrazioni illegali, riducendo nello stesso tempo le pratiche di traffico di migranti e diminuendo il numero di casi mortali di migranti coinvolti in incidenti ferroviari.[29] Difatti, da quel momento le migrazioni di transito divennero legali e furono affrontati in modo più strutturato e più organizzato. I migranti entravano nel paese dal punto di pas-

---

[24] Legis, "2015 Annual Report Legis", January 10, 2016, < http://www.legis.mk/uploads/LEGIS_Annual-Report_2015%20-%20Copy%207.pdf>, (03/21)

[25] *The Guardian,* "14 migrants killed by train while walking on tracks in Macedonia", April 25, 2015 <https://www.theguardian.com/world/2015/apr/24/several-migrants-hit-by-train-killed-central-macedonia>, (03/21)

[26] Legis, *2015 Annual Report Legis*, cit., pp. 6-8.

[27] A. Sibel, *"*The rights of refugees, migrants and asylum seekers in Republic of Macedonia" Annual report for 2018*, Helsinki Committee for Human Rights of the Republic of Macedonia*, 2018 <https://mhc.org.mk/wp-content/uploads/2019/05/Help-On-Route-ANG-2018-final.pdf> (03/21)

[28] Emendamenti sulla Legge sull'asilo e protezione temporanea, Gazzetta Ufficiale della Repubblica di Macedonia N.101/2015.

[29] B. Beznec, and M. Speer and M. Stojić Mitrović, "Governing the Balkan route: Macedonia, Serbia and the European Border Regime." *Research Paper Series of Rosa Luxemburg Stiftung Southeast Europe* N. 5, December 2016, <https://bordermonitoring.eu/wp-content/uploads/2017/01/5-Governing-the-Balkan-Route-web.pdf>, (02/21).

saggio tra la Grecia e la Macedonia chiamato "Kamen 59" [Pietra 59]. Venivano registrati nel Centro di transito *Vinojug,*[30] e anche durante il processo di registrazione le ONG Legis, Macedonian Young Lawyers Association, La Strada e altri, in collaborazione con UNHCR e OIM assistevano la polizia nella fornitura di interpreti, mediatori e personale che li avrebbe aiutati a raccogliere dati personali dai migranti. [31]

5. Detenzione arbitraria di migranti e rifugiati

Un'altra minaccia alla sicurezza umana che migranti e rifugiati hanno dovuto affrontare nella Macedonia del Nord riguardava lo scandalo rivelato da Amnesty International[32] and Human Rights Watch[33] con l'aiuto della ONG Legis,[34] che concerneva la detenzione arbitraria di 1003 migranti e violazione dei loro diritti umani, verificatisi nel Centro di accoglienza per gli stranieri Gazi Baba a Skopje.[35] Nello specifico, migranti illegali catturati dalla polizia insieme ai loro trafficanti, in base all'art. 253 e art. 278 del Codice di Procedura Penale,[36] venivano messi ingiustamente in custodia dalla polizia con lo scopo di testimoniare contro i loro trafficanti di fronte al Tribunale. Comunque, la loro detenzione si è rivelata illegale perché la Legge sull'asilo e sulla protezione temporanea non prevedeva la detenzione e quindi, quando i migranti furono arrestati con i trafficanti, la Corte non poteva rilasciare un ordine di detenzione, che normalmente sarebbe stato rilasciato entro 24 ore dalla cattura, proprio perché non disponeva di una base legale sulla quale rilasciare l'ordine di detenzione. Di conseguenza, i migranti erano privati dalla possibilità di impugnare l'inesistente decisione di detenzione di fronte alla Corte[37] e di sfidare la detenzione arbitraria delle autorità statali. La polizia ha abusato di questo vacuum normativo continuando a detenere migranti e rifugiati con lo scopo di assicurare una loro testimonianza contro i trafficanti. Il periodo di detenzione dei migranti variava

[30] Questo Centro di transito fu costruito specialmente per lo scopo di registrare migranti, però era anche un posto dove riposare, ricevere assistenza medica, cibo e vestiti caldi.

[31] T. Stojanovski and A. Stojanovski, "Migration and its security aspects on the Western Balkans", in A. Nikodinovska Krstevska and B. Tushevska Gavrilovikj, *Migration at sea: International Legal Perspectives and Regional Approaches*, Giannini Editore, Napoli, 2015, pp. 49-60, <http://www.isgi.cnr.it/wp-content/uploads/2017/10/Migration-at-sea.-International-Law-Perspectives-and-Regional-Approaches.pdf> , (04/21).

[32] *Amnesty International,* "Urgent Action. Hundreds unlawfully held in inhuman conditions", 26 February 2015, <https://www.amnestyusa.org/files/uaa04615.pdf >, (03/21).

[33] *Human Rights Watch*, "As Though We Are Not Human Beings: Police Brutality against Migrants and Asylum Seekers in Macedonia", September 2015, <https://www.refworld.org/docid-/55ffdccc4.html>, (03/21).

[34] Smailovikj, *The Humanitarian aspect of the refugee crisis*, cit., p. 80.

[35] Veigel et altri, *The 'Gazi Baba' Reception Center for Foreigners in Macedonia*, cit., pp. 103-119

[36] Gazzetta Ufficiale della Repubblica di Macedonia N.150/2010.

[37] Human Rights Watch, A*s though We Are Not Human Beings*, cit., pp.42-48.

di caso in caso, però poteva anche superare un anno.[38] Questo era soprattutto dovuto alla difficoltà della Corte di trovare interpreti per casi penali.[39] A prescindere da ciò, i migranti detenuti subivano anche delle violazioni dei loro diritti umani che si verificavano nel Centro di accoglienza per gli stranieri. Il Centro era una struttura di tipo chiuso dove ai migranti non era permesso di uscire. Erano trattenuti in condizioni precarie in stanze sovraffollate, dove mancava ventilazione e luce naturale e un'adeguata igiene e assistenza medica. Spesso subivano trattamenti degradanti da parte della polizia.[40] La detenzione illegale era ovviamente in contrasto con gli impegni internazionali del paese in materia di diritti umani,[41] in forza dei quali le autorità devono provvedere a condizioni di detenzione sicure e umane.[42]

Dopo la scoperta dello scandalo, il Governo macedone ha chiuso il Centro di accoglienza per gli stranieri e i migranti ivi detenuti sono stati rilasciati. Tuttavia, dopo un iniziale periodo di inattività il Centro ha ripreso a funzionare e nel 2018 la Commissione Europea nel suo Rapporto sullo stato del progresso della Macedonia ha denunciato che ci sono circa 95 migranti detenuti in custodia in questa struttura.[43]

6. Conclusione

Da quanto illustrato si può vedere che le attività delle organizzazioni non governative nella Macedonia del Nord durante la crisi migratoria sono state particolarmente importanti per assicurare i diritti fondamentali dei migranti e dei rifugiati. Ciò si evince soprattutto dalle iniziative intraprese nel campo legislativo da parte di organizzazioni non governative sia nazionali che internazionali, che hanno proposto emendamenti riguardanti la Legge sull'asilo e migrazione. Infatti, in base a questi emendamenti, successivamente adottati dal Governo macedone, a migranti e rifugiati è stato riconosciuto il diritto di transitare sul territorio macedone e di raggiungere altri paesi dell'Europa del Nord, avvalendosi interamente della libertà di mo-

[38] Smailovikj, *The Humanitarian aspect of the refugee crisis*, cit., p.77.

[39] *UN High Commissioner for Refugees (UNCHR),* "The Former Yugoslav Republic of Macedonia, As a Country of Asylum: Observations on the situation of asylum-seekers and refugees in the Former Yugoslav Republic of Macedonia", 2015, <https://www.refworld.org/docid/55c9c70e4.html >, (03/21).

[40] Human Rights Watch, A*s though We Are Not Human Beings*, cit., pp. 23-41.

[41] Nello specifico, la Macedonia del Nord è parte contraente dei seguenti strumenti internazionali: Convenzione europea sui diritti umani (1950) dal 10 aprile 1997; Convenzione sullo status dei rifugiati (1951) e il Protocollo (1967) del 18 aprile 1994; Convenzione internazionale sui diritti civili e politici (1966) del 18 aprile 1994; membro dell'Organizzazione delle Nazioni Unite dell' 8 aprile 1993; membro del Consiglio d'Europa dal 9 novembre 1995; nonché è un paese candidato a divenire paese membro dell'Unione Europea dal 2005.

[42] Ibid, pp.39-41.

[43] *European Commission*, "Progress Report for the former Yugoslav Republic of Macedonia" (COM(2018) 450 final),<https://ec.europa.eu/neighbourhood-enlargement/news_corner/key-documents_en?f%5B0%5D=field_file_country%3A86>, (03/21).

vimento, della quale abbiamo discusso prima. Il ruolo che essi hanno giocato è stato quello di proteggere migranti e rifugiati dalla violazione del principio di non-refoulment, così come quello di procurare ed assicurare le prime necessità come cibo, acqua, assistenza medica, vestiti caldi, riposo e simile. Oltre a questo, le ONG hanno straordinariamente scoperto la detenzione arbitraria di migranti e rifugiati che avveniva nel Centro di accoglienza per stranieri 'Gazi Baba'a Skopje dove, a causa di una lacuna legislativa, migranti e rifugiati venivano detenuti arbitrariamente e sottoposti a condizioni di detenzione sfavorevoli, accompagnate spesso da violazioni di diritti umani di base da parte della polizia di stato. In conclusione, si può dire che questi attori non statali hanno avuto un ruolo catalizzante nelle politiche nazionali riguardanti migranti e rifugiati durante la crisi migratoria del 2015-2016, e con le loro varie attività hanno contribuito ad assicurare la sicurezza umana dei migranti e rifugiati nella Macedonia del Nord contro le varie minacce precedentemente individuate. In merito a ciò, si riconosce che gli attori non statali svolgono un ruolo preventivo e correttivo nella promozione dei diritti umani dei migranti e rifugiati e soprattutto nell'effettiva promozione, protezione e implementazione della loro sicurezza umana sia nello spazio marittimo sia sullo spazio terrestre.

LA FINZIONE DELLA ZONA SAR "LIBICA": QUALE GIURISDIZIONE SULLE ACQUE INTERNAZIONALI?

Fulvio Vassallo Paleologo

1. Introduzione

A partire dal 2018 le autorità europee hanno ritirato progressivamente tutti gli assetti navali impegnati nella zona SAR (di ricerca e soccorso) del Mediterraneo centrale ormai attribuita alla responsabilità di una fantomatica "Libia", che ancora oggi non è facile riconoscere come Stato unitario. Gli accordi bilaterali intercorsi con il governo di Tripoli, come il Memorandum d'intesa del 2 febbraio 2017, e la istituzione di una fittizia zona SAR "libica" nel 2018, hanno costituito gli schermi formali dietro i quali si è nascosta la sostanziale delega delle attività di intercettazione, al di fuori delle loro acque territoriali, alle autorità libiche, in molti casi colluse con le milizie che nelle città costiere, soprattutto tra Sabratha, Zawia e Tripoli, gestivano, oltre alla detenzione arbitraria dei migranti e alle partenze dei barconi, il contrabbando di petrolio ed il traffico di armi.

L'Unione Europea ha predisposto già dal 2004 un articolato sistema di contrasto dell'immigrazione "illegale" alle frontiere esterne, soprattutto attraverso l'agenzia Frontex, dotata di autonoma personalità giuridica, adesso ridefinita come "Guardia di frontiera e costiera europea", con sede a Varsavia. Nel dicembre del 2019 entrava in vigore il Regolamento (UE) 2019/1896, relativo alla Guardia di frontiera e costiera europea. Il nuovo Regolamento mette al centro delle attività dell'agenzia i sistemi elettronici di controllo, raccordando le attività delle diverse agenzie europee che operano nel settore del controllo delle frontiere marittime esterne (EUROSUR, EMSA, EUROPOL). Tra i punti più importanti del nuovo Regolamento è il rilancio della cooperazione con i paesi terzi al fine di rendere più efficaci le prassi di intercettazione /soccorso in mare e di respingimento/espulsione. Le deliberazioni del Consiglio dell'Unione Europea del 23 settembre 2020, e la Raccomandazione adottata lo stesso giorno dalla Commissione Europea sui soccorsi in mare operati da attori non statali, confermano le politiche di esternalizzazione dei controlli di frontiera e la collaborazione con i paesi terzi della sponda sud del Mediterraneo per contrastare quella che si continua a definire soltanto come "immigrazione illegale". Anche se in questi documenti si auspica la fine della criminalizzazione dei soccorsi umanitari, in realtà si riproducono le condizioni per ricondurre i salvataggi in mare operati dalle ONG ad attività sottoposte ad un rigoroso controllo amministrativo e militare, con il rischio che possano risultare sanzionabili in base alle norme sul contrasto dell'immigrazione irregolare.

Tutti i rapporti internazionali provenienti dalle Nazioni Unite, da Statewatch, da

Amnesty International,[1] confermano gli abusi commessi nel tempo dalla sedicente Guardia costiera libica, e poi quelli commessi in Libia, ai danni dei migranti intrappolati nei centri di detenzione. In questi centri vengono ancora oggi internati centinaia di minori non accompagnati, secondo quanto denuncia l'UNICEF. L'UNHCR ha chiesto più volte la chiusura dei centri di detenzione di varia natura e la sospensione dei respingimenti collettivi verso le coste libiche. Ma anche dopo la fine della fase più acuta del conflitto interno che ha dilaniato la Libia in questi ultimi anni, la situazione non sembra sostanzialmente mutata.

Alle denunce corrispondono le proposte, ma gli Stati europei rimangono sordi.[2] Emerge dunque il tema della responsabilità, non solo politiche, dei governi, dei vertici delle operazioni di Frontex e degli apparati amministrativi e militari nazionali quando cooperano con le autorità libiche nelle attività di intercettazione dei migranti in alto mare, contribuendo al blocco dei barconi in acque internazionali e alla loro successiva riconduzione in Libia. Attività che difficilmente potrebbero qualificarsi come "salvataggi" nel senso che si attribuisce a questo temine in base alle Convenzioni internazionali.[3] Si potrebbe invece ritenere che, per effetto del ricorso al monitoraggio elettronico ed al tracciamento delle imbarcazioni cariche di migranti individuate nel Mediterraneo centrale da assetti operativi di Frontex/Eunavfor Med, e da questi comunicati alle autorità marittime e di polizia degli Stati che collaborano nelle attività di contrasto dell'immigrazione irregolare, che si risolvono in respingimenti delegati alle autorità libiche, si possano riscontrare ipotesi di responsabilità sul piano internazionale e a livello nazionale, anche dove la giurisdizione degli Stati si esercita al di fuori delle acque territoriali.

2. Dagli accordi bilaterali con il governo di Tripoli alla creazione di una finta zona sar libica

Nel 2012 l'Italia veniva condannata dalla Corte europea dei diritti dell'Uomo per i respingimenti collettivi eseguiti dalla Guardia di Finanza il 6 maggio 2009 verso il porto di Tripoli.[4] Da allora nell'Unione Europea si rilanciavano le politiche e le prassi di esternalizzazione (altrimenti definita: dimensione esterna), già anticipate dal Trattato di amicizia tra Italia e Libia stipulato nel 2008[5] e si tentava di aggi-

1 Si rinvia al Rappporto dell'Alto commissariato delle Nazioni Unite per i diritti umani (OHCHR), *"Lethal Disregard"* in <https://sicurezzainternazionale.luiss.it/2021/05/26/lethal-disregard-documento-dellonu-incolpa-ue-libia-le-morti-migranti/> (06/21)

2 Si veda *"Europa: piano d'azione – la protezione dei migranti sulla rotta del Mediterraneo centrale in venti mosse. Le proposte di Amnesty, ECRE e HRW",* in <https://www.hrw.org/it/news/2021/06/30/378971> (06/21)

3 U. Leanza, F. Caffio, "*Il SAR Mediterraneo, La ricerca e soccorso nel diritto marittimo: l'applicazione della Convenzione di Amburgo del 1979",* in <http://www.fondazionemichelagnoli.it/files/Leanza-Caffio_RM.pdf> (06/21)

4 A. Liguori, "La Corte europea dei diritti dell'Uomo condanna l'Italia per i respingimenti verso la Libia del 2009: il caso Hirsi", *Rivista di diritto internazionale*, 2012, pp. 415-44.

5 Il trattato Italia-Libia di amicizia, partenariato e cooperazione, Dossier Senato della Repubblica, n.108, gennaio 2009, <http://www.iai.it/sites/default/files/pi_a_c_108.pdf> (06/21).

rare il divieto di respingimento sancito anche dall'art. 33 della Convenzione di Ginevra, in quanto la Libia non era, e non è ancora oggi, un paese che può garantire porti sicuri di sbarco. Per creare una barriera legale che scoraggiasse l'attraversamento del Mediterraneo centrale si è inventata nel 2018 una zona SAR (ricerca e salvataggio) libica,[6] frutto di una intensa trattativa tra diversi governi e l'IMO a Londra,[7] dopo che si erano intensificate le prassi di cooperazione operativa previste dagli accordi bilaterali, come il Memorandum d'intesa tra Italia e le autorità tripoline, stipulato il 2 febbraio 2017.[8] Accordi simili sono stati successivamente conclusi tra Malta, che ha una vastissima zona SAR contigua a quella riconosciuta ai libici, e lo stesso governo di Tripoli.[9] Malta però non ha mai accettato gli emendamenti apportati nel 2004 alla Convenzione di Amburgo del 1979 sui soccorsi in mare, e dunque ancora oggi rifiuta sistematicamente di assumere il coordinamento di operazioni SAR che non avvengano nel suo mare territoriale e che non siano condotte da mezzi maltesi.[10] Le autorità maltesi, peraltro, dopo essere state scoperte in flagrante durante una operazione di respingimento collettivo verso la Libia, attuata il 13 aprile 2020 e culminata con la "strage di Pasquetta" di quello stessso anno, con 12 vittime**,** sembrano avere rallentato le attività della flotta di pescherecci "ombra" che, agli ordini del governo de La Valletta**,** eseguivano respingimenti collettivi verso i porti libici, analoghi a quelli per cui l'Italia è stata condannata nel 2012 dalla Corte europea dei diritti dell'Uomo (caso Hirsi). Sono però aumentati i casi in cui motovedette libiche svolgono attività di intercettazione in acque internazionali in quella che dovrebbe essere la zona SAR maltese. Su uno di questi casi, nel quale da una motovedetta libica, dopo vari tentativi di speronamento, si era aperto il fuoco su un barcone che cercava di sottrarsi alla intercettazione in acque internazionali, nel mese di luglio di quest'anno, è stata aperta una indagine da parte della Procura di Agrigento.[11]

La zona di ricerca e salvataggio (SAR) attribuita alla Libia nel 2018[12] si è rive-

---

[6] F. Vassallo Paleologo, "*Una zona SAR per la Libia che non esiste"*, 2018, <https://www.a-dif.org/2018/06/28/una-zona-sar-per-la-libia-che-non-esiste-si-perfeziona-la-politica-dellannientamento/> (06/21).

[7] Vedi il Comunicato stampa della Guardia costiera italiana <https://www.guardiacostiera.gov.it/stampa/Pages/Comandante-Generale-incontra-Segretario-Generale-IMO-e-Ambasciatore-Italiano-Londra.aspx> (06/21).

[8] Sulla politica di collaborazione dell'Italia con la Libia in tema di migrazione, F. De Vittor, "Responsabilità degli Stati e dell'Unione europea nella conclusione di accordi per il controllo extraterritoriale della migrazione", *Diritti umani e diritto internazionale*, 2018, p. 223 ss.

[9] F. Tumminello, "*Il buio nel Mediterraneo: gli accordi tra Malta e Libia*," 2020, <https://www.iusinitinere.it/il-buio-nel-mediterraneo-gli-accordi-tra-malta-e-libia-29051> (06/21),

[10] G. Cataldi*,"L'impossibile "interpretazione conforme" del decreto "sicurezza bis" alle norme internazionali sul soccorso in mare",* 2020, <https://www.asgi.it/notizie/limpossibile-interpretazione-conforme-decreto-sicurezza-bis-norme-internazionali-soccorso-in-mare/ > (06/21).

[11] G. Alibrandi, *"Spari contro i migranti, la Procura di Agrigento chiede di indagare la Guardia costiera libica",* consultabile in <https://www.tpi.it/cronaca/spari-migranti-procura-agrigento-indagare-guardia-costiera-libica-20210709805282/> (06/21)

[12] Y. Maccanico, "Mediterranean: As the Fiction of a Libyan Search and Rescue Zone begins to Crumble, EU States Use the Coronavirus Pandemic to Declare Themselves Unsafe", 2020,

lata sempre di più come una zona di morte, Ancora nel 2021, secondo quanto denuncia l'OIM, l'incremento delle vittime è costante.[13] Spetterebbe alle Nazioni Unite, che pure definiscono con l'UNHCR la Libia come un paese "non sicuro",[14] verso cui non devono essere effettuati respingimenti, intervenire sull'IMO (Organizzazione internazionale del mare) con sede a Londra, che pure risulta essere organizzazione delle stesse Nazioni Unite, per porre fine alla finzione della cosiddetta zona SAR (di ricerca e salvataggio) libica, di una Libia che non ancora esiste come entità territoriale unica, con un coordinamento unificato delle operazioni di ricerca e salvataggio (SAR). Non si può consentire che gli interventi della sedicente Guardia Costiera Libica, che altri definiscono di "salvataggio", si concludano con vittime in mare e con deportazioni a terra, perché i naufraghi sembrano sparire non appena sbarcati in poro. Di fatto, queste persone, ricondotte a terra con modalità spesso violente, vengono cedute di nuovo alle stesse milizie e alle stesse bande di trafficanti da cui sono fuggite. E questo i governi europei non possono ignorarlo. Come non si può ignorare che la Libia non ha mai sottoscritto la Convenzione di Ginevra sui rifugiati, né dà effettiva attuazione ad analoghi strumenti convenzionali previsti a livello regionale dall'Organizzazione dell'Unione Africana (OUA). La Libia rimane ancora oggi caratterizzata, del resto, da una fitta rete di corruzione e di complicità tra milizie, riconosciute dal governo provvisorio di Tripoli o dalle autorità locali, ed organizzazioni criminali che gestiscono il traffico di persone.

Il Rapporto finale del Gruppo di esperti ONU sulla Libia pubblicato nel mese di marzo di quest'anno[15] ha cercato di fare luce sulla rete di contrabbando di carburante e di esseri umani nella città di Zawiya, sulla quale aveva indagato per anni, senza esito, anche la Procura di Catania.[16] Tale attività si sarebbe intensificata durante la seconda metà del 2020, quando la domanda mondiale di carburanti per il trasporto marittimo è diminuita a causa della pandemia di coronavirus e i prezzi di mercato sono calati. Il rapporto menziona anche l'arresto di Abd al Rahman al Milad, noto come "Bija", nell'ottobre 2020. Questa vicenda ha evidenziato una competizione di interessi all'interno dei servizi di sicurezza del Governo di accordo nazionale, a scapito del rispetto dello "Stato di diritto". Dopo l'arresto, infatti, il procuratore militare libico richiedeva il trasferimento di Bija sotto la sua autorità, e poi nel mese di aprile di quest'anno, lo stesso Bija veniva liberato e reintegrato nel ruolo di comandante della Guardia costiera libica, per l'impegno profuso nella difesa di Tripoli durante i ripetuti attacchi del generale Haftar.

<https://www.statewatch.org/analyses/2020/mediterranean-as-the-fiction-of-a-libyan-search-and-rescue-zone-begins-to-crumble-eu-states-use-the-coronavirus-pandemic-to-declare-themselves-unsafe/> (04/21).

[13] IOM, Rapporto 2020, <https://missingmigrants.iom.int/region/mediterranean> (06/21).

[14] E. Bonini, "La Libia non è un posto sicuro". L'UNHCR critica la politica migratoria dell'UE, <https://www.eunews.it/2020/07/29/la-libia-non-un-posto-sicuro-lunhcr-critica-la-politica-migratoria-dellue/133043> (06/21).

[15] Rapporto finale del Gruppo di esperti ONU sulla Libia (2020), <https://www.nova.news/cosa-ce-scritto-ed-e-stato-omesso-nel-rapporto-degli-esperti-onu-sulla-libia/> (06/21).

[16] <https://www.lasicilia.it/news/catania/115425/dirty-oil-catturato-a-lampedusa-il-maltese-debono.html> (06/21)

Secondo il report degli esperti Onu, le infrastrutture delle reti di contrabbando di Zuwara e Abu Kamash sono ancora intatte e non hanno perso la capacità di svolgere attività illecite nel contrabbando di petrolio e nel traffico di esseri umani. Di fatto, malgrado le missioni internazionali ed europee che si succedono in Libia, come UNSMIL, EUBAM ed Eunavfor Med IRINI, la situazione sul terreno, ed in mare, è ancora caratterizzata da una grande incertezza, derivante anche dalla presenza di numerose milizie straniere e dal ruolo altalenante delle diplomazie europee, dopo che la Turchia ha stabilito una forte presenza militare a difesa del governo di Tripoli.

La ricomparsa del comandante Al Milad (Bija) a piede libero, getta ombre sul futuro della collaborazione tra le autorità marittime italiane, europee e libiche. Perché è il segnale di una situazione di illegalità e di corruzione che raggiunge i nuovi assetti del governo provvisorio ed è ancora diffusa nella maggior parte delle città costiere della Tripolitania. Dallo scorso anno alle unità della guardia costiera libica si sono affiancati anche i nuclei operativi dei GACS (*General Administration for Coastal Security*) e la ripartizione delle competenze operative, soprattutto quando si dovrebbero coordinare azioni di soccorso, appare sempre più incerta.[17]

Gli accordi bilaterali stipulati dal governo italiano e da quello maltese con le autorità libiche non sembrano comunque in grado di giustificare la disapplicazione del diritto internazionale o dei Regolamenti europei.[18] Le zone SAR in acque internazionali (che sono zone di responsabilità per la ricerca e il salvataggio, non zone di sovranità nazionale)[19] rimangono soggette all'applicazione delle Convenzioni internazionali di diritto del mare che stabiliscono precisi obblighi di coordinamento e di soccorso, compreso lo sbarco in un porto sicuro, a carico degli Stati.[20]

3. I sistemi di controllo delle frontiere marittime europee

Nel dicembre del 2019 entrava in vigore il Regolamento (UE) 2019/1896 del 13

[17] Human Rights Watch, "EU: Time to review and remedy cooperation policies facilitating abuse of refugees and migrants in Libya, NGOs Joint Statement", < https://www.hrw.org/news/2020/04/28/eu-time-review-and-remedy-cooperation-policies-facilitating-abuse-refugees-and> (06721).

[18] I. Papanicolopulu e G. Baj, "Controllo delle frontiere statali e respingimenti nel diritto internazionale e nel diritto del mare", *Diritto, Immigrazione e Cittadinanza,* 2020/1, p. 24.

[19] I. Tani*,* "Ricerca e soccorso nel Mediterraneo centrale tra diritto internazionale e nuove (discutibili) qualificazioni del fenomeno migratorio", 2019, <https://www.dirittoimmigrazionecittadinanza.it/archivio-saggi-commenti/saggi/fascicolo-n-3-2019-1/474-ricerca-e-soccorso-nel-mediterraneo-centrale-tra-diritto-internazionale-e-nuove-discutibili-qualificazioni-del-fenomeno-migratorio> (06/21).

[20] F. Vassallo Paleologo, *"Gli obblighi di soccorso in mare nel diritto sovranazionale e nell'ordinamento interno",*<https://www.questionegiustizia.it/rivista/articolo/gli-obblighi-disoccorso-inmare-neldiritto-sovranazionale-enell-ordinamento-interno_548.php> (06/21); S. Trevisanut, "*Is there a Right to Be Rescued at Sea? A Constructive View"*, *Question of International Law*, 23 giugno 2014.

novembre 2019[21] relativo alla Guardia di frontiera e costiera europea che abrogava i precedenti Regolamenti (UE) n. 1052/2013 e (UE) 2016/1624. Non è stato però abrogato il Regolamento UE 656/2014, dal quale, a carico degli Stati, si ricavano precisi obblighi di salvataggio nei confronti delle persone migranti che si trovano in situazioni di pericolo nel Mediterraneo.[22]

Il nuovo Regolamento adottato nel 2019, aumenta di molto le risorse da destinare all'agenzia FRONTEX. Si prevede anche il rilancio della cooperazione con i paesi terzi al fine di rendere più efficaci le prassi di intercettazione /soccorso in mare e di respingimento/espulsione. Si inquadrano nella "dimensione esterna" delle politiche europee anche le più recenti Raccomandazioni della Commissione europea sul soccorso nel Mediterraneo, adottate il 23 settembre 2020. Anche se si sollecita "il riconoscimento del sostegno fornito da attori privati e ONG nell'esecuzione di operazioni di soccorso in mare e a terra", chiedendosi di "evitare di criminalizzare coloro che danno assistenza umanitaria alle persone in pericolo in mare", si rafforza la politica basata sugli accordi di collaborazione con le autorità libiche, nelle attività di intercettazione in acque internazionali con la riconduzione delle persone bloccate in mare in territorio libico.

Nelle più recenti politiche europee di controllo delle frontiere esterne, che assumono sempre più carattere intergovernativo, si assiste dunque al trasferimento delle responsabilità dalle sedi di decisione politica a Bruxelles agli Stati membri ed agli organi amministrativi e di polizia di Frontex, che ha una personalità giuridica autonoma rispetto a quella dell'Unione Europea. E questo amplia la possibilità di negoziazione di Frontex e del suo direttore nei rapporti con i governi dei paesi terzi. [23] Per quanto riguarda il contrasto dell'immigrazione irregolare via mare, sono

[21] D. Vitiello, E. De Capitani, "Il Regolamento (UE) 2019/1896 relativo alla riforma di Frontex e della Guardia di frontiera e costiera europea: da "Fire Brigade" ad amministrazione europea integrata?", <http://www.sidiblog.org/2019/12/06/il-regolamento-ue-20191896-relativo-alla-riforma-di-frontex-e-della-guardia-di-frontiera-e-costiera-europea-da-fire-brigade-ad-amministrazione-europea-integrata/> (06/21).

[22] Secondo il Considerando n.20 del Regolamento (UE) 2019/1896 "L'attuazione del presente regolamento non incide sulla ripartizione delle competenze tra l'Unione e gli Stati membri né sugli obblighi che incombono agli Stati membri in base alla convenzione delle Nazioni Unite sul diritto del mare, alla convenzione internazionale per la salvaguardia della vita umana in mare, alla convenzione internazionale sulla ricerca e il salvataggio marittimo, alla convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale e al suo protocollo per combattere il traffico di migranti via terra, via nave e via aria, alla Convenzione del 1951 relativa allo status dei rifugiati, il relativo protocollo del 1967, alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, alla convenzione delle Nazioni Unite relativa allo status degli apolidi e ad altri strumenti internazionali pertinenti. Al considerando 21 si ribadisce che" L'attuazione del presente regolamento non incide sul Regolamento (UE) n. 656/2014 del Parlamento europeo e del Consiglio. Le operazioni marittime dovrebbero essere condotte in modo tale da garantire, in tutti i casi, la sicurezza delle persone intercettate o soccorse, delle unità che partecipano alle operazioni in mare in questione e la sicurezza di terzi".

[23] In base all'art.71 e seguenti del Regolamento Frontex del 2019, "Gli Stati membri e l'Agenzia cooperano con i paesi terzi ai fini della gestione europea integrata delle frontiere e della politica in materia di migrazione. Sulla base delle priorità politiche definite ai sensi dell'articolo 8, paragrafo 4, l'Agenzia fornisce assistenza tecnica e operativa ai paesi terzi nell'ambito della politica dell'Unione in materia di azione esterna, anche per quanto riguarda la protezione dei diritti fondamentali e dei dati per-

sempre più evidenti le prove di una crescente interazione tra le diverse agenzie europee che si occupano della sicurezza e del controllo delle frontiere e le autorità di polizia dei paesi della sponda sud del Mediterraneo. *Statewatch*[24] ricorda come le immagini raccolte dai droni dell'Agenzia europea per la sicurezza marittima (EMSA) siano state immediatamente valutate dalle Guardia costiera delle nazioni territorialmente responsabili, dunque anche dalle autorità libiche, e contestualmente inviate al quartier generale di Frontex ed integrate nel Sistema di sorveglianza delle frontiere (EUROSUR) per una loro analisi da parte dell'agenzia europea e del network di controllo di tutti gli Stati membri UE che hanno frontiere esterne.[25] Tutti i dati raccolti da Frontex e scambiati con altre agenzie di controllo, sono utilizzati per rilevare e prevenire le migrazioni sin dalla fase iniziale. I dati di EUROSUR e dei centri nazionali di controllo delle frontiere costituiscono il cosiddetto "*Common Pre-frontier Intelligence Picture*" che consente di estendere l'area di sorveglianza di Frontex sino al continente africano.

Nell'ambito di questa stretta integrazione di agenzie europee, il "*Seahorse Mediterranean Network*" è un programma di cooperazione per "migliorare gli scambi di informazioni nell'area mediterranea", sottoscritto da sette Stati membri UE (Spagna, Italia, Francia, Malta, Grecia, Cipro e Portogallo) e dai paesi nordafricani nel quadro di EUROSUR. Si prevede anche una serie d'iniziative di formazione ed addestramento dirette agli agenti dei paesi africani in materia di sorveglianza marittima. [26]

L'8 gennaio 2020, Joseph Borrell, Alto rappresentante UE per gli Affari esteri e la politica di sicurezza, rispondendo ad un'interrogazione parlamentare, ha negato che siano mai state fornite informazioni da Frontex alla Guardia costiera libica nell'ambito delle operazioni di sorveglianza previste dal Regolamento UE (n. 656/2014) ed effettuate dagli Stati membri alle loro frontiere esterne in cooperazio-

---

sonali e il principio di non respingimento". Secondo l'art. 73 del Regolamento "L'Agenzia può, nella misura necessaria per l'espletamento dei suoi compiti, cooperare con le autorità di paesi terzi competenti per questioni contemplate nel presente regolamento. L'Agenzia rispetta il diritto dell'Unione, comprese le norme e gli standard che fanno parte dell'acquis dell'Unione, anche quando la cooperazione con i paesi terzi ha luogo sul territorio di tali paesi terzi. Inoltre, nel cooperare con le autorità di paesi terzi, l'Agenzia agisce nell'ambito della politica dell'Unione in materia di azione esterna, anche con riferimento alla protezione dei diritti fondamentali e dei dati personali, al principio di non respingimento, al divieto di trattenimento arbitrario e al divieto di tortura e di trattamenti o pene inumani o degradanti. In base all'art. 75, dello stesso Regolamento, si prevede lo scambio di informazioni con i paesi terzi nell'ambito di Eurosur in base al quale I centri nazionali di coordinamento, e, se del caso, l'Agenzia rappresentano i punti di contatto per lo scambio di informazioni e la cooperazione con i paesi terzi.

[24] Statewatch, "Border surveillance and deaths at sea: Frontex's invisible flights come under scrutiny", <https://www.statewatch.org/news/2020/july/border-surveillance-and-deaths-at-sea-frontex-s-invisible-flights-come-under-scrutiny/> (06/21).

[25] M. Monroy, "*Drones for Frontex: unmanned migration control at Europe's borders",* 2020, <https://www.statewatch.org/media/documents/analyses/no-354-frontex-drones.pdf> (06/21)

[26] A. Mazzeo*, "Sorveglianza alle frontier, droni e militarizzazione del Mediterraneo"*, <htttp://www.lavocedellevoci.it/2020/11/26/sorveglianza-alle-frontiere-droni-e-militarizzazione-del-mediterraneo/> (06/21)

ne con l'Agenzia. "Ciò si è verificato tuttavia nell'ambito dell'"*Eurosur Fusion Service — Multipurpose Aerial Surveillance* (MAS)", ha dovuto poi ammettere lo stesso Commissario Borrell."durante l'attività di sorveglianza aerea MAS nell'area di pre-frontiera – dal 2017 sino al 20 novembre 2019, quando Frontex ha individuato situazioni di pericolo nella regione SAR libica, l'Agenzia ha informato in 42 casi il Centro di coordinamento delle ricerche dello Stato membro più vicino, Eunavfor MED così come le autorità libiche".

Il 17 giugno 2020 quattro organizzazioni non governative (Alarm Phone, Borderline-Europe, Mediterranea Saving Humans e Sea-Watch) hanno presentato il rapporto "*Remote control: the EU-Libya collaboration in mass interceptions of migrants in the Central Mediterranean"*[27] che evidenzia come le azioni intraprese dalle unità di sorveglianza aerea dell'UE, in collaborazione con le autorità libiche, abbiano facilitato le intercettazioni e i respingimenti collettivi dei migranti. Il rapporto ricostruisce in particolare alcuni eventi di ricerca e salvataggio conclusi con intercettazioni e respingimenti verso e dentro la zona SAR riconosciuta alla Libia.

L'asse principale di intervento dei governi europei verso i paesi della sponda sud del Mediterraneo punta sempre di più sul contrasto dell'immigrazione "illegale" con la delega delle attività di intercettazione e respingimento, e non certo sui soccorsi in mare. Si dovrà dunque verificare, con una continua attività di monitoraggio, la compatibilità dei sistemi di controllo elettronico delle frontiere, alla luce dei rapporti con i paesi terzi e del coordinamento delle operazioni di blocco in mare, con la tutela dei diritti fondamentali delle persone. La Convenzione di Palermo del 2000 contro il crimine transnazionale, ed i due Protocolli allegati contro il traffico di migranti e la Tratta di esseri umani,[28] che sembrerebbero giustificare la "collaborazione di polizia" con tali paesi, antepongono chiaramente la salvaguardia della vita umana in mare ed il rispetto dei diritti umani, alla "lotta contro l'immigrazione illegale" ed alla difesa dei confini.

4. Politiche di esternalizzazione e prassi di abbandono in mare

Al fine di eliminare qualsiasi "fattore di attrazione" (*pull factor*) rispetto alle partenze dalle coste libiche l'Unione Europea ha ritirato progressivamente tutti gli assetti navali impegnati nell'operazione Frontex *Triton*, che ha avuto termine nel 2020 e non sono state previste unità navali di Frontex nella nuova "*Joint Operation Themis*"[29] tuttora in corso. Nel frattempo aveva termine anche l'operazione *Sophia*

[27]<thtps://www.statewatch.org/news/2020/june/remote-control-the-eu-libya-collaboration-in-mass-interceptions-of-migrants-in-the-central-mediterranean/ (06/21)

[28] Secondo l'art. 19 del Protocollo addizionale contro il traffico di persone, *"Nessuna disposizione del presente Protocollo pregiudica diritti, obblighi e responsabilità degli Stati e individui ai sensi del diritto internazionale, compreso il diritto internazionale umanitario e il diritto internazionale dei diritti dell'uomo e, in particolare, laddove applicabile, la Convenzione del 1951 e il Protocollo del 1967 relativi allo Status di Rifugiati e il principio di non allontanamento".*

[29] Sulle attività del Consiglio dell'Unione Europea, per "*Salvare vite in mare e lottare contro le re-*

di Eunavfor Med, che pure fino al 2018 aveva contribuito attivamente al salvataggio di decine di migliaia di naufraghi, successivamente sbarcati in porti italiani. La nuova missione Eunavfor Med IRINI,[30] dopo avere subito un ridimensionamento sotto il profilo dei compiti operativi, incentrati principalmente sull'embargo di armi dirette verso la Libia e solo subordinatamente sulla lotta all'immigrazione "illegale", nel biennio 2021-2023 dovrebbe accrescere i suoi rapporti di collaborazione con Frontex, e dunque incrementare l'impegno congiunto multi-agenzia nel contrasto dell'immigrazione irregolare. Tra i principi solennemente dichiarati delle autorità di Bruxelles, che nei documenti ufficiali antepongono la salvaguardia della vita umana in mare al contrasto dell'immigrazione illegale ed all'embargo di armi, e la pratica quotidiana dei centri operativi che coordinano queste missioni nel Mediterraneo, la distanza appare considerevole. Come se il contrasto dell'immigrazione irregolare, e più in generale delle organizzazioni criminali che proliferano ovunque si rafforzino gli sbarramenti alle frontiere, dovesse prevalere sulla salvaguardia del diritto alla vita delle persone migranti. Su questo sta indagando adesso il Parlamento europeo che ha richiesto in più occasioni al Direttore di Frontex una documentazione esaustiva sulle attività svolte nel Mediterraneo in base al mandato conferito all'Agenzia.[31]

La carenza di informazioni ufficiali costituisce un tratto caratteristico comune di Frontex e delle autorità italiane. I più recenti rapporti di Frontex non fanno più riferimento ad attività di ricerca e soccorso nel Mediterraneo centrale. Analoga chiusura si riscontra da parte delle autorità nazionali, malgrado il Piano SAR nazionale del 1996, e poi quello aggiornato nel 2020,[32] prevedessero precisi obblighi di comunicazione in capo alle autorità marittime. Basta confrontare i dati ufficiali forniti dalla Guardia costiera italiana fino al 2018 con l'attuale silenzio delle autorità marittime italiane di fronte alle richieste di informazioni sui soccorsi e con i dati più recenti forniti dall'OIM, [33] per avere la prova di come si sia creato uno "spazio vuoto" a livello operativo ed a livello informativo, proprio sulle rotte del Mediterraneo centrale, uno "spazio vuoto", sottratto a qualsiasi giurisdizione, che dovrebbe valere come deterrente rispetto alle partenze di imbarcazioni dalla Libia e dalla Tunisia. Le periodiche "analisi di rischio" di Frontex non forniscono dettagli sui rapporti di coordinamento con le guardie costiere dei paesi terzi. In questa vasta area di acque

---

*ti criminali" s*i rinvia a <https://www.consilium.europa.eu/it/policies/migratory-pressures/saving-lives-at-sea/> (06/21)

[30] G. Gaiani, "Al via l'operazione europea Irene per imporre l'embargo sulle armi alla Libia" <https://www.analisidifesa.it/2020/04/prende-il-via-loperazione-europea-irene-per-imporre-lembargo-di-armi-in-libia/> (06/21).

[31] P. Riva, "Un gruppo di lavoro del Parlamento Europeo sta indagando su Frontex", <https://openmigration.org/analisi/un-gruppo-di-lavoro-del-parlamento-europeo-sta-indagando-su-frontex/> (06/21).

32 F. Vassallo Paleologo, "Un nuovo decreto ministeriale disciplina il salvataggio: mai più abbandoni in mare", consultabile in *<https://www.a-dif.org/2021/02/08/un-nuovo-decreto-ministeriale-disciplina-il-salvataggio-mai-piu-abbandoni-in-mare/>* (06/21).

[33] Si rinvia al Rapporto di Infomigrants, "*Nearly 1,000 migrants returned to Libya",* in <https://www.infomigrants.net/en/post/31156/nearly-1-000-migrants-returned-to-libya> (06/21).

internazionali, ai limiti della zona SAR maltese, ed anche al suo interno, si moltiplicano i tentativi di intercettazione delle motovedette libiche. Soltanto la presenza delle ONG, che con piccoli velivoli contribuiscono alle attività di monitoraggio e soccorso, lascia filtrare una minima parte di quanto avviene in mare. È del resto evidente come le autorità marittime nazionali cerchino fino all'ultimo di nascondere la natura degli eventi di soccorso, riducendoli alla qualificazione di "eventi migratori", anche quando le imbarcazioni tracciate con i sistemi elettronici e visivi sono in evidente stato di pericolo imminente (*distress*) di affondamento.

Nel corso degli ultimi anni è scomparso il Dossier annuale della Guardia costiera italiana, pubblicato per l'ultima volta nel 2018, che documentava le importanti attività di ricerca e soccorso effettuate dalle autorità italiane, dal 2014 al 2017, nel Mediterraneo centrale in sinergia con Frontex e con le ONG. I comunicati ufficiali dei ministeri, della Marina militare e della Guardia costiera, dettagliatissimi quando si riferisce del "fermo amministrativo" delle navi delle ONG,[34] sono del tutto lacunosi quando si tratta di chiarire cosa è successo nelle operazioni di ricerca e soccorso in acque internazionali.

Per avere notizie sulle attività SAR in acque internazionali occorre risalire alla stampa locale ed ai pochi giornalisti d'inchiesta che hanno ancora qualche fonte in Libia. Ma proprio nei confronti di chi è stato testimone dei gravissimi abusi commessi ai danni dei migranti in Libia, e del sostanziale abbandono in mare subito da coloro che riuscivano a fuggire da quel paese, si è fatto ricorso ad attività di intercettazione, in violazione delle garanzie previste dalla legge per il diritto di cronaca e per i diritti di difesa. Eppure proprio dai "brogliacci" di polizia giudiziaria che contengono queste intercettazioni, e che avrebbero dovuto essere distrutti perché non rilevanti ai fini delle indagini penali, come nel caso Iuventa a Trapani, emergono dettagli e dati che confermano una sistematica omissione di soccorso, che si è protrae e si aggrava negli ultimi anni su tutte le rotte del Mediterraneo centrale.

La presenza di poche imbarcazioni delle ONG che operavano, sotto coordinamento della Centrale operativa della Guardia costiera italiana, nelle acque internazionali tra la Libia e la Sicilia, in quella che doveva essere considerata come la zona SAR libica, continua così ad essere considerata come un fattore non solo di attrazione, ma di vera e propria agevolazione dell'immigrazione irregolare, proprio come era anticipato in un Rapporto stilato da Frontex alla fine del 2016.[35] Alle iniziative giudiziarie si sono alternate campagne mediatiche che hanno attribuito ai soccorsi operati dalle ONG nel Mediterraneo centrale tutte le responsabilità del fallimento delle politiche di controllo delle frontiere marittime. Fino al punto di rendere accettabile per la maggior parte dell'opinione pubblica la negazione di una qualsiasi

[34] F. Vasallo Paleologo, "*Fermo amministrativo o abuso di potere? La guerra ai soccorsi in mare prosegue in Europa",* in <https://www.a-dif.org/2021/01/02/fermo-amministrativo-o-abuso-di-potere-la-guerra-ai-soccorsi-in-mare-prosegue-in-europa/> (06/21).

[35] Si rinvia al rapporto dell'agenzia europea FRONTEX, "*EU border force flags concerns over charities' interaction with migrant smugglers",* <https://www.internazionale.it/notizie/2016/12/15/frontex-accusa-alcune-ong-di-collaborare-con-i-trafficanti-di-migranti> (06/21)

giurisdizione, e dunque la sostanziale impunità per gli abusi commessi in alto mare, oltre che per le violazioni del diritto marittimo internazionale e della Convenzione di Ginevra del 1951 sui rifugiati.

Nelle inchieste, rilanciate nei primi mesi del 2021 da alcune procure siciliane, è risultato centrale il riconoscimento di una zona SAR libica, anche prima che questa fosse comunicata dai libici all'IMO, per giungere ad ipotizzare un sostanziale accordo tra i trafficanti, gli scafisti e componenti degli equipaggi delle ONG. Ed ancora oggi, nel procedimento Iuventa a Trapani, si giunge ad ipotizzare persino il coinvolgimento delle società armatrici, con il rilancio della tesi delle cd. "consegne concordate" (tra gli scafisti e gli operatori umanitari), una tesi finora smentita da numerosi provvedimenti di archiviazione in altre indagini contro le ONG.[36] E proprio da queste indagini, prima che fossero archiviate, è emerso il sostanziale coinvolgimento delle autorità italiane ed europee nel coordinamento della Guardia costiera libica, dunque la finzione della zona SAR libica, ed il ruolo omissivo di Malta, in aperta violazione con i doveri di soccorso sanciti dalla Convenzione "SAR" di Amburgo del 1979, rispetto agli obblighi di organizzazione ed intervento stabiliti a carico di ogni Stato che abbia dichiarato una zona SAR di propria responsabilità. Malgrado i richiami dell'Alto Commissariato delle Nazioni Unite per i rifugiati (UNHCR) e malgrado quanto previsto dal Regolamento Frontex n. 656 del 2014, la circostanza che la Libia non possa offrire porti sicuri di sbarco, come la reiterata violazione del principio di non respingimento, sono diventati oggetto di rimozione collettiva e di negazione della giurisdizione, con un continuo rimpallo di responsabilità tra autorità nazionali ed europee.[37]

Nel frattempo, il livello di integrazione e comunicazione tra Frontex, le autorità marittime italiane e maltesi, le autorità di Tripoli si è talmente perfezionato che sembra ormai scontato, dopo la creazione di una zona SAR "libica", comunicata nel 2018 all'IMO (Organizzazione internazionale del mare), che tutti i comandanti delle navi civili che soccorrono naufraghi in acque internazionali, comprese in quella zona, debbano concludere le loro attività di salvataggio obbedendo agli ordini di riconsegna dei naufraghi impartiti dalle tante guardie costiere libiche. Autorità eterogenee che molte indagini giornalistiche e importanti passaggi giurisprudenziali, come il procedimento Open Arms ancora aperto presso il Tribunale di Ragusa, ritengono assistite e coordinate da assetti italiani ed europei, in quanto la Libia non dispone ancora oggi di una Centrale unificata di coordinamento dei soccorsi in mare (MRCC). I fatti ed i documenti che stanno emergendo dalle intercettazioni raccolte a ridosso dell'indagine giudiziaria sugli operatori umanitari della nave Iuventa (e altri) a Trapani, e che ancora di più potrebbero emergere se si dovesse arrivare al

[36] Procura della repubblica presso il Tribunale di Palermo, DDA, Richiesta di archiviazione del 28 maggio 2018, < https://www.giurisprudenzapenale.com/wp-content/uploads/2018/06/palermo-ong.pdf> (06/21)

[37] Sui rapporti tra la giurisdizione statale e la responsabilità per le azioni di ricerca e salvataggio (SAR), vedi M. Barnabò, "Verso una sovrapposizione tra zona SAR e giurisdizione statale?", <https://www.europeanpapers.eu/en/europeanforum/verso-sovrapposizione-tra-zona-sar-e-giurisdizione-statale> (06/21).

processo, sembrano comunque capovolgere gli schemi accusatori delle procure che continuano ad indagare sulle ONG e piuttosto potrebbero fornire elementi per mettere sotto accusa i decisori politici e gli agenti statali che hanno dato attuazione al Memorandum d'intesa con il governo di Tripoli e con la sedicente guardia costiera libica. Come afferma Matteo de Bellis, ricercatore presso Amnesty International,[38]

> gli europei non possono incaricare una nave di soccorso di sbarcare in Libia – è illegale – quindi hanno creato un sistema in base al quale gran parte del coordinamento dei respingimenti viene svolto dagli europei, con risorse europee, ma usando i libici come una cortina fumogena legale. È accettabile che gli stati dell'UE ingannino il diritto internazionale e rimandino le persone alla tortura senza essere responsabili?

Il Rapporto dell'Alto Commissario per i diritti umani delle Nazioni Unite Colville pubblicato nel mese di dicembre del 2020 [39] rilancia la richiesta di una moratoria su tutte le intercettazioni e i respingimenti in Libia. Questo l'accorato appello: "In conformità con le nostre linee guida recentemente pubblicate su COVID-19 e sui migranti, ribadiamo che gli Stati devono sempre rispettare i loro obblighi ai sensi dei diritti umani riconosciuti dal diritto internazionale e del diritto dei rifugiati". Secondo Rupert Colville[40], nonostante il COVID-19, le operazioni SAR (ricerca e salvataggio) dovrebbero essere mantenute e lo sbarco rapido assicurato in un porto sicuro (*place of safety*), garantendo al contempo la compatibilità con le misure di sanità pubblica. Come si conciliano queste posizioni con il mantenimento di una zona SAR riservata alle autorità di Tripoli, che non controllano per intero neppure il loro territorio nazionale e che hanno dimostrato di non sapere garantire i soccorsi in mare e trattamenti dignitosi ai naufraghi riportati a terra? Non è ormai assodato che la Libia, nelle sue diverse articolazioni territoriali e politiche, ancora oggi, non può garantire alcun luogo di sbarco sicuro *(place of safety)*? Come si possono ignorare le responsabilità delle autorità italiane ed europee che, con sofisticati sistemi di sorveglianza elettronica, sempre più integrati, riescono a tracciare la maggior parte delle imbarcazioni, anche di piccole dimensioni, in navigazione nel Mediterraneo centrale, comunicandone la posizione alla sedicente Guardia costiera libica? Quale giurisdizione potrà affermarsi per la tutela dei diritti fondamentali delle persone che vengono intercettate nelle acque internazionali del Mediterraneo centrale e riportate a terra, in Libia, dove vengono sistematicamente esposte ad altre gravissime violazioni dei diritti umani?

---

[38] M. De Bellis, "Tortura e violenze sui rifugiati in Libia: il fallimento delle politiche europee", <https://www.amnesty.it/tortura-e-violenze-sui-rifugiati-in-libia-il-fallimento-delle-politiche-europee/> (06/21).

[39] IOM, "*COVID-19 Control Measures, Gap in SaR Capacity Increases Concern About 'Invisible Shipwrecks"',*<https://www.iom.int/news/covid-19-control-measures-gap-sar-capacity-increases-concern-about-invisible-shipwrecks> (06/21).

[40] Nazioni Unite*,"UN rights office concerned over migrant boat pushbacks in the Mediterranean",* <https://news.un.org/en/story/2020/05/1063592> (06/21).

5. La responsabilità degli Stati, il ruolo di Frontex e la giurisdizione sulle acque internazionali

Con riferimento al rispetto degli obblighi di soccorso in acque internazionali e quindi di sbarco dei naufraghi in un luogo sicuro (*place of safety*), alla luce delle strette forme di cooperazione tra gli Stati consentiti dai sistemi di controllo elettronico delle frontiere dopo gli avvistamenti ed i tracciamenti aerei sul Mediterraneo centrale, si pone quindi la questione della giurisdizione e delle responsabilità nei casi di violazione dei diritti fondamentali.[41] Come ricorda la Risoluzione n. 1821 del 21 giugno 2011 del Consiglio d'Europa (sull'intercettazione e il salvataggio in mare dei domandanti asilo, dei rifugiati e dei migranti in situazione irregolare), la nozione di "luogo sicuro" non si può limitare alle navi soccorritrici, né può essere ridotta alla mera protezione fisica delle persone, ma "comprende necessariamente il rispetto dei loro diritti fondamentali» (punto 5.2.) che, pur non essendo fonte diretta del diritto, costituisce un criterio interpretativo imprescindibile del concetto di "luogo sicuro" nel diritto internazionale". Un Rapporto più recente del Consiglio d'Europa ribadisce questi principi[42]. Lo stesso concetto di luogo sicuro di sbarco individuato dalle Convenzioni internazionali è adesso ripreso da una importante sentenza della Corte di Cassazione, che nel caso Rackete ha specificato la portata del soccorso in acque internazionali come adempimento di un dovere imposto dal diritto internazionale.[43]

Il trasferimento delle responsabilità di coordinamento delle operazioni di ricerca e salvataggio ad un'altra autorità nazionale SAR come avviene con la indicazione delle autorità libiche come responsabili degli interventi di "soccorso" nel Mediterraneo centrale deve garantire comunque un intervento di salvataggio quanto più tempestivo possibile, e il rispetto del divieto di sbarco in un porto non sicuro. Se uno Stato riceve notizia di un evento di soccorso e non ci sono altre autorità statali, in grado di garantire un porto di sbarco sicuro, che intervengono tempestivamente, non si può escludere che questo Stato eserciti un controllo effettivo sulla vita delle persone, e quindi che su questa attività di controllo si instauri una giurisdizione che potrebbe implicare un possibile giudizio di responsabilità. [44]

Non sembra dunque possibile continuare a declassare gli interventi di ricerca e salvataggio a meri "eventi di immigrazione irregolare". Le persone che si trovano a bordo di imbarcazioni fatiscenti e sovraccariche nelle acque del Mediterraneo centrale sono tutte in una condizione di pericolo immediato (*distress*) per cui non appare legittimo limitare gli interventi al monitoraggio ed al tracciamento della rotta. In acque internazionali, quando una imbarcazione sovraccarica e senza dotazioni di

---

[41] I. Papanicolopulu, "The Duty to Rescue at Sea, in Peacetime and in War: A General Overview", *International Review of the Red Cross*, 2016, p. 495 ss.

[42] M. Delli Santi, "Il Rapporto del Commissario per i diritti umani del Consiglio d'Europa sulle politiche migratorie. Rilievi politici e giuridici", *Diritto, Immigrazione e Cittadinanza*, 2021, p. 219.

[43] In argomento si rinvia ad A. Del Guercio, "Migrazioni via mare, luogo di sbarco sicuro e principio di *non-refoulement",* in questo Volume.

[44] S. Trevisanut*, "Is there a right to be rescued at sea? A constructive view,* cit., *supra* note 20.

sicurezza, versa in una situazione di pericolo immediato (*distress*), non si possono spacciare come attività di contrasto dell'"immigrazione clandestina" interventi di soccorso che le autorità statali sono obbligate a garantire per salvaguardare la vita umana. La ripartizione delle zone SAR e gli accordi bilaterali non possono prevalere sull'esigenza di salvare quante più vite possibile. La lotta contro l'immigrazione irregolare si potrebbe realizzare con maggiore efficacia colpendo nei loro territori, soprattutto in Libia, le bande criminali che operano senza essere contrastate dalle autorità statali, spesso nella più totale impunità.

La "finzione" di una zona SAR riconosciuta al governo provvisorio di Tripoli, dunque, non può reggere ancora a lungo. I libici sono ancora privi di una vera Centrale unificata di coordinamento, ancora allo stato di progetti finanziati dall'Unione Europea, ma dispongono soltanto di un Centro congiunto di ricerca e salvataggio (JRCC) e sono le autorità europee che garantiscono il tracciamento della maggior parte delle imbarcazioni in navigazione nel Mediterraneo centrale. Questa circostanza, che emerge sia dalle attività di indagine della magistratura che dai rilievi più recenti operati dalle navi e dagli aerei delle ONG, non solleva gli Stati costieri, una volta che siano informati della presenza dell'imbarcazione in acque internazionali, dagli obblighi di ricerca e soccorso in mare.[45] La ripartizione delle zone SAR non può ritardare, o peggio evitare, interventi di salvataggio che sono dovuti in base al diritto internazionale del mare, ed in particolare in base alla Convenzione SAR di Amburgo del 1979, e dei relativi emendamenti, che impongono coordinamento ed assistenza delle navi soccorritrici in vista dello sbarco dei naufraghi in un porto sicuro[46]. La pretesa zona SAR "libica" non corrisponde ancora agli standard internazionali, né ad uno stato unitario, la Libia, che rispetti il diritto di asilo ed i migranti in transito, e che disponga di una Centrale operativa nazionale di coordinamento per i soccorsi (MRCC).

6. Conclusioni

La considerazione integrata dei sistemi di sorveglianza elettronica gestiti dalle autorità militari europee, e la ripartizione fittizia delle zone di ricerca e salvataggio (SAR) nel Mediterraneo centrale, risultano di fondamentale importanza per verificare la lesione dei diritti fondamentali delle persone migranti che subiscono i respingimenti collettivi "delegati" alle motovedette della sedicente Guardia costiera libica. Probabilmente i promotori delle politiche dei "porti chiusi", e della collaborazione con le autorità libiche, ritengono che il settore maggioritario della popolazione, anche a fronte delle diffuse conseguenze economiche e sanitarie della pan-

[45] Si rinvia, sugli obblighi di protezione a carico degli Stati europei, a F. De Vittor, "Responsabilità degli Stati e dell'Unione europea nella conclusione di accordi per il controllo extraterritoriale della migrazione", *Diritti umani e diritto internazionale*, 2018, 223 ss.

[46] E. Mezzasalma, "Una nuova concezione dell'obbligo di salvataggio in mare alla luce della sentenza della Cassazione sul caso Sea Watch 3?" <https://www.giurisprudenzapenale.com/wp-content/uploads/2020/04/Mezzasalma_gp_2020_4.pdf> (06/21).

demia, rimanga ormai indifferente rispetto alle stragi che si continuano verificare in mare, ed agli abusi che subiscono le persone intercettate in acque internazionali e ricondotte in Libia. Il tema degli "sbarchi" rimane ancora, purtroppo, un elemento trainante di propaganda elettorale e questa circostanza rende più difficile la soluzione dei problemi nel rispetto del diritto internazionale ed europeo.

Non si può tuttavia cancellare il principio di legalità, in modo da sovvertire il sistema gerarchico delle fonti del diritto, che pone al vertice le norme cogenti di diritto internazionale, che mirano alla salvaguardia della vita in mare, recepite anche in Italia per le leggi di attuazione e per effetto del dettato costituzionale (art.117 Cost.).

La sentenza di condanna dell'Italia da parte della Corte europea dei diritti dell'Uomo, nel caso Hirsi, deciso nel 2012, affermava la responsabilità dello Stato anche quando i suoi agenti operino al di fuori delle acque territoriali, quando le persone vittime dei respingimenti si trovino sotto "l'esclusivo controllo" di autorità riferibili allo stesso Stato, come si può verificare quando sono imbarcate a bordo di un mezzo civile o militare battente bandiera nazionale. Quanto abbiamo rilevato in tema di ripartizione delle zone SAR e di sistemi elettronici di controllo delle frontiere potrebbe permettere di individuare precise responsabilità, quando le autorità marittime e politiche statali abbiano il controllo esclusivo su persone che vengono individuate e e tracciate in acque internazionali a bordo di imbarcazioni prive di bandiera verso le quali si può configurare immediatamente un dovere di soccorso.

Quando parliamo di queste responsabilità, che possono anche risultare inizialmente esclusive poi condivise tra più Stati, facciamo riferimento sia a possibili responsabilità penali rilevanti a livello nazionale, che alla commissione di crimini contro l'umanità, dei quali, con particolare riferimento alla sedicente Guardia costiera "libica" si sta già occupando il Tribunale Penale internazionale.[47] Per eludere queste responsabilità non sarà possibile riqualificare gli eventi di soccorso (SAR) in "attività migratorie illegali" o in "eventi migratori", né criminalizzare ulteriormente l'operato di quelle Organizzazioni non governative che, per il ritiro dei mezzi di soccorso statali, sono rimaste le uniche possibilità di salvezza per chi si trova costretto ad intraprendere la rotta del Mediterraneo centrale.

Si potrebbe dunque affermare la giurisdizione di uno stato europeo, e dunque della Corte Europea dei diritti dell'Uomo e della Corte di Giustizia UE, nei casi in cui, anche al di fuori delle frontiere nazionali, come nelle acque internazionali, autorità statali di un paese frontaliero esercitino il controllo esclusivo su persone che, trovandosi a bordo di imbarcazioni prive di bandiera nazionale, non si trovano soggette alla giurisdizione di altro stato. Un controllo esclusivo che ricorre da parte del primo Stato che riceve informazioni sulla presenza di persone in difficoltà nelle acque internazionali, e che si realizza con maggiore evidenza quando le attività di intercettazione e di tracciamento elettronico consentono di determinare l'intervento

[47] R. Noury, "Guardia costiera libica indagata dalla Corte penale internazionale. Che farà l'Italia?", <https://lepersoneeladignita.corriere.it/2017/07/02/guardia-costiera-libica-indagata-dalla-corte-penale-internazionale-che-fara-litalia> (06/21).

della guardia costiera libica, decidendo così la destinazione delle imbarcazioni cariche di naufraghi, ed in definitiva arrivando a negare il loro diritto al soccorso (e in molti casi alla vita). Come avviene nei confronti dei migranti che si trovano su imbarcazioni ubicate in alto mare dopo segnalazioni inviate, anche da Frontex, alla centrale di coordinamento della Guardia costiera italiana, oltre che alle autorità maltesi e libiche. Rimangono le perplessità già rilevate sul Decreto interministeriale del 7 aprile 2020 che sembrerebbe presupporre il riconoscimento formale di una zona di ricerca e salvataggio (SAR) libica, obbligando i comandanti delle navi private, che operano attività SAR in quella zona, di avvertire le "autorità competenti", per non rischiare, in caso di mancato coinvolgimento di queste autorità, un divieto di ingresso nelle acque italiane.

Il recente rafforzamento degli accordi di cooperazione con la Guardia costiera libica ha ulteriormente accresciuto il rischio che la normativa italiana, e le prassi operative che ne sono seguite, possano entrare in conflitto con il diritto internazionale e aggirare i divieti ribaditi dalla Corte europea dei diritti dell'Uomo nel caso Hirsi. La Corte di Strasburgo ha ritenuto, proprio a partire dal caso Hirsi, che

> gli Stati non possono aggirare gli obblighi della CEDU stipulando accordi con Stati terzi, ma al contrario, devono assicurarsi della compatibilità con la CEDU di tutti gli altri obblighi assunti per non esporsi al rischio di condanne per inadempimento da parte della Corte, in particolare rispetto ai divieti di respingimento derivanti dagli articoli 3 e 4 del Quarto Protocollo allegato alla CEDU.

Quanto rilevato sulla sorveglianza aerea ed elettronica, sulla "finzione" della zona SAR "libica" e sulle modalità di intervento delle motovedette che salpano dalla Tripolitania, assistite dall'Italia con la missione Nauras della Marina militare, fa ritenere che precise responsabilità di intervento persistano anche durante e dopo le attività di intercettazione operate dai libici. Almeno nei casi in cui si riesca a provare che le motovedette libiche operino sotto il coordinamento delle autorità italiane ed europee, come nel caso in cui la stessa Guardia costiera libica abbia comunicato di non potere effettuare gli interventi SAR nella vastissima area che le è stata riconosciuta.

Si potrebbe anche profilare una responsabilità internazionale dell'Italia per la violazione dei diritti umani in Libia, anche se il riconoscimento della giurisdizione da parte della Corte europea dei diritti dell'Uomo non appare certo agevole.[48] Ma si potrebbe valutare il comportamento delle autorità europee alla luce degli obblighi di soccorso sanciti dal Regolamento Frontex n.656 del 2014, radicando in questo modo come sede giurisdizionale la Corte di giustizia UE di Lussemburgo. Sembra anche importante richiamare la possibilità di denunciare ai Commissari ai diritti umani delle Nazioni Unite e del Consiglio d'Europa le violazioni più gravi degli obblighi

[48] G. Pascale, "Esternalizzazione delle frontiere in chiave antimigratoria e responsabilità internazionale dell'Italia e dell'Ue per complicità nelle *gross violations* dei diritti umani commesse in Libia", *Studi sull'integrazione europea,* XIII (2018).

di soccorso rilevanti sotto il profilo del diritto internazionale. Anche in assenza di un procedimento giurisdizionale, l'autorevolezza dei Rapporti internazionali può emergere davanti ai tribunali, come si è già verificato in Italia, proprio con riferimento a procedimenti penali avviati nei confronti di Organizzazioni non governative.

Di certo tutte le autorità politiche e militari coinvolte nei "*pull-back*" delegati alla guardia costiera libica non possono ignorare la sorte delle persone che vengono riportate a terra e riconsegnate alle stesse milizie dalle quali erano riuscite a fuggire. Ed anzi, in molti casi, la riconduzione in Libia dei migranti intercettati in mare appare frutto di un intento preciso di chi conclude accordi con le autorità libiche alle quali si riconosce una zona SAR di competenza esclusiva, e non soltanto una mera eventualità, o un effetto collaterale.

Non si può accettare in definitiva una sospensione a tempo indeterminato di qualsiasi esercizio della giurisdizione sulle persone che si trovano in acque internazionali. Fino al punto di negare, oltre al principio di non respingimento (art.33 Convenzione di Ginevra), il diritto al soccorso ed una qualsiasi tutela del diritto alla vita, ignorando del tutto il divieto di tortura e di altri trattamenti inumani o degradanti, sancito a livello internazionale, europeo e nazionale.

Alcuni casi di abbandono in mare, seguito dall'intervento delle motovedette libiche in acque internazionali, potrebbero configurare una vera e propria omissione di soccorso. Come osserva Flavia Pacella,[49] con riferimento agli accordi di cooperazione con le autorità libiche volti a contrastare l'immigrazione via mare, potrebbero profilarsi specifici profili di responsabilità delle autorità italiane per crimini contro l'umanità anche di fronte al Tribunale penale internazionale, in quanto "la conclusione degli accordi in parola potrebbe astrattamente integrare, sia sotto il profilo dell'actus reus che della mens rea, la particolare forma di responsabilità dell'agevolazione materiale ex art. 25(3)(c) dello Statuto di Roma".[50]

In base alle Convenzioni di Amburgo sul "SAR" ed alla Convenzione SOLAS, recepite nell'ordinamento italiano e richiamate dal Regolamento europeo Frontex n.656 del 2014, esercitano una giurisdizione le autorità statali che vengono a conoscenza dell'esistenza di persone che sono in difficoltà su una imbarcazione fatiscente e sovraccarica in alto mare, dunque in una condizione di *distress* che impone soccorsi immediati, che comunque vanno attivati anche se gli Stati competenti non danno risposte o reagiscono tardivamente. Non si può certo sostenere che le stesse

[49] F. Pacella, "Cooperazione Italia Libia : Profili di responsabilità per crimini di diritto internazionale", *Diritto Penale Contemporaneo*, 2018 <https://archiviodpc.dirittopenaleuomo.org/d/5838-cooperazione-italia-libia-profili-di-responsabilita-per-crimini-di-diritto-internazionale> (04/21).

[50] Secondo Flavia Pacella*,* cit.,"è opportuno sottolineare che la cooperazione con la Libia potrebbe configurare anche la responsabilità internazionale dello Stato italiano. Il diritto internazionale consuetudinario prevede due condizioni cumulative affinché uno Stato sia internazionalmente responsabile per l'assistenza fornita ad un altro Stato nella commissione di un illecito: (i) che lo Stato c.d. assistente agisca con la consapevolezza delle circostanze dell'atto illecito posto in essere dallo Stato c.d. assistito e (ii) che l'atto sia, in astratto, internazionalmente illecito anche se commesso dallo Stato c.d. assistente. Nel caso di specie, come autorevolmente sostenuto altrove, entrambi tali requisiti sembrano essere prima facie soddisfatti."

autorità politiche e militari ignorino la sorte dei migranti trattenuti in Libia contro la loro volontà o quanto accade alle persone che sono intercettate in mare, spesso più un sequestro che un evento di soccorso, e riportate a terra. Diverse sentenze degli organi giurisdizionali italiani attestano la gravità degli abusi subiti dai migranti intrappolati in Libia e l'elevato livello di collusione tra le milizie ed i trafficanti, proprio nei passaggi cruciali dai porti ai centri di detenzione (e viceversa). Non si può nascondere, proprio sulla base delle testimonianze convergenti dei sopravvissuti che sono riusciti ad arrivare in Italia, confermate in diversi procedimenti penali.[51] quanto avviene nei centri di detenzione libici dopo il blocco in mare e la riconduzione a terra. Ed è in base a queste stesse testimonianze che si potranno accertare le responsabilità per la complicità italiana ed europea, anche quando non si riscontri un diretto coordinamento, con le attività di intercettazione in mare da parte della sedicente Guardia costiera "libica", che si è voluto ritenere autorità di controllo esclusivo nella zona SAR "libica", inventata nel 2018 proprio a seguito del Memorandum d'intesa tra l'Italia e il governo di Tripoli concluso nel febbraio del 2017. Un preciso disegno politico, avallato anche dall'Unione Europea con la Dichiarazione di Malta del 3 febbraio 2017,[52] che si è tradotto in prassi omissive che hanno leso i diritti fondamentali delle persone migranti ed in molti casi hanno prodotto naufragi con migliaia di morti e dispersi. Che altrimenti si sarebbero forse evitati, o quanto meno ridotti, se gli Stati avessero continuato a garantire un immediato coordinamento delle operazioni di ricerca e salvataggio (SAR), finalizzato alla salvaguardia della vita umana in mare, anche nelle acque internazionali, indipendentemente dalla ripartizione delle zone SAR, come si era verificato nel 2014 (con l'operazione *Mare Nostrum*).

[51] G. Mentasti, "Centri di detenzione in Libia: una condanna per il delitto di tortura (art. 613 bis c.p). Nuove ombre sula cooperazione italiana per la gestione dei flussi migratori", *Sistema Penale*, 2 ottobre 2020 <https://www.sistemapenale.it/it/scheda/mentasti-gip-messina-centri-detenzione-libia-condanna-carcerieri?out=print> (04/21).

[52] Dichiarazione di Malta del 3 febbraio 2017, <https://www.consilium.europa.eu/it/press/press-releases/2017/02/03/malta-declaration/> (06/21).

MARITIME CYBER SECURITY REGULATION: INTERNATIONAL AND INDUSTRY CO-REGULATION

Fenella Billing - Christian Frier

1. Introduction

Ships are increasingly relying on different types of technologies, such as digitalization, system integration and automatization, as well as advanced ship-shore communication networks. This phenomenon is even more obvious in the emerging area of automated vessels. Technological developments are praised for bringing general safety improvements and cost reduction by facilitating the infrastructures of global trade. This includes, *inter alia*, the use of smart contracts and electronic transport documents, as well as more advanced ship/port logistic systems, reducing time in port. The advantages of both operational technologies (OT) and especially information technologies (IT)[1] are thus evident in a trade that requires private stakeholders, ports and flag State administrations to interact globally and exchange critical data. However, as with other breakthrough technologies, these advantages have come with the risk of maritime cyber-attacks, which paradoxically add to the existing vulnerabilities in modern shipping.[2]

Maritime cyber risk refers to the extent a technology asset or network could be compromised or threatened by cyber-attacks.[3] This could include perpetrators identifying the *locus* of ships by monitoring navigation systems with the intention to launch physical attacks, blocking or withholding data to the detriment of the owners or even perpetrators seeking to take control over a ship's operational technologies. These risks are real: recent statistics show a 900 percent increase in cyber-attacks in past three years.[4] Accordingly, experts suggest it is not a question *if* an organization will be the target of cyber-attacks, but *when* it occurs and *how* well the ship is protected. Recognizing that international merchant shipping is instrumental to global trade, where an estimated 90 percent of all cargo is at some point carried by ships, a successful cyber-attack can not only affect the individual stakeholders involved, but also has huge potential to impact critical infrastructure. Accordingly, cybercrime

[1] The definitions of OT and IT technologies are explained in more detail in section 3.

[2] See for instance C. Corcione, *Maritime Piracy and New Technologies,* in this Volume; and R. Hopcraft, K. M. Martin, "Effective Maritime Cybersecurity Regulation – The Case for a Cyber Code", *Journal of the Indian Ocean Region*, 2018, pp. 354-366, p. 355; A. Rana, "Commercial Maritime and Cyber Risk Management", *Safety and Defense*, 2019, pp. 46-48.

[3] IMO, MSC-FAL.1/Circ.3, Annex, p. 1.

[4] Marine Insight (20 July 2020) <https://www.marineinsight.com/ shipping-news/maritime-cyber-attacks-increase-by-900-in-three-years/#> (08/21).

prevention – preventing cyber-attacks from happening – through cyber risk management has been a significant focus of international and industry-based regulation.[5]

Maritime cyber risk regulation is 'multi-layered'. It comprises an international legal framework with broad treaty obligations in different public law sources at the international and regional (European Union) levels, as well as multiple non-treaty instruments issued by the International Maritime Organization (IMO), the UN's specialized agency promoting safety and antipollution initiatives.[6] In addition, this framework is supported by a torrent of industry self-regulation, crafted by maritime industry organizations aimed at enabling private actors to ensure their own risk management practice is well-considered and effective. The existence of these two levels of 'public' and 'private' regulation, each comprising various layers, raises the question of fragmentation, such that conflicts or gaps may exist between the obligations or standards raised.

The issue of fragmentation is generally considered in relation to the (horizontal) splintering of obligations between various law-making treaties within specialised international law 'regimes'.[7] However, this paper raises a form of vertical fragmentation in the multilayering of obligations and standard-setting in cyber risk management, from the international State-driven level down to the industry-driven bottom-up approach. Nevertheless, the goal is the same: to examine whether this results in negative effects in standard-setting, namely regulatory 'conflicts' or a 'loss of overall perspective',[8] which may lead to confusion, differential standards or regulatory gaps.[9] Therefore, this paper has two main objectives. The first objective is to identify and discuss the multi-layer legal framework. The second objective is to present our understanding of the functioning of the regulatory system in place. The aim is to reflect on the adequacy of the system and highlight pertinent questions for the future of cyber risk management regulation.

2. The International Legal Framework

It is a prerequisite for operating a ship that the vessel is deemed seaworthy, meaning it can perform the intended voyages without, *inter alia*, endangering the

[5] International Association of Classification Societies (IACS), Recommendations on Cyber Resilience, IACS Rec. 2020/Corr.1 2020, p. 2 (hereinafter IACS recommendations).

[6] A. Blanco-Bazán, "IMO – Historical Highlights in the Life of a UN Agency", *Journal of History of International Law,* 2004, pp. 259-283, p. 259.

[7] International Law Commission (ILC*), Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law, Report of the Study Group of the ILC Finalized by Martti Koskenniemi*, Report to the UN General Assembly A/CN.4/L.682, 13 April 2006, para. 5 ff.

[8] ILC 2006 para 8.

[9] T. Pankakoski and A. Vihma speak of negative and positive aspects of fragmentation in "Fragmentation in International Law and Global Governance: *A Conceptual Inquiry*", 12/1 *Contributions to the History of Concepts,* 2017, pp. 22-48, p. 22.

safety of life. Seaworthiness is an integral part of 'safety at sea', in addition to maintaining communications, preventing collisions, manning, training, decent labour conditions and protection against marine pollution. This is codified in public international law, including the United Nations Convention on the Law of the Sea (UNCLOS) and the treaty framework negotiated under the auspices of the IMO.[10] This organization provides institutional infrastructure allowing for a significant treaty-making role with high numbers of signatory States, as well as the adoption of technical codes and guidelines from the different IMO committees, collectively allowing for international harmonisation of shipping legislation.[11] This Section, therefore, lays out the relevant international public law framework for safety at sea and prevention of cyber-attacks, commencing with the UNCLOS and other treaties dealing with safe shipping, presenting the IMO's non-treaty instruments and concluding with some remarks on European Union (EU) cyber security regulation.

2.1. Flag state Responsibility under UNCLOS

The jurisdictional starting point of shipping regulation is the flag State principle as set forth in UNCLOS. Although these provisions deal with flag State duties in the context of Part VII entitled 'High seas', they nevertheless attach to flag States generally as a consequence of registration. A flag State that has granted nationality under art. 92, has prescriptive and principal enforcement powers in accordance with art. 94. This lengthy provision stipulates areas of responsibility in relation to administrative, technical and social matters 'concerning the ship', including registration.[12] In particular, Article 94(3) requires states to take necessary measures in relation to, including: (a) the construction, equipment and seaworthiness of ships; (b) manning and training of crew; and (c) maintenance of communications and collision prevention. The inclusive list is often referred to as the 'CDEM' standards.[13] Article 94(4) elaborates further and requires flag State measures concerning: (a) pre and post-registration surveyance of ships' equipment and instruments for safe navigation; (b) appropriately qualified master and officers concerning navigation, communications and equipment; and (c) properly trained master, officers and crew with applicable knowledge of international regulations about safety of life, prevention of collisions and maintenance of communications. Cyber risk prevention for the purpose of ship resilience is encompassed in the concept of seaworthiness.

The requirements set out in art. 94(3) and (4) should also be viewed in light of

[10] See Art. 94(3) and (4) UNCLOS.

[11] Blanco-Bazán, cit. *supra* note 6, pp. 259-260; for an historical introduction to the IMO, see also A. Chircop, "The International Maritime Organization" in D. Rothwell, A. Oude Elferink, K. Scott, and T. Stephens (eds.), *The Oxford Handbook of the Law of the Sea*, Oxford University Press, Oxford, 2015, pp. 416-517; R. Beckman, Z. Sun, "The Relationship between UNCLOS and IMO Instruments", *Asia-Pacific Journal of Ocean Law and Policy*, 2017, pp. 201-246, pp.202-204.

[12] Art. 94(1) and (2)(b) UNCLOS.

[13] CDEM is an abbreviation for construction, design, equipment and manning.

'generally accepted international regulations, procedures and practices' as pointed out in art. 94(5). This so-called 'rule of reference' effectively incorporates obligations found in other treaties or non-binding instruments and gives them the force of a treaty obligation under UNCLOS.[14]

Despite the importance of the flag State principle in UNCLOS, legislative competence of the flag State has arguably become less important throughout the last century, at least in part as a result of widespread internationalisation and adoption of treaties.[15] In addition, flag States are generally reluctant to promote domestic regulation and standards for vessels flying their flag, as this requires administrative machinery most States lack. Furthermore, there is also a risk of re-flagging if flag State compliance is burdensome or more costly compared to other registries. These factors, coupled with the need for technical detail without a direct State interest, has resulted in a lack of national level regulation and propelled a bottom-up industry self-regulation, which is well reflected in SOLAS.

2.2. SOLAS Convention and the ISM Code

A starting point to considering IMO's treaty-based regulation on safety is Chapter IX of the Convention on the Safety of Life at Sea (SOLAS) about 'Management for the Safe Operation of Ships'. Ratification of SOLAS by 164 states represents 99.19% of the world's transport tonnage, reflecting the Convention's purpose of protecting international merchant shipping 'as a whole'.[16] The extent of treaty-instruments in the maritime domain comes from an understanding that international merchant shipping cannot be effectively regulated by national regulation alone.[17] Yet treaties, which cannot be amended easily, are not always well-suited sources of law for highly detailed technical regulation. Given that no two vessels are truly similar and that ships are operated under a range of changing conditions, the treaty-based framework is supplemented by a 'sub-layer' of detailed regulation. Accordingly, under the SOLAS safe ship operation umbrella, the International Safety Management (ISM) Code has been adopted and made mandatory.[18]

With its coming into force in 1998, the purpose of the ISM Code was to provide an international standard for ensuring 'safety at sea, prevention of human injury or loss of life, and avoidance of damage to the environment … and to property.'[19] In addition, to meet the demands of European States in the Paris MOU,[20] the IMO

[14] D. Guilfoyle, *Part VII. High seas in UN Convention on the Law of the Sea: A commentary,* Proelss edt., Oxford, 2017, p. 712.

[15] T. Falkanger, H.J. Bull, and L. Brautaset, *Scandinavian Maritime Law: The Norwegian Perspective*, *4th edition*, Scandinavian University Press (Universitetsforlaget), Oslo, 2017, pp. 56-57.

[16] O. Daum, "Cyber Security in the Maritime Sector", JMLC 2019, p. 14.

[17] K.M. Siig, Private classification societies acting on behalf on the regulatory authorities within the shipping industry, SIMPLY 428, 2016, p. 221.

[18] International Management Code for the Safe Operation of Ships and Pollution Prevention (ISM Code).

[19] ISM Code para 1.2.1.; see also Daum, p. 13.

[20] Paris Memorandum of Understanding.

amended SOLAS and inserted Chapter XI-1, extending port state control beyond merely inspection of technical certificates to also be concerned with operational seaworthiness.[21] This amendment led to the adoption of the International Ship and Port Facility (ISPS) Code. In turn, under these mandatory codes, several non-binding cyber-security specific IMO guidelines have also been adopted.

In complying with the *ISM Code*, the company operating the vessel must draw up a safety management system (SMS) for each ship. The SMS is one of the central features in ensuring regulatory compliance at the industry level that originates from the international harmonisation framework. The cornerstone of the legally binding ISM Code is the requirement that 'the company', being shipowners, charterers or any other person with responsibility for a ship, establishes a safety management system (SMS), 'ensuring compliance with mandatory rules and regulations' and that 'applicable codes, guidelines and standards' recommended by the IMO, State administrations, classification societies and industry organisations, are 'taken into account'.[22]

In accordance with the principles laid down in Chapter IX SOLAS, 'the goal [of the ISM Code] is to have shipowners develop a culture of safety at all levels …[which] is not only given priority, but is also documented.' Paragraph 1.2.2.2 of the Code stipulates that one of the safety management objectives is 'to establish safeguards against all identified risks;' and in paragraph 1.2.2.3 to 'continuously improve safety-management skills of personnel ashore and aboard ships, including emergency preparation for safety and environmental protection.' Daum provides a number of examples of cyber-attacks in the maritime domain and rightly points out that such attacks 'may affect the safe operation of a ship', thus posing 'identified risks'.[23]

An SMS that is specifically adapted for the circumstances of the individual ship requires the owner or operator to ensure documentation and verification of regulatory compliance.[24] This is in line with international shipping law in general, providing private actors with both a certain margin of interpretation but also a potential leeway for non-uniform standard setting. Under the IMO Guidelines, flag States are responsible for oversight of the SMS and formally do so through the issuing of Safety Management Certificates (SMCs).[25] However, rather than having their own officers conduct the surveys required for issuing the certificates, the practice has developed whereby the flag State administration issues certificates on the basis of surveys conducted by industry-based classification societies using industry guidelines and standards (discussed at Section 4 below). Due to the private interests of the classification societies, questions may arise about the effectiveness, transparen-

[21] Blanco-Bazán, cit. *supra* note 6, p. 282.

[22] ISM Code, para 1.2.3; see section 4 below about the practice between ship owners and classification societies

[23] Daum, cit. *supra* note 16, p.14; on the role of IMO codes, see also Hopcraft and Martin, cit. *supra* note 2, pp. 358-359.

[24] Falkanger et al., cit. *supra* note 15, p. 87.

[25] IMO Resolution MSC.428(98).

cy and validity of the State supervision. This practice that has developed around the operationalisation of the ISM Code and SMS requirements clearly demonstrates that shipping regulation relies heavily on private entities: ship owners have a significant role in formulating the compliance standards passed down from the UNCLOS and SOLAS; flag States rely on classification societies to endorse them.

2.3. The IMO's Non-treaty Instruments

In addition to facilitating treaty-making, the IMO should be recognised as a 'clearing house' for discussions and collaboration between States and a range of private stakeholders with consultative status, in particular shipping associations and shipowners.[26] As Kirgis points out, the IMO is an organisation that finds ways 'to channel members' conduct in discrete areas, for example, through codes and guidelines which, while not mandatory per se, can obtain a similar effect to formal rules.'[27]

According to the IMO Convention, which serves as the constitutional basis of the IMO's structure and competence,[28] in addition to proposals for or amendments to safety regulations, the IMO's Maritime Safety Committee (MSC) must develop recommendations and guidelines and submit them to the Council. Thus, the trend for multiple recommendations on almost all subjects relevant to States and industry stakeholders alike has especially been the case in areas that are not comprehensively governed by a parent convention.

In 2017, IMO issued two guidelines on maritime cyber risk management, including a resolution with 'high-level recommendations', encouraging States to implement by 1 January 2021 or first annual verification.[29] The MSC issued the 'Maritime Cyber Risk Management in Safety Management Systems Resolution' (IMO Cyber Risk Resolution),[30] which requires ship owners and operators to assess cyber risks and implement relevant measures across all functions of their safety management system. As a supplement to the Resolution, the MSC also released the 'Guidelines on Maritime Cyber Risk Management (IMO Cyber Risk lines).[31] Both documents leave much to the interpretation of the Company responsible for the individual ship's Safety Management System (SMS).

---

[26] See for example Hopcraft, Martin, cit. *supra* note 2, p. 359.

[27] F.L. Kirgis, "Specialized Law-Making Processes", in O. Schater, C.C. Joyner (eds), *United Nations Legal Order* Cambridge University Press, Cambridge, 1995, Vol 1, p. 161; on formal compared with less formal types of IMO regulation, see A. Petrig, "Unconventional Law for Unconventional Ships? The Role of Informal Law in the International Maritime Organization's Quest to Regulate Maritime Automated Surface Ships", in N. Klein (ed), *Unconventional Lawmaking in the Law of the Sea* Oxford University Press, Oxford, forthcoming 2021.

[28] 1948 Convention on the International Maritime Organization, 6 March 1948, entered into force 17 March 1958.

[29] Maritime Safety Committee, Maritime Cyber Risk Management in Safety in Safety Management Systems, MSC. 428(98), No. 2, 16 June 2017.

[30] International Maritime Organization (IMO) Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems, MSC 98/23/Add.1, 16 June 2017.

[31] IMO, *Guidelines on Maritime Cyber Risk Management*, MSC-FAL.1/Circ.3, 5 July 2017.

The documents are non-binding recommendations about countering current and emerging cyber risks as well as vulnerabilities in the maritime industry at an 'acceptable' level, in relation to costs and benefits.[32] The Guidelines identify IT structures, in on-shore infrastructure as well as on ships, that are vulnerable to cyber-attacks, including cargo handling systems, container tracking systems, communication systems, passenger service systems as well as crew-introduced equipment such as USB sticks.[33] Daum summarises the main cyber risk management measures to include appointment of cyber security officers, initiating protocols, implementing safeguards and automatic defensive measures, subsequent improvement and conducting cyber-attack sensitive training.[34]

Implementation of the IMO Guidelines 'depends on the voluntary commitment of the maritime actors.'[35] Though non-binding, the Guidelines carry the same 'internationally embracing legal purpose' as in the ISM Code and SOLAS of ensuring safe operation of ships, including protection of human life and the marine environment.[36] Nevertheless, their non-binding nature has led to some criticism based on the time-consuming and expensive nature of cyber security measures and the lack of legal consequences, meaning that some actors will not implement the measures or will implement them to a significantly lesser degree than flag and port State and industry counterparts.[37] These approaches can undermine the general level of protection of international merchant shipping.[38]

2.4. European Union Regulation

The EU has nominated maritime cyber security to be a critical infrastructure concern. The European Union Agency for Cybersecurity (ENISA) focuses on providing guidance to Operators of Essential Services (OES), in particular ports, given their critical transport functions.[39] The 2016 NIS Directive[40] focuses on in-

[32] Daum, cit. *supra* note 16, pp. 2-3, interpreting 'acceptable' to mean 'bare bones', and p. 11 ff; see further A. Chopra and M. Chaudary "Risk Management Approach", in *Implementing an Information Security Management System. Security Management Based on ISO 27001 Guidelines*, Apress, 2020, pp. 86-87.

[33] International Maritime Organization (IMO), Guidelines on Maritime Cyber Risk Management, MSC-FAL.1/Circ.3, 5 July 2017, 2.1.1 and 2.1.6; see further Daum, cit. *supra* note 16, p. 6 ff; and Rana, cit. *supra* note 2, pp. 46-47.

[34] Daum, cit. *supra* note 16, p. 12, referring to the IMO, *Guidelines on Maritime Cyber Risk Management*, MSC-FAL.1/Circ.3, 5 July 2017, 3.5 and 2.1.5.

[35] Ibid, p. 14.

[36] Ibid, p. 14.

[37] On the potential ineffectiveness of relying on flag states' role in countering illegal, unreported and unregulated (IUU) fishing, see T.-H. Tai, S.-M. Kao and W.-C. Ho, "International Soft Law against IUU Fishing for Sustainable Marine Resources: Adoption of the Voluntary Guidelines for Flag State Performance and Challenges for Taiwan", *Sustainability,* 2020, p. 6013.

[38] Daum cit. *supra* note 16, p.15.

[39] ENISA, *Cyber Risk Management for Ports: Guidelines for Cybersecurity in the Maritime Sector*, December 2020.

[40] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 con-

creasing network and information system security at the national level of the member states.[41] In part, it does so by requiring OES to conduct risk assessments that, together with implementation of mitigation measures, promotes a risk management culture.[42] While some EU member states issue guidance to OES about how to conduct cyber risk assessments, most port operators use one of a number of industry standards.[43] The ISPS Code requires OES to conduct port facility security assessments and plans. However, ENISA found a 'fragmented approach in the performance of cyber risk assessments' across EU ports, and significant gaps for the port facilities complying with the ISPS Code, key areas being left unassessed.[44] While the primary focus of the international framework is flag States and, significantly, industry stakeholders, the principal EU-focus is EU port States.

3. Industry Self-Regulation

Industry self-regulation,[45] self-governance[46] and similar concepts, where drafters are also the addressees' of instruments, are common in most sectors. Furger especially highlights that the overwhelming majority of *safety* standards are created by private actors within different industries, including the maritime industry.[47] The trend of involving private actors in setting standards, to ensure compliance with mandatory regulation within highly technical areas, is no exception in shipping. Obligating private actors in the ISM Code to also take 'non-treaty instruments' into account, referring to IMO guidelines and self-regulation, has invited an important role for industry-self regulation in modern shipping.

In most areas of shipping, industry guidelines are functioning simply as recommendations supplementing existing regulation, without adding new rules. Their main scope and justification are to operationalize duties deflected from public law, by placing the responsibility internally in the ship owning organization. Occasionally, in areas without a substantive parent convention, it seems feasible to argue that guidelines can even create new duties. An example of industry rulemaking follows from the set of IMO guidelines addressing the use of private armed guards and pira-

---

cerning measures for a high common level of security of network and information systems across the Union, 19 July 2016 OJEU L 194/1 (NIS Directive).

[41] D. Gliha, "Maritime Cybercrime – 21st Century Piracy' Issue 20 2017, p. 233.

[42] ENISA 2020, 8.

[43] ENISA 2020, 8.

[44] ENISA 2020, 9.

[45] See R. Baldwin, M. Cave & M. Lodge, *Understanding Regulation: Theory, Strategy and Practice* Oxford University Press, Oxford, 2012, pp. 137-38; for the use of self- and co-regulation, see F. Cafaggi, A. Renda, "Public and Private Regulation Mapping the Labyrinth", *CEPS Working Document No. 370*, 2012, abstract.

[46] E. R. DeSombre, *Flagging Standards.Globalization and Environmental, Safety, and Labor Regulations at Sea,* MIT Press, Cambridge MA and London, 2006, p. 181-182.

[47] F. Furger, "Accountability and systems of self-governance: the case of the maritime industry", *Law and Policy*, 1997, p. 8.

cy. The guidelines from 2011 to industry stakeholders stated that: "the absence of applicable regulation and industry self-regulation coupled with complex legal requirements governing the legitimate transport, carriage and use of firearms gives cause for concern."[48] Today, a decade later, no changes have been made to the treaty-framework, whereas IMO and maritime industry organizations have issued a range of best management practices, codes of conduct, guidelines and standards within the field.[49] Some of these are now endorsed in the IMO guideline intended for flag States, thus reinforcing the importance and legitimacy of privately crafted instruments. Harrison, in an earlier study, points to both ballast-water and anti-fouling systems as other areas in which non-treaty instruments have functioned as a prelude to the negotiation and adoption of formal treaty obligations.[50] A more recent example of industry self-regulation filling in a void is the Polar Code.[51] The Code applies to navigation in polar waters, as additional requirements were needed with increased navigation in the harsh and pristine environment. The Code was first issued as a set of IMO guidelines with input from industry stakeholders, which later became mandatory under both the SOLAS (safety) and MARPOL (pollution prevention) conventions.[52] Ultimately, the Code thus became a mixture of overall goals and technical rules.[53] This has resulted in a mix of vague and precise provisions, which are likely to have implications for the interpretation of the Code, by admitting a 'margin of interpretation' for flag States.[54] The Code's more vague goal based approach is partly solved by mandating the International Association of Classification Societies (IACS) to adopt rules in different areas, such as "ice-classes".

Returning to maritime cyber security, the current state of regulation resembles the situation of repression of piracy by the use of private armed guards a decade ago.[55] Given the *lex generalis* regulation and the absence of a substantive parent convention or applicable annexes, the overall system relies heavily on the involvement of private actors. In the following sub-sections, the principal industry stakeholders and instruments are discussed in more detail, examining whether these instruments are simply facilitating operationalization and division of responsibilities and tasks, or actually adding additional duties.

---

[48] 23 May 2011, Annex p. 1]. The Passage Is still Upheld in the Current Revised Version, 25 May 2012.

[49] See for example BMP5.

[50] J. Harrison, *Making the Law of the Sea: A Study in the Development of International Law*, Cambridge University Press, Cambridge, 2011, pp. 164-165.

[51] For a general introduction to the Polar Code, see Ø. Jensen, "The International Code for Ships Operating in Polar Waters: Finalization, Adoption and Law of the Sea Implications", *Arctic Review on Law and Politics*, pp. 60-82.

[52] C. Frier & K. Østergaard, "The Polar Code's suitability as legal protection against negative externalities in the Arctic as part of the Polar Silk Road" in Keyuan Zou, Shicun Wu and Qiang Ye (eds.), *The 21st Century Maritime Silk Road. Challenges and opportunities for Asia and Europe*, Routledge, pp. 117-119.

[53] Certain parts of the Polar Code are not made mandatory, see Jensen, cit. *supra* note 51, pp. 67-68.

[54] Jensen, cit. *supra* note 51, p. 70.

[55] B. Feldtmann, C. Frier & P. Mevis, "National Models for Regulation On-Board Protection od Vessels: Some Cross-cutting Issues", *Erasmus Law Review*, 2018, pp. 267-271.

3.1. Maritime Industry Guidelines

The Guidelines on Cyber Security Onboard Ships[56] is a specific set of maritime industry guidelines produced and supported by several maritime trade associations.[57] The drafters are similar to the group of stakeholders responsible for the widely accepted Best Management Practice on deterrence of pirate-attacks,[58] which are referenced or incorporated by several European flag States.[59] The industry associations' position is fortified by their consultative status to the IMO. Theses associations often operate on both regional and global levels. Some associations are organized along jurisdictional lines, whereas other associations are focusing on specific activities or trades.[60] In general, these associations offer a wide range of services to their members, including issuing guidelines of different kinds and scope.

The cyber security guidelines entail a number of principles and introduce a six-step cyber risk management plan, including awareness and preventive measures, management and operation measures, and incident response planning.[61] The guideline also distinguishes between two main groups of technologies. Information technology (IT) refers to the use of networks and devices to store, retrieve and transmit data and information, whereas operational technology (OT) covers the hardware and software that directly controls and monitors the ship, which must function independently of the IT system onboard.[62] Another important aspect of the guidelines for stakeholders is to divide roles, responsibilities and tasks, especially those related to vessel-operation that are outsourced to third parties. The guidelines thus continue to map out "job descriptions" based on the SMS. A common denominator is that all descriptions included in the scheme are offshore, ranging from top management to IT managers and fleet managers. Each category entails one responsible party and multiple supporting parties. For instance, the ship IT manager is both responsible for OT/IT risk assessment and for ship infrastructure, whereas the managing director is responsible for wider policy considerations. In terms cyber risk management training of crew, the Marine HR manager is considered responsible.

In summary, the guideline is both lengthy and very detailed compared to the IMO cyber guideline or any of the public law sources. To illustrate the best man-

---

[56] The first version of the Industry Guidelines on Cyber Security Onboard Ships was published in 2016, with version 2 in July 2017, version 3 in December 2018 and version 4 in Dec 2020.

[57] BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC)

[58] Best Management Practices to Deter Piracy and Enhance Maritime Security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea, version 5 (BMP5).

[59] See Feldtmann, Frier and Mevis, cit. *supra* note 55, p. 267-271.

[60] For example, INTERTANKO (the International Association of Independent Tanker Owners) organises specifically tanker owners

[61] Cyber-security Guideline, Version 4, p. 5.

[62] Ibid., p. 7.

agement character of the industry's own guidelines, it is already revised in a fourth version, also demonstrating the flexibility of industry regulation to adjust to current and emerging needs.

3.2. Standardisation

Two other instruments of particular importance are standards issued by the International Standardization Organization (ISO) and the National Institute of Standards and Technology (NIST), respectively. Both of these are referred to on IMO's webpage. NIST is a US institution, whereas ISO is a non-governmental international organization with more than 150 national standardisation bodies.[63] Both bodies are issuing an array of industry-based standards.

The notion 'standard' is given different meanings in legal texts and commercial settings. In general, it refers to a minimum level of quality and/or a norm for continuous measurement, such as the CDEM standards in Article 94 UNCLOS (explained at 2.1 above). The notion is also used to indicate a lower threshold of quality, such as 'sub-standard shipping', typically referring to vessels not adhering to the applicable CDEM standards. However, standards coming from a standardisation organization refer to the process of developing and implementing often technical rules, which are drafted through a *bottom-up* process under the organizational structure of NIST, ISO or another standardisation organization. In essence, standards are instruments of regulation, which are largely 'invisible'.[64]

The predominant standards dealing with cyber security are *ISO/IEC-27001* and the *cyber security-standard framework* from NIST. The NIST standard framework has been developed in a collaborative effort involving stakeholders from the industry, academia and government. Just like the NIST-standard the ISO-27001 is also generic, in the sense that it can be applied to all companies, regardless of industry.[65] While ISO have a long-standing tradition of negotiation and issuing shipping standards, *ISO-27001* is not drafted in that setting. This means neither of the standards specifically consider the challenges of safeguarding ships.

The ISO sets out requirements for an information security management system (ISMS). The main standard is supported by more specific standards, for example, on how to manage the security of assets such as financial information, employee details or information entrusted by third parties. The standards are very much about creating a security culture, just like the industry guidelines. The main difference is that the ISO standard does not govern the division of responsibilities of ships. This means the industry guideline is more helpful for ship operations. However, consid-

---

[63] For a historical introduction to ISO, see C. N. Murphy, J. Yates, *The International Organization for Standardization (ISO): Global Governance through Voluntary Consensus*, Routledge, 2009, chapter 1.

[64] S. Wood, *The International Organization for Standardization in Business Regulation and Non-state Actors: Whose Standards? Whose Development*?, Routledge, 2013, p. 83.

[65] ISO/IEC 27001 is widely known, providing requirements for an information security management system (ISMS), though there are more than a dozen standards in the ISO/IEC 27000 family.

ering the extent of information sharing, the company can also benefit from being ISO or NIST-compliant.

4. Cyber Security Regulation: Fragmentation or Co-regulation?

The multi-layered nature of regulation that has grown in relation to ship safety is also characteristic of the regulation of maritime cyber security. In the absence of a more comprehensive international treaty, multiple layers of regulation have been added, each layer providing a degree more specificity than the previous. The industry self-regulation is adapted to the circumstances of the individual ship and the owner is obliged to ensure documentation verifying regulatory compliance, which is vetted by a classification society. Classification society selects and supplies the regulations, industry standards and best practises with which ship owners must comply, 'with the ship owner potentially being subject to civil law consequences in case of non-compliance.'[66] Classification societies can even be 'authorised to issue administrative rules' on behalf of a State.[67] Thus, in some areas of maritime regulation, as Siig states, classification societies can have a '(possibly controlling) influence' on regulatory enforcement and even the content of the rules.[68] Furthermore, contractual obligations between ship owner and cargo owner as well as stipulated terms of marine insurance potentially give shipping standards *de facto* status of binding obligations.[69] The multi-layered regulation in addition to the potentially influential role of classification societies and insurers, calls for an assessment of whether new rules relating to the same compliance areas are being created in different types of cyber security regulation, or whether the various layers are merely providing additional detail. New rules come with the potential of creating conflict or simply a lack of cohesiveness and confusion. A lack of regulatory alignment in relation to maritime cyber risk prevention may be evident if ship owners can only comply with one instrument or standard by failing to comply with another.[70] Such a concern relies on a clear line between making new rules that are not broadly aligned or developing more detailed but aligned system of rules.

Having explained the various layers of regulation above, there appears to be a significant connection between, firstly, the ISM Code and the SMS and, secondly, industry self-regulation. Even at the level of the ISM Code and the accompanying SMS, these international obligations do not provide for operationalisation on their own. They speak to industry actors and create a need for operationalisation at the industry level. Thus, while acknowledging a broader state interest in secure infrastructure and maritime cyber security in general, it appears that the principal role of the international tier of cyber security regulation is to harmonise the assignment of

[66] Siig, cit., *supra* note 17, p. 218.
[67] Ibid.
[68] Ibid.
[69] See further Petrig, cit. *supra* note 27, pp. 12-14.
[70] For inspiration, see ILC 2006 para 24.

responsibility for compliance to industry actors, acknowledging that States cannot be effectively accountable for what happens in relation to each individual ship. While the existence of areas of cyber security that have been overlooked and remain unassessed cannot be ruled out – just as ENISA found concerning fragmentation in regulation of EU ports (at 2.4 above) – it appears that the non-treaty instruments are a necessary and significant auxiliary to international regulation. Therefore, it appears that the relationship between the international cyber security framework and industry self-regulation is best understood as one of 'co-regulation'. This term encompasses a dual approach, where the international regulation ensures harmonisation in relation to operationalisation of cyber risk management, whereby the apportioning of responsibility for compliance is laid down in industry guidelines. Accepting that this co-regulation is a better conceptualization, the question is whether this is a positive or negative development? The answer to this question will depend on the extent of substantive alignment following all the way down from the broad flag-State obligations in UNCLOS, to the significant international harmonisation in IMO-treaties and guidelines and to the various layers of private regulation. Another question, in the absence of conflicts, is whether fragmentation has led to regulatory gaps - either as a patchwork of gaps that appear geographically, between regions or locations, or between sectors; or general gaps, that appear internationally, in relation to aspects of cyber risk management that as yet have not been adequately addressed.

5. Conclusions

Despite the multiple layers of international regulation, the picture is only partially complete without the industry guidelines. The importance of international law and the IMO as a regulatory body in steering a degree of harmonisation in relation to a risk that must be perceived as global – a product of globalisation – cannot be underestimated. However, on its own, international regulation is too broad and states are not and cannot be in a position to provide the operational guidance necessary for adaption to specific ships. This two-tier multi-layered approach can be understood as co-regulation, with both the international framework and the industry self-regulation contributing to the collective legal framework.

Defining acceptable standards of safety for a new technology is a process ridden with technical uncertainties. This is especially the case when new technology emerges, for which past experience is lacking. In such cases, operationalization of the international cyber security regulation is achieved by conducting extensive negotiations between all major industry interests, strongly influenced by the classification society's technical experts. This means that a range of private stakeholders, not least the maritime associations, may all be involved in the rule-making and implementation process, although to varying degrees.

MARITIME PIRACY AND NEW TECHNOLOGIES

Carlo Corcione

1. Piracy Background and Framework

Piracy is perhaps present since the starting of human activities at sea.[1] It is agreed with Bellamy that piracy, "like wars, has been around throughout history, for as long as humanity has been able to record events and issues, and probably even longer before then."[2] Kothari aptly reports that the maritime industry has always been vulnerable to maritime crimes including piracy, armed robbery, hijacking, stowaways, illegal migrants, narcotics, arms smuggling, fraud, and others.[3]

Political instability, poor economic conditions, difficulty in finding other sources of wealth, and a lack of security by the local governments[4] are among the main causes for piracy growth. Piracy, together with armed robbery and terrorism, is the main threat to maritime security.[5] The main difference between piracy and maritime terrorism is that the former is motivated by financial gain while the latter has a political agenda.[6] The main difference with armed robbery is geographical with piracy international and armed robbery national.[7]

The peak of modern piracy, mainly centered in Somalia, was between 2007 and 2011 with 300 to 400 vessels attacked per year, 20% of which were hijacked.[8] Ver-

[1] Thucydides, in writing the Peloponnesian war in 431 BC, mentioned a pirate attack in the ancient Greece waters. Thucydides, *History of the Peloponnesian War*, Prometheus, Amherst New York, 1998, p. 32.

[2] C. Bellamy, "Maritime Piracy", *The RUSI Journal*, 2011, pp.78-83.

[3] Kothari, Bhim S., "The Role of Technology in Maritime Security: A Survey of its Development, Application, and Adequacy" (Dissertation 362, World Maritime University 2008).

[4] A. Shortland & F. Varese, "The Protector's Choice: An Application of Protection Theory to Somali Piracy", *The British Journal of Criminology*, 2014, pp. 741-764. L.M. Diaz, L. & B. Dubner, "Foreign Fishing Piracy vs. Somalia Piracy Does Wrong Equal Wrong", *Barry Law Review*, 2010, pp. 73-96.

[5] Maritime security has been defined as, "The state of being free from the threat of unlawful acts such as piracy, armed robbery, terrorism, or any other form of violence against ships, crews, passengers, port facilities, offshore installations, and other targets at sea or in coastal areas." Dalakis Dimitrios. Adriana Nordfjeld, Maximo Mejia, "Port and martime Security" (ECLAC/WISTA/ Red MAMLA/ Latin American E-Forum Opportunities in the Americas and the Caribbean beyond the 2020 global emergency Conference, remotely from Chile, July 2022).

[6] Ibid.

[7] Armed robbery instead is, "Any illegal act of violence or detention or any act of depredation, or threat thereof, other than an act of piracy, committed for private ends and directed against a ship or against persons or property on board such a ship, within a State's internal waters, archipelagic waters and territorial sea; (Resolution A.1025(26) (Annex, paragraph 2.2).

[8] T. Treves, "Piracy, Law of the Sea, and Use of Force: Developments off the Coast of Somalia", *European Journal of International Law,* 2009, pp. 399-414.

ga explains piracy is nothing more than a business activity, a criminal business activity to be precise, but nonetheless a business activity. Thus, as all other business activities, it has a specific business model.[9] The most structured piracy business model has been the Somali one, with annual revenues of 200 million of dollars and profits around 120 million of dollars in the years between 2008 and 2012.[10] Piracy started with the intention of preventing foreign vessels from invading waters and destroying fishing activities. Indeed, Somali pirates called themselves *badaadinta badah* (saviors of the sea).[11] Piracy causes shipping companies to pay higher premiums and armed guards. This is reflected in hire costs and renders ripple effects down the logistics chain. Therefore, eventually the whole supply chain incurs the cost of piracy not only the maritime part of it.[12]

Analyzing piracy geographically, Southeast Asian and West African piracy focuses on commercial products and petty cash. Especially in Somalia, piracy has (or possibly had) a professional and broader business model including ransoms and activities on land.[13] It is reported that in the second quarter of 2020, piracy at sea increased by 25% compared to the same quarter of 2019, with almost 100 vessels reporting incidents involving piracy or suspected piracy. Approximately 80 vessels were boarded, 10 reported attempted attacks, six vessels were fired upon, and one vessel was hijacked. In terms of crew, more than fifty were kidnapped, over 23 made hostage, ten assaulted, and six injured.[14]

Piracy these days is predominantly in West Africa (specifically the Guinea Gulf), where it essentially means violent thefts and kidnapping (at the moment approximately 90% of worldwide crew kidnapped is in this area) instead of vessel hijackings for ransom (as in Somalia). In West Africa pirates attack outside national waters and, under local law, ships cannot enter a port in this region with private armed guards onboard.[15] Therefore, escort vessels work with local navies. Currently there is no standard contract available for escort vessels but The Baltic and International Maritime Council (BIMCO) is working on a draft.[16]

Only ten years ago, Somali coasts, the Gulf of Aden, and the strait of Bab al Mandab were the centre of piracy yet are now calmer. However, as the Evergreen disaster in Suez has demonstrated, ships are weary of passing and when do so carry

[9] E. Verga, "Sparrows' Generation", Longitude, 2015, pp. 112-119.
[10] Ibid.
[11] Ibid.
[12] Ibid.
[13] Ibid.
[14] Standard P&I Club Bulletin, September 2020 Maritime Security Piracy.
[15] To the feasibility of entering high risk areas such as West Africa, usually insurers recommend to ship owners to comply fully with all the recommended BMP planning, voyage, and reporting procedures and to take all relevant steps as identified in a voyage specific risk assessment to ensure the safety of crew and cargo.
[16] *The Baltic and International Maritime Council (BIMCO)*, https://www.bimco.org/news/contracts-and-clauses/20210203-bimco-to-develop-standard-contract-for-security-escort-vessel-employment (03/21).

armed guards onboard.[17] To fight piracy in Somalia, the solution was (and still is in different areas) to employ armed guards. In 2013, one result of the coordination between private parties (vessels owners, cargo owners, and other stakeholders) and maritime non-state actors (P&I clubs) was the approval from different flag states of armed guards provided by private companies. The relationship between the shipping companies and the armed guards is largely regulated by a contract called GUARDCON.[18] It is notable no vessel with armed guards onboard has been highjacked in Somalia and armed guards are a great deterrent against piracy.[19]

Southeast Asia, also known for piracy, saw a decrease in 2019 with only 25 cases.[20] The Americas (Colombia, Ecuador, Haiti, Mexico) and North Africa (Libya) have recently witnessed random attacks, probably related to random bands of pirates rather than structured business organizations.[21]

From a legal and regulatory perspective, piracy is effectively a cross-border issue as maritime security is effectively cross-jurisdictional. On an international level, piracy at sea has been tackled primarily as a problem of naval law enforcement, governed by international maritime law.[22]

Piracy is seen as a *crimen iuris gentium* internationally regulated by the Geneva Convention of 1958 and the United Nation Convention on the Law of the Sea (UNCLOS) of 1982. Effectively, as aptly mentioned by Azubuike, these conventions codify the relevant customary international law of piracy. Therefore, even non-ratifying States are bound by these rules.[23]

The International Maritime Organization (IMO), created to assist maritime safety,[24] approximately 30 years ago also started to address maritime security. In terms

---

[17] *Forbes*, <https://www.forbes.com/sites/roberthart/2021/03/26/shipping-companies-stuck-near-suez-are-reportedly-alerting-us-navy-over-piracy-risks/?sh=7b8b0e7f3e36> (03/21).

Riparte L'Italia <https://www.ripartelitalia.it/greta-tellarini-effetti-blocco-canale-di-suez/> on the relationship between the piracy in west Africa and piracy in Somalia (03/21).

[18] See C. Corcione "Guardcon: contratto standard per l'ingaggio di guardie armate a bordo delle navi", in E. Turco Bulgherini and F. Salerno(eds.), *Infrastrutture e navigazione: nuovi profili della sicurezza marittima ed aerea. Convegno di* studio, Aracne Editrice, Roma, 2013.

[19] Ibid.

[20] Standard bulletin cit. note 14.

[21] Ibid.

[22] C. Bueger, T. Edmunds, "Beyond Seablindness: A New Agenda for Maritime Security Studies" *International Affairs*, 93(6), pp. 1293-1311 <https://doi.org/10.1093/ia/iix174.> It could be relevant here to specify the difference between maritime law and the law of the sea. Maritime law refers to the entire body of laws, rules, legal concepts and processes that relate to the use of marine resources, ocean commerce, and navigation. While the law of the sea is a body of public international law governing the geographic jurisdictions of coastal States and the rights and duties among States in the use and conservation of the ocean environment and its natural resources. P. Hoagland, J. Jacoby, M.E. Schumacher, Law of the Sea, Encyclopedia of Ocean Sciences (2nd Edn), edited by John H. Steele, Academic Press, 2001, pp. 432-443.

[23] L. Azubuike, *International Law Regime Against Attack*, Annual Survey of International & Comparative Law, Art. 4, pp. 43-59.

[24] Bueger cit. *supra* note 22, Maritime safety deals with accidents caused by internal factors such as crew errors, technical issues with the ship and incidents by chance, while security addresses essentially external threats.

of the latter, it has launched various initiatives, including an anti-piracy plan, issued guidelines, and adopted the International Ship and Port Facility Security Code (ISPS Code2).[25]

Piracy is the only maritime crime that gives right to any state to exercise its own jurisdiction in high seas. There are different ways to classify piracy. Jones does so according to severity: [26]

i. Opportunity Crimes
ii. Low Level Armed Robbery
iii. Medium Level Armed Assault and Robbery
iv. Major Criminal Hijacking

The International Maritime Bureau (IMB) instead considers piracy according to how the attack is conducted. In particular:

i. Opportunity theft by persons who manage to gain access to the vessel, in port or at anchor, and steal anything handy such as paint or mooring ropes
ii. Planned robbery, alongside, at anchor or underway, targeted mainly at money, crews' personal effects, and ships' equipment, often carried out by increasingly organized, determined and well-armed gangs
iii. Permanent hijacking of ships and cargoes with crews sometimes being murdered cast adrift or held to ransom.[27]

It is relevant to note here that there are many efforts by major shipping countries to fight piracy. China for instance, which has an economic interest in Africa, continuously conducts counterpiracy operations in the area of Somalia with naval task forces as well as deploying military forces to protect Chinese vessels as well as foreign ones.[28] However the piracy issue is not solved as yet and, as further explained in the paper, the advent of new technologies will pose new threats for the shipping community in fighting piracy in the future.

2. Piracy and New Technology

New technologies provide all sectors advantages and disadvantages[29] and could apport several advantages to the maritime industry, transforming it into a safer and cleaner industry[30] but it can also present drawbacks on both practical and regulatory

[25] Ibid.

[26] S. Jones, *Maritime Security: A Practical Guide,* The Nautical Institute, London, 2006, pp. 16-18.

[27] J. Abhyankar, "Piracy and Armed Robbery at Sea: An Overview" in M. Q. Mejia & J. Xu, *Proceedings of the International symposium for Coastal Zone Piracy and Other Unlawful Acts at Sea*, WMU Publications, Malmö, 2007, pp. 97 – 119.

[28] J. Henry, "China's Military Deployments in the Gulf of Aden: Anti-Piracy and Beyond", *Asia Visions*, IFRI Policy Paper no. 89, 2016, pp. 14–23.

[29] M.E. Porter, "Technology and Competitive Advantage", *Journal of Business Strategy*, Volume 5, Issue 3, 1985, pp. 60-78.

[30] Ibid.

aspects.[31] The world is going towards the omnipresence of Internet and Wi-Fi connections and therefore all activities will somehow engage in Artificial Intelligence (AI), cloud computing, and big data; all of which are becoming increasingly relevant in companies' daily life.[32] Shipping nor piracy will be exempt from this revolution.

New technology for the scope of this paper is considered a new technique that brings more improvement than existing technology (improvement in terms of competitive advantage or simply reducing costs).[33] This paper takes into consideration new technology in shipping only in reference to maritime piracy, arguing that the concept of piracy (at least as it is under today's legal framework) will have to be revised when new technology is fully implemented in the shipping sector. It is anticipated that new technology will not defeat piracy because it will be adopted by the pirates as it will be adopted by the shipping sector; in other words, every time the shipping sector becomes more technologically sophisticated, so will piracy.

To narrow the scope, it is argued that two main groups of new technology will affect piracy, Artificial Intelligence and Big Data, which together form the main technology behind the autonomous vessels (this paper uses the terms vessels and ships interchangeably).

AI could be exploited by the international community (and therefore also the maritime community) to predict and prevent security attacks.[34] AI should help to detect new threats in advance, to plan appropriate defenses in advance.[35] AI could anticipate and mitigate attacks improving voyage planning and improve the post incident procedure in terms of aggregating information.[36] In other words, AI could identify suspicious patterns based on past incidents and prepare a defense against new ones.[37]

Big data and data sharing are relevant technologies to achieve an integrated approach to common information sharing.[38] A good example of data hub is the Piracy Reporting Centre from IMB, which coordinates the reporting of piracy attacks and it is a central hub that shares information among private and states.[39] For instance,

---

[31] J. Clarke, *The Changing Face of Maritime Law and Risk—Cyber, E-Commerce, Automation of Vessels: Shipping Laws and Regulations*, Global Legal Group, London, 2020, p. 1.

[32] U. Holtgrewe, "New Technologies: The Future and the Present of Work in Information and Communication Technology", *New Technology, Work and Employment*2014, pp. 9-24.

[33] B. H. Hall, K. Beethika, "Adoption of New Technology" (2003) Working Paper 9730 http://www.nber.org/papers/w9730 (11/11). For the meaning of technology see J.J. Salomon, "What is technology? The Issue of its Origins and Definitions", *History and Technology*, 1984, pp 113-156.

[34] H. M. Roff, "Advancing Human Security through Artificial Intelligence" *International Security Department and US and the Americas Programme*. Research paper, 2017.

[35] Ibid.

[36] *Safety4Sea*, <https://safety4sea.com/steering-with-artificial-intelligence-to-combat-maritime-piracy/> (03/21).

[37] Ibid.

[38] Ex-post Evaluation of PASR Activities in the field of Security and Interim Evaluation of FP7 Security Research Maritime Security and Surveillance - Case Study, 2011, United Kingdom <www.cses.co.uk> (03/21).

[39] Part I: An Overview of Trends, Costs And Trade,2014, (United Nations Conference on Trade

technology called Track-Before-Detect could limit piracy as detecting the skiffs commonly used by pirates and Advanced Digital Signal Processing could identify pirates' sudden change of route thus detecting false alarms.[40]

Supply chains are constantly working to be more efficient and in this respect sharing data between all stakeholders is essential.[41] For example, international action against piracy off the coast of Somalia has been facilitated by the information-sharing platform Mercury, which allows various stakeholders—including national navies, international missions, and civil information-sharing centres—to communicate with each other through synchronous text-based chat, with a live feed on naval operations and piracy incidents providing real-time data to all participating actors.[42]

Reporting pirates' attacks has been brought forward by IMB, other non-state actors, and flag States via the Declaration Condemning Acts of Violence Against Seafarers.[43] The use and process of data together with artificial intelligence form the core of the technology used for autonomous vessels. It is believed that autonomous vessels will be disruptive for piracy. Autonomous vessels are not navigating yet but they will soon.[44] The Nippon Foundation has budgeted almost 10 billion US dollars for shipping technology to develop autonomous technologies over the next 20 years.[45] When referring to autonomous vessels, the main advantages are lower costs (crew and insurance premiums) and some believe a reduced risk of piracy attack. While this could be true in terms of hostage-taking,[46] it is argued that with autonomous vessels pirates will find another way to take advantage of the vessels and the concept of piracy will be revised rather than becoming *extinct,* so to speak.

It should be said that there is no uniform definition of ship nor vessel. Indeed, when talking about autonomous vessels, the word "vehicle" is often preferred. In any case, the general definitions of vessels do not clarify whether to be a vessel, there is the need to have a crew onboard.[47]

---

and Development, New York and Geneva, 2014).

[40] M. Mudric, The GUARDCON Contract, Knock-For-Knock Clauses, Dcfr and Unfair Terms (PART I): 21 JIML. 2015. See also G. Bevilacqua, *Counter Piracy Armed Services, the Italian System and the Search for Clarity on the Use of Force at Sea*, "The Italian Yearbook of International Law", p. 39.

[41] The maritime world is getting used to exchanging data in order to help preserve the ecosystem. Examples of this are The European Marine Observation and Data Network (EMODnet) https://emodnet.eu/en/what-emodnet (03/21) and The Sea Cargo Charter https://www.seacargocharter.org/wp-content/uploads/2020/10/Sea-Cargo-Charter-FAQ.pdf (03/21).

[42] Bueger cit. *supra* note 22.

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] Ibid.

[47] N. Klein, "International Law Studies, Maritime Autonomous Vehicles within the International Law Framework to Enhance Maritime Security", *Journal of Maritime Law & Commerce*, 2016; See also G. M. Gauci, "Is It a Vessel, a Ship or a Boat, Is It Just a Craft, Or Is It Merely a Contrivance?", *Journal of Maritime Law & Commerce*, 2016.

3. The Issue

The shipping sector will eventually fully adopt new technology and so will pirates. It can therefore be presumed that autonomous vessels will not be safe from pirates despite there not being a hostage risk because they will be liable to cyber-attacks that would most likely disrupt the operation of the vessel.[48] As a matter of fact, with the implementation of new technology in shipping, the exposure of ships to cyber-attacks increases.[49] Cyber-attacks will disrupt GPS systems, control systems, and data bases, and they will allow information to be stolen.[50] Pirates are already hacking into cargo details including bills of lading, which are becoming more and more electronic,[51] in order to disrupt vessels' schedules and make them so vulnerable that the pirates can board them and look for barcodes.[52]

Having stated the above and clarified that technology and business models (including pirates' business models) constantly evolve, from a legal perspective the definition of piracy is not.[53] It still related to two conventions from approximately sixty and forty years ago.

The two conventions define piracy as:

(a) [...] any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:

(i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;

(ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;

(b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;

(c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).[54]

Reading the definition of piracy above we can essentially summarize that piracy

---

[48] *The Baltic and International Maritime Council* (BIMCO), The Guidelines on Cyber Security Onboard Ships, 2020.

[49] K. Tam, Cyber-Risk Assessment for Autonomous Ships http://hdl.handle.net/10026.1/11245 International Conference on Cyber Security and Protection of Digital Services ("Cyber Security"), 2018.

[50] Many companies still do not report cyber-attacks as afraid customers will stop using their services. The shipping industry is usually very resistant to change and as such it still views cyber security as a cost that can be avoid while it should be seen as to prevent a much bigger cost.

[51] C. Corcione, *The Electronic Bill of Lading, The Key of the Warehouse in the Digital Era,* Aracne Editrice, Rome, 2021; N. Newman, Cyber Pirates Terrorise the High Seas, Engineering and Technology, 2019, pp. 54-57.

[52] Ibid.

[53] For an analysis on the current state of piracy definition see G. Bevilacqua, *Criminalità e sicurezza in alto mare*, Editoriale Scientifica, Napoli, 2017, 072.

[54] Art. 101 of Montego Bay Convention and Art. 15 of Geneva Convention.

is an illegal Act of violence, detention or depredation committed in high seas[55] by the crew or passengers of a private ship against another ship or persons or property onboard. It is argued that the whole definition as above will need to be revised when new technologies will take place and ships will be autonomous or remotely controlled.

About twenty years ago Professor Joseph Sweeney, wrote an article that, as visionary as it could sound, aimed at predicting the future of vessels 25 years later (i.e. by 2025). Reading the article, the vessel that Sweeney invented to make the case had a master, a chief mate, three junior mates, and seven crew members. There is no reference in the article to "unmanned ships" or "autonomous vessels" or "remote control vessels". Therefore, in the imaginary world of Professor Sweeney, vessels still had crew onboard. We are almost in 2025 and Sweeney is right in the sense that vessels still have crews. However, as anticipated and as stated by the Nippon foundation, by 2025 the aim is to have the first autonomous vessel and after more will follow.

This paper is not as ambitious as Professor Sweeney's one, but simply aims to test the definition of piracy against a scenario when (probably not too far in the future) autonomous (or remote control) vessels will be the norm thanks to AI and Big Data technologies, with the latter becoming consequentially also commodity. Pirates in fact follow commodity trends. They used to attack tankers but when oil prices crashed, they stopped.[56] Big Data has been defined "the oil of the 21st century" and thus pirates pay attention to it, focusing on shipping databases in order to obtain bar codes and container serial numbers.[57]

Having set the above one can now scrutinize the definitions of illegal acts of violence, detention and depredation, and the definition of autonomous ships.

Violence essentially means "actions or words which are intended to hurt people".[58]

Detention means holding of person or property in custody while depredation means "despoiling, ravaging, or plundering;".[59] In other words it is a brutal action.

Several academic discussions are taking place on the meaning of the word ship (or interchangeably vessel) in reference to autonomous or unmanned technology.

An autonomous ship is generally considered to be a ship that can navigate from one point to another without a crew onboard. This definition becomes more precise:

a) remotely operated autonomous ship—controlled remotely from ashore by a control centre that effectively (through data transmission and artificial intelligence) guides the ship to the destination;

---

[55] For private means.

[56] *Qz.com* https://qz.com/619281/oil-is-now-so-cheap-even-pirates-arent-stealing-it-any-more/ (03/21).

[57] D. Heilbing, "Societal, Economic, Ethical and Legal Challenges of the Digital Revolution: From Big Data to Deep Learning, Artificial Intelligence, and Manipulative Technologies", *SSRN Electronic Journal*, in: Jusletter IT 21 May 2015.

[58] According to the Cambridge Advanced Learner's dictionary.

[59] Ibid.

b) completely autonomous ship—using artificial intelligence and pre-programed instructions (the latter being the only human intervention in the process) to navigate from one point to another.[60]

In the above cases, data will be the core of the technology and perhaps the most appealing to steal and it is therefore fair to assume that pirates will prefer to board ships to steal data or, more probably, attack the control centre itself. The latter could be a literal attack or a cyber-attack.

Having highlighted this change of scenario, this paper argues that for future piracy cases involving autonomous ships, five main points need to be clarified.

The first point to be addressed is whether a ship without crew can be considered a ship in terms of international maritime piracy, in particular in terms of the definitions provided in the aforementioned Geneva Convention and UNCLOS.[61]

Secondly, it must be agreed whether an autonomous ship navigating at sea without humans onboard can still suffer act of violence, detention, or depredation, as it appears from the above analysis only humans can suffer such crimes.

Thirdly, there must be agreement as to whether stealing data onboard a vessel can fall under the current definition of violence, detention, or depredation.[62]

Fourthly, it is imperative to decide whether a cyber-attack (in other words without a physical action) to the ship's data base (or the ship's data in the control room) can be an act of maritime piracy falling under the terms, violence, detention, or depredation.

Fifthly, and considering the fact that a ship will be essentially controlled by a control room ashore, it must be decided whether a line between high seas and territorial seas can still be drawn when considering maritime piracy and armed robbery.

This paper argues that the current and future issue of maritime piracy is that it cannot be analyzed in isolation from cyber piracy and as such maritime piracy will no longer be a high sea issue but instead a supply chain issue. In the future, piracy might not be committed (or it will be only partially committed) at sea and it might not be an act of violence, detention, or depredation. Either piracy definition is changed or maritime piracy will continue to exist, but we will have even less control over it as we cannot define and in turn identify it.

It is reported that while piracy receives a wealth of interest from state and non-state actors, less attention is paid to the technology impact on piracy[63] and there is surely room for an academic debate followed by an international effort to clarify the new scenario.

---

[60] P.W. Pritchett, "Ghost Ships: Why the Law Should Embrace Unmanned Vessel Technology", *Tulane Maritime Law Journal,* 2015 pp. 197-225.

[61] UNCLOS does not define the word "ship" but in defining "pirate ship" (Article 103), it mentions that a pirate ship is intended to be under the control of a person (or persons) therefore it embraces the concept that a ship is with persons onboard, but this will change in the future. It should be seen whether control it means physical control or also remote control.

[62] In this respect, data collection marine objects must also be defined as they are currently not considered ships, yet they might turn out to be very relevant and appealing for future pirates.

[63] Bueger cit. *supra* note 22.

Agreeing with Percy and Shortland that piracy is ultimately a land issue,[64] and with Murphy that it is imperative to change politics perspectives on how to deal with it[65] this paper argues that isolating piracy only to the maritime leg of the supply chain will be a mistake.[66] The increasing importance of the link between what happens at sea and the whole trade behind it has been recently highlighted by the Evergreen case in the Suez Canal. The maritime leg is not the "backdrop to the stage on which the real action is seen to take place" nor simply "a means of connection between activities taking place at coasts."[67]

A feature of modern maritime security is in fact its interconnectivity. Most maritime security issues are not to be understood and addressed as problems of the maritime environment alone. Instead, they are invariably interlinked with challenges on land as well.[68] Accordingly, piracy is not a maritime transport issue anymore as defined by UNCTAD in 2014[69] but it comes from ashore and affects the whole supply chain. UNCTAD state that the issue of maritime piracy has developed into a multifaceted transnational security challenge.[70] This paper adds that it is also a multifaceted trans-sector challenge as it will entail transportation on one hand and technology/cyber risk on the other.

There is currently no international convention totally dedicated to piracy, and this must change as piracy is the first crime recognized as against international law and subject to universal jurisdiction.

4. Remarks and Future Research

Maritime piracy has always been present in the history as it has always adjusted itself to current times. International regulations should do the same. So far operations against piracy have been successful in reducing it (such as in Somalia). It is now important to delve deeper into what is the concept of piracy in the future and conceptualize its definition in order to provide a starting point for law makers in the future and revise conventions.[71]

From Barbarossa to Blackbeard from Jack Sparrow to Captain Philips piracy

---

[64] S. Percy & A. Shortland, "The Business of Piracy in Somalia", *Journal of Strategic Studies*, 2013, pp. 541-578.

[65] M. Murphy, "Somali Piracy: Not Just a Naval Problem", The Center for Strategic and Budgetary Assessments – CSBA. <http://www.csbaonline.org> (11/11).

[66] C. Corcione, *Third Party Protection in Shipping*, Informa Law, Routledge, London, 2019.

[67] S. Percy & A. Shortland cit. *supra* note 64.

[68] Ibid.

[69] United Nations Conference on Trade and Developments (UNCTAD), Maritime Piracy, Part 1: An Overview of Trends, Costs and Trade Related Implications, *Studies in Transport Law and Policy*, 2014 No. 1.

[70] Ibid.

[71] M. Ahmad, "Maritime Piracy Operations: Some Legal Issues"*, Journal of International Maritime Safety*, *Environmental Affairs, and Shipping*, 2020 pp 62-69.

has always been the perfect topic for movies and fictional stories.[72] However the reality is that piracy is a real criminal organization costing to the world economy over half a billion dollars per year.[73]As all criminal organizations, piracy keeps evolving its business model[74] and it has already started to embrace new technologies. There is the need for a regulation that considers both types of crimes (piracy and cyber piracy) together.[75] It would be difficult to imagine pirates in the future demanding ransoms or stealing money from the master safe locker.[76] Shipping is continuously adopting more technologies with the aim to be more efficient and less expensive. The global shipping community is supporting the spread of technology and facilitates cross-border cooperation between different players in the shipping industry and we must exploit this to fight piracy.[77]

Piracy has always been considered a *iuris gentium*, carried in high seas. However, it should be remembered that the high seas are the geographic area where piracy happens now but not in the future and is thus not the only place where should be fought. The issue is that technology improves faster than the human capacity to adapt to it. This is also true with law, often too slow to adapt to current times, especially if related to international conventions. For this research, it is agreed that academics of different sciences should fuel debate over this topic linking technology research with legal and socio-economic research as in the case of piracy. We should remind ourselves that the core function of science (including technology) should always be to improve human condition (including security).[78]

non-state actors, shipping registries and flag entities should evaluate cyber risks in relation to maritime piracy and how these can be fought[79] in existing management systems. In fact, the digitalization of shipping and increased automation systems exposes ships to both cyber[80] and physical attacks. Cyber-attacks and piracy attacks are perceived to be different issues but in reality, they will become two sides of the same coin.[81] Consequently, the three illegal acts of violence, detention, and

---

[72] J.M. White, *Chapter One. Ottoman Pirates, Ottoman Victim*, *Piracy and Law in the Ottoman Mediterranean*, Stanford University Press, California, 2020, pp. 23-59. P. T. Leeson, "Pirational choice: The Economics of Infamous Pirate Practices", *Journal of Economic Behavior & Organization*, 2010, pp. 497-510.

[73] *BBC,* https://www.bbc.com/news/business-37257236 (03/21).

[74] S. Percy & A. Shortland cit. *supra* note 64.

[75] There are already for instance insurances such as CyNav that are covering broader aspect of shipping and cyber matters. Clarke cit. *supra* note 31. Regarding insurance, P&I clubs cover third-party liabilities arising out of piracy yet are not equipped to offer cyber risk analysis related to piracy and it does not cover technology risks.

[76] Clarke cit. *supra* note 31.

[77] Ibid.

[78] R. Christie and A. Acharya, report of following conference "Human Security Research: Progress, Limitations and New Directions", Bristol, 2008.

[79] IMO's Maritime Safety Committee adopted Resolution MSC.428 (98) on Maritime Cyber Risk Management in Safety Management Systems.

[80] K Tam, "Cyber-Risk Assessment for Autonomous Ships", (2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security, Plymouth, 2018).

[81] Ibid.

depredation, and the term ship (considering autonomous ship) should be revised when dealing with piracy.

In conclusion, it is agreed with the late Professor[82] Roebuck that definitions are essential for any study because they draw delimitations. This paper brings this concept forward saying that if we want to keep fighting piracy, we need to define it according to the new scenario embracing new technology.

Piracy has been written about extensively in the context of international law, security and defence measures but there is scant research on new technology impacting on piracy and especially on the impact that these new technologies will have on piracy business models and as such on the definition of piracy itself.

This paper aimed to highlight that gap and encourage future research to be undertaken in order to propose new definitions. This paper urges proposals for a shift in the legal definition of piracy as both piracy and new technology are rapidly changing. The lack of current uniformity of definitions does not help and ensues confusion; thus, a definition based on the new concept of piracy is imperative.

[82] D. Roebuck, "Cleopatra Compromised: Arbitration in Egypt in the First Century BC 74", *The International Journal of Arbitration, Mediation*, Volume 73, Issue 3, 2008, pp263-268. Indeed, "Definitio" in latin means to limit something, to create a boundary. L. Castiglioni, S. Mariotti, *Il Vocabolario della Lingua Latina*, Loescher editore, Bologna, 2019.

SEZIONE II / SECTION II
SICUREZZA UMANA NEL CYBERSPAZIO / HUMAN SECURITY IN CYBERSPACE

HUMAN SECURITY OF MIGRANTS IN THE ONLINE WORLD

Olga Koshevaliska

"Human security is like 'sustainable development' – everyone is for it, but few people have a clear idea of what it means"[1]

1. Introduction

From a time-perspective we can say that the year 2020 will be remembered after the Covid – 19 virus. Other important events and happenings did take please, but nothing was that dramatical and looking back in the near past, nothing was so disturbing in the last decades. Covid-19 did not only impact on our social life, but it also spread just like a virus on every cell in the human security as well. It stopped the physical interaction, or more – it made it a "medical crime" to be near to someone, to have normal contact, to travel, to shop, to show up at court hearings, to learn while being inside of the classroom etc. While on the one hand Covid -19 completely lock down us inside of our homes, on the other hand it fully exposed us in the online world. Eager to know more, to find out more, to be in step with everyday news, we overexposed ourselves in the digital world. Everything that we usually did in the real world was transferred online. This pandemic brings out the best but unfortunately also the worst in humanity. This raised new questions, new dilemmas, new problems for the human security in cyberspace. Transferring our social life in the online world has serious effect on us but we can all agree that it have had a severe impact on the vulnerable groups such as migrants.

With a huge number of people working online from home, often with outdated security systems, cybercriminals use the opportunity to take advantage of this specific situation, and find more ways for and focus even more on new cybercriminal activities.[2] In EUROPOL's special report it is emphasized that "with a record number of potential victims staying at home and using online services across the European Union (EU) during the pandemic, the ways for cybercriminals seeking to exploit emerging opportunities and vulnerabilities have multiplied."[3] This goes specially for migrants.

---

[1] R. Paris, "Human Security: Paradigm Shift or Hot Air?", *International Security*, 2001, pp. 87-102.

[2] EUROPOL Report, "Catching the virus – cybercrime, disinformation and the COVID-19 pandem"->file:///C:/Users/PC/AppData/Local/Temp/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0%20(2).pdf> (04/21)

[3] EUROPOL Report, "Catching the virus - cybercrime, disinformation and the COVID-19 pandemic", <https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic>, (04/21).

In the context of migration, the online world was field with xenophobia, hate speech, discrimination and show how some people really think and feel for these vulnerable groups. Migrants and refugees are overexposed in the online world for longer period that we know. They cannot pack their whole life and all their belongings in a backpack, so it is convenient for them to transfer important, private things into a digital form. Family photos, birth certificates, social security number, important documents, diplomas, everything is stored in the online world so they can have access to it when they find their new home. This facilitated the access to their personal data and privacy not only for their personal use or for the ones that have migrant's best interest at heart, but also for the ones that want to use their disadvantage position and manipulate with their lives. Easy access to everything abovementioned makes them an easy target for malware attacks, phishing, ransomware, identity thefts, spam, hate speech and hate crimes, data breach, unlawful use of personal data etc. In a best way scenario, if all these aforementioned data get compromised – there is a slight possibility to be restored and the damage to be "undone". In this context we have to emphasize that there is a new trend of "digitalizing" the refugees' lives – by using their biometrics, and this new trend of using biometrics from refugees can have even more severe impact of their lives, and in case their biometrics to be compromised – the damage could not be "undone".

2. Migration and IT technology

Almost the whole 2020, migrants in order to get free legal aid, to get directions, finally to get any kind of necessary information had to share their personal data, their plans, route, agenda or almost everything that can be a treat to their privacy and human security. This is due to the fact that refugees and migrants depend on technology along their journey but also in their efforts to integrate into their new societies and reestablish their lives. "Social media, mobile apps, online maps, instant messaging, translation websites, wire money transfers, cell phone charging stations, and WiFi hotspots have created a new infrastructure for movement as critical as roads or railways."[4] As cyberthreats are becoming more advanced and prevalent, and data privacy and protection is vital for the refugee population, the importance of building cybersecurity protections into the network architecture cannot be understated. The refugee crisis in Europe has repeatedly highlighted the urgent need for communication technology for people on the move, from mapping their journeys to accessing services at their destinations. How important is IT for migrants we see from the first question that they ask when arriving in a new shelter camp. "Is there a Wi-FI?"[5]

[4] M. Latonero, "For refugees, a digital passage to Europe", Thomas Reuters News, <http://news.trust.org/item/20151227124555-blem7/> (04/21).

[5] See L. Ramrayka: "Company Focus: Delivering Critical Cybersecurity for Refugees", <https://deeply.thenewhumanitarian.org/refugees/articles/2017/03/02/company-focus-delivering-critical-cybersecurity-for-refugees> (04/21). According to this interview from Refugees Deeply they

Also, migrants before the start of their life journey, in order to make sure that they have all necessary documents, such as passports, birth certificates, diplomas, personal IDs etc., they photo or scan them and keep them online, so they have a copy of them if they lost the original on their way.[6] Migrants are very depended on social media and IT tools before, during and after their life journey.[7] Smartphone access to social media is a crucial source of information in migration decision-making because in this way migrants improvise and modify routes to Europe based on the latest and most relevant information.[8] But smartphones that ease migrants to "keep moving on" and communicate with families and friends, that provide orientation and navigation and survival tools, also involve geo-locatable data that enable state and non-state actors in monitoring and excluding, capturing, and detaining migrants and they are also used by hostile regimes, intelligence services etc. to trace and target activists and political opponents.[9]

This online vulnerability of migrants, caught the eye of many academic research works that ultimately show the impact of the IT technologies on migrants lives, researching which technologies do refugees depend of, and how could they be harmed; what online security and privacy practices do refugees have; and what barriers do they face that prevent them from implementing stronger security and privacy practices; what could be done to empower refugees with greater capabilities to protect their online security and privacy and etc.?[10] All of these research works, showed without no doubt, that there is a strong vulnerability of migrants rights because of their overexposed in the online world.[11] There is no fine line between IT as resource and as a threat, as well as using it for invisibility or for exposure, for mo-

---

have published data that Cisco's successfully blocks an average of 2,000 cyberthreats per day by using their cloud security software.

[6] See D. Nikolovska "Using Social Media in Migration", <https://refugeelaw.mk/mk/2020/08/13/%d0%ba%d0%be%d1%80%d0%b8%d1%81%d1%82%d0%b5%d1%9a%d0%b5-%d0%bd%d0%b0-%d1%81%d0%be%d1%86%d0%b8%d1%98%d0%b0%d0%bb%d0%bd%d0%b8%d1%82%d0%b5-%d0%bc%d1%80%d0%b5%d0%b6%d0%b8-%d0%b2%d0%be-%d1%86%d0%b8%d0%ba/> (03/21).

[7] M. Gillespie, L. Ampofo, M. Cheesman, B. Faith, E. Iliadou, A. Issa, S. Osseiran, and D. Skleparis, "Mapping refugee media journeys: Smartphones and social media networks," 2016.

[8] See R. Dekker, G. Engbersen, J. Klaver, & H. Vonk, "Smart refugees: How Syrian asylum migrants use social media information in migration decision-making", *Social Media+Society*, Sage Publishing, 2018, <https://journals.sagepub.com/doi/full/10.1177/2056305118764439>; R. Dekker, G. Engbersen, M. Faber, "The use of online media in migration networks", *Population, Space and Place*, 2016, pp. 539–551. M. Gillespie, S. Osseiran, M. Cheesman, "Syrian Refugees and the Digital Passage to Europe: Smartphone Infrastructures and Affordances", *Social Media + Society,* Sage Publishing, 2018, <https://journals.sagepub.com/doi/10.1177/2056305118764440?icid=int.sj-full-text.similar-articles.1 > (03/21).

[9] Ibid.

[10] L. Simko, A. Lerney, S. Ibtasam, F. Roesner, and T. Kohno, "Computer Security and Privacy for Refugees in the United States" *Paul G. Allen School of Computer Science & Engineering, University of Washington,* Seattle, 2018.

[11] See A. R. Schrock, "Communicative affordances of mobile media: Portability, availability, locatability, and multimediality" *International Journal of Communication,*

2015, pp. 1229–1246.

bility and immobility. For instance, a smartphone makes migrants visible, connected, and networked, but this may also expose them to risks. Spaces of control can be invisible and difficult to research.[12] Refugees migrating to Europe walk a fine line between taking precautions to remain invisible to surveillant actors and organizations, and depending on smartphones for support, care, protection, and information.[13]

Also, these research works show that refugees as a vulnerable population,

> may be different from other user populations in terms of their interactions with technology and their computer security needs and practices. Refugees, by definition, are fleeing from real threats, and hence might have unique perspectives on threats and adversaries. Further, there might be a range of cultural, linguistic, and technological challenges that refugees must overcome to sufficiently protect their computer security and privacy.[14]

A side from the coronavirus, migrants, in the past few mounts have been overexposed on discrimination and xenophobia as well, especially on the social media. In fact, the social media became the main facilitator of xenophobia in the past few mounts.[15]

2.1. Migrants and Biometric Data

Another concept on human security in cyberspace is the use of biometric identification of migrants. Biometric data are "any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual."[16] Biometrics can be used to digitally identify a person to grant access to systems, devices, or data or for authentication or identification of an individual. Examples of these biometric identifiers are fingerprints, facial patterns, voice or typing cadence.[17] Each of these identifiers is considered unique to the individual, and they may be used in combination to ensure greater accuracy of identification. When it comes to security measures, bio-

---

[12] B. Latour, *Reassembling the social: An introduction to actor-network-theory*,Oxford University Press, Oxford, 2005.

[13] M. Gillespie, S. Osseiran, M. Cheesman, "Syrian Refugees and the Digital Passage to Europe: Smartphone Infrastructures and Affordances", *Social Media + Society*, Sage Publishing, 2018, https://journals.sagepub.com/doi/10.1177/2056305118764440?icid=int.sj-full-text.similar-articles.1> (03/21)

[14] L. Simko et al, cit. *supra* note 10.

[15] J. Nikolic "The impact of the coronavirus covid-19 on migration movements – fight of migrants and refugees against the virus and xenophobia" in: *Human Security in the 21st Century: Challenges to Health Security,* OSCE Mission to Serbia, 2020, p.46.

[16] J. D. Woodward, N. M. Orlans, & P. T. Higgins, "Biometrics: Identity Assurance in the Information Age" *McGraw-Hill Osborne Media,* 2003.

[17] See M. Korolov*, "*What is biometrics? 10 physical and behavioral identifiers that can be used for authentication*",* <https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html> (04/21).

metrics like fingerprints or iris recognition are more heavily used because of their uniqueness.[18] It's easier to distinguish someone by an iris scan rather than, passport that can be forged.

What makes biometrics so compelling for use in refugee crises is its ability to give individuals who have nothing something powerful — a proof of identity even without a government-issued credential like an identification card or passport.[19]

Even though biometric identification seems like it would have undisputable protection it is far from perfect. There are also concerns that biometrics systems, once in place, could be expanded to contain more data, lets say to start off with an iris scan, than proceed with fingerprints, than expand to include DNA analysis, for example.

Iris scans, as a biometric technology has been used from UNCHR from 2002.[20] Firstly it was used for managing the repatriation of Afghan refugees and to provide them with assistance packages and in current days it is used to facilitate the use of biometric wallets and a digital currency called Ethereum.[21]

The use of Ethereum is a relatively novel idea that was tested by the United Nations on Syrian refugee camps in Jordan.[22] In Jordanian refugee camps, Syrian refu-

---

[18] See S. Soliman "Tracking refugees with biometrics: More Questions than answers", <https://warontherocks.com/2016/03/tracking-refugees-with-biometrics-more-questions-than-answers/> (04/21).

[19] According to Sarah Soliman "biometrics can dramatically decrease the amount of fraud in the distribution of aid, save refugees from long waiting to receive benefits etc." But Soliman, as a biometrics engineer, has three main questions regarding governance of the United Nations' use of biometrics with refugees that we find crucial in this research: Who deserves a peek at the United Nations biometrics database; Who owns the data; What is the future of the U.N. biometrics database? Questions that deserve a straight answer.

[20] In 2002, the United Nations High Commissioner for Refugees (UNHCR) first used biometric technology to manage the repatriation of Afghan refugees to Afghanistan. UNHCR provided assistance packages to refugees who wanted to return home. Iris scanning was used to make sure that each refugee received a package only once, and to prevent 'false refugees' from trying to claim a package. UNHCR claims that using this biometric measurement system for refugee management in Afghanistan has been a success because it achieves the goal of confirming the legitimacy of claimants. Since then, UNHCR has been expanding the use of iris scan to gather personal data from refugees. For more see K. Lindskov Jacobsen article regarding the benefits of using iris scans to gather data about refugees. The author argues that UNHCR fails to recognize some significant possible risks associated with the use of iris scans for refugee management.

[21] Ethereum is a decentralized blockchain based technology that supports a cryptocurrency (digital currency) called Ether. A blockchain works as a decentralized online database that permanently records digital transactions. While digital money is usually employed using smartphones, tablets or personal computers, the UN has chosen to utilize biometric technology to funnel aid to refugees. This choice ties the refugees' biometric data with Ethereum so that there is no need for refugees to own sophisticated digital devices to engage in financial transactions. Their eyes instead become their "wallet" — capable of being utilized in shops within the refugee camp and withdrawn as cash at banks and ATMs in Jordan. See N. Menezes, "The UN Uses Ethereums Blockchain to Distribute Funds to Jordanian Refugee Camps", *BTCMANAGER*, <https://btcmanager.com/un-uses-ethereum-to-distribute-funds-to-jordanians/>; and E. Hinchliffe "Ethereum: The not-Bitcoin crytptocurrency that could help replace Uber", *Mashable*, <https://mashable.com/article/ethereum-bitcoin-explainer>.

[22] See N. Menezes, cit. *supra* note 21.

gees receive Ether (Ethereum's digital currency, similar to Bitcoin) in the form of Jordanian dinars through biometric technology.

> Essentially, they receive mobile money directly from the UN using iris scans that act both as a proof of identification as well as an electronic wallet. The use of biometric wallets promises to be empowering for the financial inclusion of refugees but the pairing of biometric data with Ethereum in the provision of aid also has the potential to pose as a cybersecurity risk.[23]

Sneha Indrajit emphasizes that a potential leak of biometric data could be highly threatening to the lives of Syrian refugees as it could prevent them from receiving aid and would effectively render an already vulnerable population even more vulnerable. The degree of consent given by Syrian refugees in the collection of their biometric data is also questionable given their vulnerable status as refugees. Giving up their biometric information is their ticket to receiving aid and their only option of survival. Given the risks associated with the collection of biometric identifiers, the need to give up biometric information in exchange for aid could be seen as coercive and unethical.

The problem would become even more serious if the Syrian government gains access to their biometric data. This will represent a clear risk for human security. Also, "the biometric technology used for the identification of Syrian refugees, have an expected error rate of three percent that means in a refugee population of two million, translates to 60, 000 false matches."[24]

Furthermore, biometric data is just as vulnerable to being stolen as is personal data to be compromised, due to its sensitivity, the result of theft can be severer. "You may be able to get a new credit card in two weeks, but who will issue you a new set of fingerprints to replace the stolen ones?"[25]

The security of biometric technology is in direct correlation of how well this data is stored and who has access to this data. "The current policy implemented to mitigate the risk of privacy and security breaches in the UNHCR's biometric database for refugees is the use of a centralized database, the so-called Biometric Identity Management System (BIMS) that manages the biometric identities of refugees."[26]

The delicate part of all of this is that governments of host countries as well as countries of origin could obtain access to the biometric databases of humanitarian

---

[23] See S. Indrajit*: The Cybersecurity Risks of Using Biometric Data to Issue Refugee Aid*, <https://jsis.washington.edu/news/cybersecurity-risks-using-biometric-data-issue-refugee-aid/#_ftn12> (04/21).

[24] See K. L. Jacobsen "Experimentation in Humanitarian Locations: UNHCR and Biometric Registration of Afghan Refugees." *Security Dialogue,* 2015; and also S. Nillasithanukroh, "Rethinking the Use of Biometric Systems for Refugee Management." *Chicago Policy Review*, 24 February 2016.

[25] *Biometric Identification and Identity Theft*, <https://www.thebalance.com/biometric-identification-and-identity-theft-1947595> (04/21).

[26] P. Currion, "Eyes Wide Shut: The Challenge of Humanitarian Biometrics," *Irin News*, <http://www.irinnews.org/opinion/2015/08/26/eyes-wide-shut-challenge-humanitarian-biometrics> (04/21).

actors, such as the UNCHR, either by request or by demand, and use it for a different purpose to the one for which it was originally intended, such as for example - law enforcement or national security screening. Further, data could also be sold for profit, used by foreign countries for intelligence, or used to publicly humiliate, dishonor, undermine, weaken the humanitarian organizations.[27] In addition to this, past practices have shown that databases initially established for one purpose often become opted for law enforcement or intelligence ends. For example, the European Commission promised that its EURODAC database of asylum applications would be protected from other uses, until 2012 when it agreed to allow Europol and other law enforcement agencies access to it.[28]

In the end, biometric data can pose a threat to human security of refugees in case of loss, theft or misuse of biometric data that could lead to jeopardizing the refugee's legal identity in circumstances in which they don't have other way to prove their identity. Beneficiaries in humanitarian crises are fleeing persecution and have good reason to want to protect their identity, location, and movements. By collecting biometric data and storing it in centralized databases, humanitarian or aid organizations could place beneficiaries at serious risk, something that we have already seen before.[29] At the end of the day, the lost of personal data or biometrics maybe due to humanitarian workers losing laptops, USB keys and other digital files containing beneficiary data.

But what is concerning is that UNCHR adopted a document so called Data Protection Policy in 2015, in which is provided that UNHCR "may transfer personal data [of refugees] to third parties, on condition that the third party affords a level of data protection the same or comparable to this Policy."[30] This policy has safeguards built in but justifying the transfer of personal data so broadly is a risk by itself and poses vulnerability to human security. According to UNHCR, "confidentiality of data is particularly important for refugees and other people in need of international protection, as there is a danger that agents of persecution or rights violations may ultimately gain access to such information, potentially exposing a refugee to danger even in his/her asylum country."[31]

---

[27] Data which have been stolen or leaked from insufficiently secure medical databases have been repurposed in a similar way: G. Hosein, A. Martin, "Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations", report prepared by the Policy Engagement Network for the International Development Research Centre, *London School of Economics and Political Sciences*, December 2010.

[28] See P. Currion, cit. *supra* note 26.

[29] These concerns are not just theoretical. "Documents published by National Security Agency whistleblower Edward Snowden showed that US and British intelligence agencies targeted humanitarian organizations like UNICEF, UNDP and Medecins du Monde for surveillance" See J. Ball, N. Hopkins, "GCHQ and NSA targeted charities, Germans, Israeli PM and EU Chief," *The Guardian*, <http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner> (04/21)

[30] See *Policy on the Protection of Personal data of persons of concern to the UNHCR*, UNHCR, May 2015.

[31] A. Farraj, "Refugees and the Biometric Future: The impact of Biometrics on refugees and asy-

Given all the risks that we aforementioned for biometric technology that tackle human security, it is worth asking why it is being applied, or better said live tested, on a population as vulnerable as refugees. According to some authors:

> iris recognition is far from an inexpensive option and the potential risks of biometric identity fraud could compromise the legitimacy of biometric identification as well as threaten the livelihoods of Syrian refugees. The appeal of biometric identification, however, lies in its potential uses for border control and law enforcement. This is especially since biometric technology is key in enforcing immigration law and the technology could potentially be used to control refugee populations. Thus, the use of biometric technology on such a large scale treads a fine line between identification and surveillance.[32]

Therefore, we can conclude that the application of biometrics to refugees and asylum seekers raises several concerns, including violation of privacy, misidentification, stigmatization, potential to block asylum applications and surveillance. These concerns demand that policymakers take into account the unique circumstances of refugees and asylum seekers and take steps to ensure that their well-being is in fact furthered by the collection, storage, and utilization of their biometric information. At the end, we must be sincere to the current situation that despite the risks, the "pairing of Ethereum with biometrics in the provision of aid to refugees can be more beneficial than harmful if implemented with the proper protections in place. These protections should include greater regulations on how the biometric data of refugees is collected and shared so that it favors the safety and privacy of refugees."[33] Although biometric technology is not bulletproof from misuse, there exist safeguards that are to some extent responsive to unique concerns of refugees and asylum seekers.[34] To the extent that these safeguards can be improved and expanded upon, biometrics will continue to be an important tool in protecting refugees and asylum seekers.

3. Conclusion

From the questionaries that Humarcyspace[35] research unit disseminated to researchers, company, and a digital rights association we have a clear picture on

---

lum seekers", *Columbia Human Rights Law Review*, 2011, pp. 891-941.

[32] Ibid.

[33] S. Indrajit, *The Cybersecurity Risks of Using Biometric Data to Issue Refugee Aid*, <https://jsis.washington.edu/news/cybersecurity-risks-using-biometric-data-issue-refugee-aid/#_ftn12>, (04.2021).

[34] A. Farraj, cit. *supra* note 31.

[35] HUMARCYSPASE (Protecting HUman SEcurity with non-state-actors in the MARitime and CYber SPAce) is a project from the field of International law conducted by the Law Department at the Univeristy of Campania 'Luigi Vanvitelli' in Caserta, Italy, with prof. Giorgia Bevilacqua as the Principal Investigator (https://www.unicampania.it/index.php/ricerca). The project is conducted in partnership with the University of Goce Delcev, Stip, North Macedonia (http://eprints.ugd.edu.mk/24422/), (04/21).

greatest threat to human security in cyberspace listed as surveillance of users as well as real threat to privacy and personal data. As for the most recurrent threats that can be experienced for cybercriminal activities are malware attacks, phishing, ransomware, identity thefts, spam, hate speech and hate crimes, data breach, unlawful use of personal data etc. Migrants, refugees, and asylum seekers are even more exposed to these treats. Refugees are among the world's most vulnerable people. Studies have shown that undue surveillance towards marginalized populations can drive them off the grid.[36] Real fears around data collection may result in refugees seeking unauthorized routes to European destinations. This can make them invisible to officials and more susceptible to criminal enterprises. Data collection on refugees should balance national security and public safety with the need to preserve human dignity, human rights, and human security.[37] Humanitarian organizations, enforce agencies, governments and refugee agencies need to establish trust when collecting data from refugees. As governments and leaders coordinate a response to the crisis, appropriate safeguards around data and technology need to be put in place to ensure the digital passage is safe and secure.[38] Regardless if a person is a migrant, refugee or an asylum seeker, when individuals reveal their personal data for a particular purpose, it should be handled with due care to protect their best interests and to ensure that they are fully aware of any implication on their human rights and human security. The international standards for collecting and processing personal data are acknowledged worldwide. However, the lack of a binding international instrument has been the subject of much debate.[39] To truly protect the rights of refugees however, it is crucial that there is increased regulations and transparency in the way in which the personal data and biometric data of refugees is shared.

There must be more advanced law solutions to the cybercrime, the legal framework is insufficient to serve its purpose of real, actual and adequate answer to cybercrimes. Although international human rights law does not focus specifically on biometric technology, it does outline basic rights and entitlements that may inform these discussions and help formulate plans for mitigating risks.[40] In the end, it is necessary to strengthen the international legal framework to respond effectively to these challenges and risks on human security. In addition, stronger capacity to deal with all of these challenges and better cooperation will be of benefit of all, as cyberspace knows no borders.

---

[36] S. Brayne, "Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment" *American Sociological Review*, 2014, pp. 367–391.

[37] O. Koshevaliska, "Privacy versus security when exchanging personal data in criminal matters in EU", PhD Thesis, UKIM, Skopje, 2012. Also, J. Ananiev, O. Kosevaliska, "*National security versus protection of personal data in the EU"*, *Iustinianus Primus Law Review*, 2012, pp. 1-13; L. Nanev, O. Kosevaliska, "*Protection of personal data in the criminal legislation in Macedonia*", *Balkan Social Science Review (BSSR)*, 2013, pp. 69-84; O. Kosevaliska, G. Buzarovska - Lazetik, L. Nanev, "Personal Data Protection in Macedonian Criminal Legislation vs. Its Protection in UE", *Annals of the Bucharest University – The Law Series (Aub - Drept)*, 2013, pp. 135-149.

[38] M. Latonero, cit. *supra* note 4.

[39] *IOM: Data protection Manual*, International Organization for Migration, Geneva, 2010.

[40] A. Farraj, cit. *supra* note 31.

HUMAN TRAFFICKING: ONLINE RECRUITMENT - A SERIOUS RISK TO MIGRANTS' CYBER SECURITY IN REPUBLIC NORTH MACEDONIA

Elena Maksimova

1. Introduction

Electronic and fast communication have significantly facilitated life in recent years, but also left a strong mark on the way of coexistence with others. Today, when human contact is reduced and minimized, when communication with others and the maintenance of social life is done through phones, tablets and computers, when we work, educate and live with the help of the Internet and electronic devices, is inevitable for crime to change its direction too. To direct its manifestation in the same place where people of today live - in cyberspace. Wide application are the most essential need of information and communication technology and use of social networks exists in a special way among people affected by natural disasters or armed conflicts. Crisis situations in which social networks would have a huge impact are increasing. In 2015, we witnessed a state of emergency caused by the large influx and transit of about 1 million refugees and migrants in our country.[1]

Trafficking in human beings and smuggling of migrants have emerged as one of the most serious crimes committed against migrants using Balkan route and transiting through the Republic of North Macedonia. The fluidity of the borders of these two types of crimes, imposed the need for their detailed criminological analysis.[2] So, this constant monitoring of these criminalities and their study, gave us the knowledge of "modern" way of getting that first, initial touch with possible/potential victims of these acts – online / cyber recruitment. Online interactions and encounters appear to facilitate several aspects of human trafficking such as - targeting of potential victims, access to personal data, arrangement of logistics and transportation, recruitment through social media, chat forums and other websites, advertisement of victims, their exploitation and

[1] D. Nikolovska, *The use of social network in the migration cycle*, University "St. Cyril and Methodius",
Faculty of Law "Iustinianus Primus" – Skopje Refugee Law Clinic, <https://refugeelaw.mk/mk/2020/08/13/%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B5%D1%9A%D0%B5-%D0%BD%D0%B0-%D1%81%D0%BE%D1%86%D0%B8%D1%98%D0%B0%D0%BB%D0%BD%D0%B8%D1%82%D0%B5-%D0%BC%D1%80%D0%B5%D0%B6%D0%B8-%D0%B2%D0%BE-%D1%86%D0%B8%D0%BA/ >

[2] See: P. Campana & F. Varese, "Exploitation in Human Trafficking and Smuggling", *European Journal on Criminal Policy and Research*, 2016, pp. 89-105.

surveillance.[3] Therefore, two main methods are used by traffickers to recruit victims via the Internet - spurious advertisements for employment, marriage, dating agencies, etc. or chatrooms.[4]

Each of the three cumulative elements of the trafficking definition can be committed in a 'cyber' way: the recruitment, the transportation, and the offering of the victims and even the actual exploitation.[5] In trafficking, but also in smuggling migrants, perpetrators use all kind of means to recruit victims from traditional to more modern ones. When trafficking is committed with the use of Internet it is called "cyber trafficking". Cybercrime is easily committed, it is cheaper, it is anonymous, it is fast and leaves only digital traces, the criminal does not have to leave their home place, and it can be hard to locate.[6] The perpetrators aggressively adopt the new ways of communication, and take advantage of each new technology and application to trace victims, transmit illegal materials, and avoid detection by law enforcement.[7] More and more forms of trafficking appear every day and more of them are using cyberspace as means of recruitment or for the advertisement of trafficking "services and products".[8]

Looking at the migrant crisis, and the closure of the Balkan route and the recent pandemic, cyber recruitment has become a particularly widely used way of contacting migrants. International Organization for Migration (IOM) alarmed about the treat that human trafficking would adapt to the COVID – 19 pandemics, and that the usage of internet tools for recruitment will increase.[9] United Nation Office on drug and crime (UNODC) also reacted in this way,[10] and so does the Europol and its European Migrant Smuggling Center.[11] The use of Internet-based applications has eased the process of identifying and contacting victims, the logistics of transferring money, and the coordination between dif-

---

[3] *Migrant smuggling networks*. *Joint Europol-INITERPOL report*, May 2016, <https://www.europol.europa.eu/publications-documents/europol-interpol-report-migrant-smuggling-networks>.

[4] *Trafficking in human beings: Internet recruitment, Misuse of the Internet for the recruitment of victims of trafficking in human beings*, Directorate General of Human Rights and Legal Affairs, Council of Europe, 2007.

[5] *Völkerrechtsblog*, *International Law & International Legal Though,* < https://voelkerrechtsblog.org/de/on-cyber-trafficking-and-the-protection-of-its-victims/> (03/21)

[6] *Trafficking in human beings*, cit. *supra* note 4.

[7] S. Sarkar, *How traffickers exploit the COVID – 19 pandemic*, research proposal, 2020, <https://www.researchgate.net/publication/340428231_How_traffickers_exploit_the_COVID-19_pandemic>

[8] A. P. Sykiotou, *Cyber trafficking: recruiting victims of human trafficking through the net*, in C.D. Spinellis, Nikolaos Theodorakis, Emmanouil Billis and George Papadimitrakopoulos (eds.), *Europe in Crisis: Crime, Criminal Justice and the Way Forward. Essays in Honour of Nestor Kourakis*, Ant. N. Sakkoulas Publishers L.P., Athens, 2017, p. 1547-1587.

[9] *International Organization for Migration* <https://rosanjose.iom.int/SITE/en/blog/when-human-trafficking-adapts-pandemic> (04/21).

[10] UNDOC warned that "traffickers innovate and take advantage of new technologies to work in flexible ways, including extending their operations across borders".

[11] They aware that "this crisis will have a lasting impact on our societies and economies".

ferent groups. Moreover, the anonymity and use of many online services simplifies a transnational crime such as trafficking in persons.[12] The perpetrators use various means of communication, various applications and are generally anonymous, which makes it difficult to detect the crime, but on the other hand crossing the border from smuggling into human trafficking is particularly easy. And if the bait set by the perpetrators in normal conditions by luring people is usually the promises for better work, better life, easy earnings, socializing, etc., it is set here long before the perpetrator reaches for the victims, and that is - transit across borders and reaching the final destination.

2. Victimization of Irregular Migration in the Republic of North Macedonia - An Opportunity for Human Traffickers

Migrants and refugees traveling or being smuggled through North Macedonia are vulnerable to trafficking, particularly women and unaccompanied minors.[13] The UNODC Global Report on Trafficking in Persons for 2016, notes that many trafficking cases "start with people eager to migrate but with no other option than to rely on someone who they believe will facilitate their irregular migration into a better life". In particular, the Global Report notes that the lack of regular migration and family reunification channels leaves no other option for people fleeing conflict and persecution but to make "dangerous migration decisions", often exposing them to the risk of being trafficked and exploited on route or in destination countries. In practice the boundaries between smuggling and trafficking are often blurred, mostly because they are influenced by the same political and socioeconomic factors. This conflation is described as problematic and is said that can jeopardize the proper identification and assistance of victims of trafficking, as government authorities may focus on the identification of smuggling offences at the expense of the identification and protection of victims of trafficking.[14] Traffickers also frequently bribe police officers and labor inspectors, and police have been investigated and convicted for complicity in human trafficking,[15] and in smuggling of migrants too. Because of the lack of collaboration of migrants, many of cases that are probably cases of trafficking in person, go under of the indictment smuggling of migrants. There is no incrimination in the Criminal

---

[12] UNODC – United Nations Office on Drugs and Crime, *Global report on trafficking in persons*, 2018.

[13] *2020 Trafficking in Persons Report - Macedonia*, United States Department of State, 2020, <https://www.state.gov/reports/2020-trafficking-in-persons-report/north-macedonia/> (02/21)

[14] *Trafficking along migration routes to Europe, bringing the gap between migration, asylum and anti-trafficking*, International Centre for Migration Policy Development, EU, 2018, p. 20.

[15] *2019 Trafficking in Persons Report - Macedonia*, United States Department of State, 2019, <https://www.state.gov/reports/2019-trafficking-in-persons-report-2/north-macedonia/> (02/21)

Code trafficking victims for unlawful acts committed as a direct result of being subjected to trafficking; however, the government may have deported, detained, or restricted freedom of movement of some trafficking victims due to inadequate identification efforts[16], which has a push effect for the migrants who urge to reach their destination country. So, the lack of statistic does not necessarily mean the lack of cases.

2.1. Risky time periods in Republic of North Macedonia for migrants' victimization

From the beginning of the migrant crisis until today, significant time periods that were particularly conducive to further victimization of migrants are:

1. Selective policy in the admission of migrants originating from a particular country[17]
2. Further restriction of the mentioned selective policy[18]
3. The closure of the Balkan route[19]
4. Closing borders as part of measures to prevent the spread of the COVID 19 pandemic.[20]

Although migration is often voluntary, it still increases the vulnerability of individuals and leads to abuse of rights, exploitation, violence etc. Increased migration flows also pointed to the lack of protection of migrants in our country, both those who passed and those who found themselves stuck in it. The

[16] *2018 Trafficking in Persons Report - Macedonia*, United States Department of State, 2018, <https://www.refworld.org/docid/5b3e0ae7a.html> (02/21).

[17] During November 2015, Slovenia launched a discriminatory selection for the reception of refugees based on their country of origin. This practice as a chain reaction was reflected at all border crossings on the Balkan route. As a consequence, only refugees from Syria, Afghanistan and Iraq were allowed through the Republic of Macedonia, and refugees with documents from other countries were not allowed

[18] At the beginning of 2016, the border was closed for people coming from Afghanistan.

[19] In early March 2016, a change in EU policies also imposed the closure of borders along the Balkan route. The closure of the border along the Balkan route meant that great outrage number of women with children and unaccompanied children are stuck in states along the route. On the day of closing the borders, on the territory of Macedonia in the reception-transit centers and in their immediate vicinity there were a total of 1,024 refugees. Almost all of them were at high risk of becoming victims of migrant smuggling, and many of them had multiple risk factors to become victims of human trafficking.

[20] In March 2020, the President of the Republic of North Macedonia declared a state of emergency to combat the outbreak of COVID-19. At the same time government tightened measures to combat the coronavirus with a decision to completely close all borders, including the airport in Skopje. A decision of the Government closed all border crossings in the country for foreign nationals, as well as the Skopje airport. Exceptions to the decision were trucks in transit, representatives of the diplomatic corps and other persons for whom the Ministry of Interior will give approval. Airport services were able to be used only for state, military, cargo, humanitarian needs, as well as for empty flights. In this period, from January until September 24.153 persons are prevented from entering in Macedonia illegally, from whom only 6568 until the closer of the borders, and 2700 victims of smuggling were prevented by the police. Most of the refugees/migrants at this point entered the country with the help of smugglers and paid approximately 600 euros to transit through the country.

chances of reaching the desired destination on a regular basis decrease with the course of events, so the only option they inevitably resort to is illegal transit and migration. Those who do not have enough funds to pay for the smugglers' travel are often forced to look for work in the country in which they are stuck (such as in our country – mostly through online adds), which opens the possibility for their labor exploitation by seasonal employers, or they are forced to work for their smugglers - in the country of destination or to guide other migrants or to recruit people for them.[21]

3. Cyberspace and Human Trafficking – From Recruitment to Exploitation

3.1. Initial contact (fishing)

Having in mind what was mentioned before, we arise another question – how can smugglers abuse cyberspace and make online recruitment among migrants to become human trafficking cases?

A UNHCR research done for Afghanistan migrants[22] shows that basic tool for existence in the migration journey are smartphones. In 2015, the International Rescue Committee, because of the regular inspection of the item's migrants carry in their travel bags concluded that the possession and use of mobile phones has been reported in almost all travel bags.[23]

They buy new one before their journey starts so they can contact to the families back home with help of the applications. They also create new Facebook accounts to communicate with Afghans in Europe. But somewhere along this journey this initial will that migrants have can drop out or can be blurred with some acts done towards them[24] or forced to be done by them.[25] So, in this point, smuggling can turn into human trafficking, even if migrants are not fully aware of it.

---

[21] S. Cvejiki and S. Kitanov, *Regional mapping of migrant smuggling on Western Balkan*, IOM International organization for migration, 2017.

[22] *From a refugee perspective. Discourse of Arabic speaking and Afghan refugees and migrants on social media from March to December 2016*, UNHCR – The UN Refugee Agency, 2016, p. 23 <https://www.unhcr.org/publications/brochures/5909af4d4/from-a-refugee-perspective.html.> (03/21)

[23] B. Frouws, M. Phillips, Hassan, A., & M. Twigt, "Getting to Europe the WhatsApp way: The use of ICT in contemporary mixed migration flows to Europe", *Regional Mixed Migration Secretariat Briefing Paper,* 2016.

[24] During dangerous segments of the journey, from origin country to destination country, people would be forced to climb into crammed, suffocating spaces in vehicles, onto overcrowded pick-up trucks driving at neck-breaking speed or be made to walk across dangerous slippery mountain paths in the dark without proper shoes. There are stories of people left behind to die if they are injured or too exhausted to move on. What can be found on social media is evidence that smugglers force their clients on overcrowded boats at gunpoint.

[25] *From a refugee perspective. Discourse of Arabic speaking and Afghan refugees and migrants on social media from March to December 2016*, UNHCR – The UN Refugee Agency, 2016, p.23 <https://www.unhcr.org/publications/brochures/5909af4d4/from-a-refugee-perspective.html.> (03/21)

Journey, in general, starts in the country of the origin of the migrants. Smugglers are highly informed on visa requirements and procedures for asylum requests, and this expertise allows them to exploit weaknesses and gaps in international and national regulations.[26] Abovementioned UNHCR survey from 2016, shows that over a hundred financial agents (sarafs), that keep the deposited smuggling fees as intermediaries between smuggler and client, and manage financial transfers, are present on Facebook. And over 100 "asylum and immigration consultants" offer so-called "advice on asylum claims" and provide fake "proofs" of persecution. Most of these advertisements are on Arabic because "customer's" usual way to travel is to book an all-inclusive trip (from the country of origin to the promised country of destination). There are other offers as well. In their promotion strategy, smuggling networks are not only selling a trip, but the European dream (like the "American Dream"). Stolen documents like passports are also advertised, but when it comes to this document frauds, smugglers are much more cautions on online communication than in communication about providing a trip. Here they do not talk about the transactions on social networks, but rather request to be contacted on private channels. When clients post enquire on Facebook these messages are swiftly removed, presumably to cover the tracks. When Balkans route was closed, and Macedonia barred refugee entries from Greece, local criminals in Turkey offered to move names up on the waiting lists of certain EU embassies, where asylum-seekers were registered for interviews. One smuggler even reassured potential clients on Facebook that they should keep coming, as the former Yugoslav Republic of Macedonia's (name used internationally at the time) border would "reopen soon".[27]

Trust is crucial within illicit markets, especially when smugglers offer different services.[28] As far as the migrants as concerned, choosing a reliable smuggler means a great difference between a safe or risky trip. The use of the Internet and social networks in the recruitment stage does not exclude offline strategy. The use of social networks and mobile applications is crucial not only in recruitment phase but during transportation too. Smugglers can remain in contact with migrants and provide information on possible accommodation and venues to recharge their mobile phones. The payment is usually settled in the destination country, through intermediaries, who are trusted and well-known within local communities.[29]

---

[26] A. Antonopoulos, G. Baratto, A. Di Nicola, P. Diba, E. Martini, G. Papanicolaou, & T., Terenghi., *Technology in Human Smuggling and Trafficking. Case Studies from Italy and the United Kingdom*, Springer, 2020, p.23.

[27] *From a refugee perspective. Discourse of Arabic speaking and Afghan refugees and migrants on social media from March to December 2016*, UNHCR – The UN Refugee Agency, 2016, pp.27 - 28

[28] K, Von Lampe & P. Johansen, *Organized crime and trust: On the conceptualization and empirical relevance of trust in the contexts of criminal networks*, Global Crime, 2004, pp. 159–184.

[29] A. Antonopoulos et al., *Technology in Human Smuggling and Trafficking*, cit. *supra* note 26, p. 27.

Some researchers[30] divide the perpetrators involved in this kind of human trafficking in three main categories:

1. First, they talk about the *solo entrepreneurs*[31]
2. *small-medium / family-based criminal groups*[32] and
3. *large organized and loose criminal networks*.[33]

Because Facebook and Instagram are the most used social networks, traffickers often use personal information of the target group, available on the Internet and social networks, to create online profiles - tailored to the characteristics of potential victims so that victims can be attracted easier.[34]

Risk factors for being trafficked are plenty. There are migration-related policies, that prohibiting migrant workers to change their employers. This can be crucial in creating situations of vulnerability to exploitation, including through human trafficking, forced labor and slavery.[35] Smuggled migrants are vulnerable to violence, abuse, and exploitation. They have unequal power relationship with smugglers, an inability or unwillingness to seek protection from the state and the lack of options about exit strategies.[36] They are at a high risk of victimization through other crimes, including extortion, kidnapping, sexual and gender-based violence, deprivation of food and water, and even homicide.[37] In 2020 and the pandemic, the problem of victimizing migrants into human trafficking schemes has intensified. Countries around the world closed their borders, preventively, and that made perpetrators to find new ways to abuse irregular mi-

---

[30] F. Terenghi, A. Di Nicola et al. (eds.), *Market structure and social organization of trafficking in human beings in the EU. Financing of organized crime. Human trafficking in focus*, Center for the Study of Democracy, Sofia, 2018, pp. 29–53.

[31] With low profile, that manage the trafficking operations from recruitment to exploitation on short distances, for example only between two European countries. This kind of traffickers groom their potential victims by establishing a relationship, or they may be husbands or partners of the victims.

[32] These are organized small/ medium large-scale trafficking operations, mostly among two/three European countries, and are based on ethnic, familial, kinship bonds (e.g., Albanians and Romanians).

[33] These networks control the entire trafficking chain – from the initial contact and active recruitment (also providing documents if needed), as well as transportation and corruptive practices, exploitation (e.g., Chinese, Nigerians). They are structured into flexible, horizontal, and decentralized networks made of a large number of affiliates, divided into sub-units and run trafficking operations on a global scale, members that are not linked by ethnic, familial and kinship ties, and perform specific roles and duties.

[34] D. Boyd, H. Casteel, M. Thakor & R. Johnson, *Human trafficking and technology: A framework for understanding the role of technology in the commercial sexual exploitation of children in the U.S.*, Microsoft Research Connections, Cambridge, 2011.

[35] *Issue Brief #5, Smuggling of migrants, trafficking in persons and contemporary forms of slavery, including appropriate identification, protection and assistance to migrants and trafficking victims,* United Nations, <https://refugeesmigrants.un.org/sites/default/files/ts5_issue_brief.pdf > (03/21)

[36] *OHCHR, Situations of migrants in transit* (A/HRC/31/35), para 55-58. In 2015, reports estimated that for every 1,000 passengers aboard smugglers' boats on the Andaman Sea and the Bay of Bengal, 11 or 12 died from starvation, dehydration, disease and abuse. See: UNHCR Tracks, Abandoned at Sea, Stories of refugees and aid workers, 2015. Also see: IOM, Missing Migrants Project, 2017.

[37] See: *Abandoned at Sea, Stories of refugees and aid workers*, UNHCR Tracks, 2015. Also see: *Missing Migrants Project*, IOM, 2017.

grants that wish to get to some of the EU countries. The ones that financially are struggling are often victimized in labor or further sexual exploitation[38].

3.2. The organized transport

Republic of North Macedonia is mainly transit country for organized chains of human trafficking and for migrants/refugees who want to reach to European Union countries. So, they want to pass the country as fast as possible so they could continue their journey. Before closure of the borders during 2014, until June 2015, Republic of North Macedonia did not allow migrants and refugees to use public transport and forced them to walk throughout the country to reach the Republic of Serbia. During the organized railway transport policy, in the second half of 2015 and the beginning of 2016, public company "Makedonski Zeleznici AD Transport" (Macedonian Railways) in a short period of time made a correction of the ticket price for the refugees who transited through the country twice.[39] And the closure of the Balkan route in 2016 did not stop the trend. Migrants continued to use the route, illegally, and to use organized criminal group's services more often. In 2020 there was increased number of cases of smuggling migrants, a lot of which were involved in serious car accidents while transporting trough Coridor 10,[40] so that tells us that pandemic did not stop the trend on offer and demand of the smuggling migrant services.[41]

Social media is increasingly popular among refugees as a source of information in preparing for where to migrate, contact with smugglers, government information from the state of defense as a destination, and evaluation of shared refugee and migrant experiences of others in a similar situation. Through social networks, refugees have easy access to the facts they need and thus create a plan for which route, ie which route they would choose and the degree of danger on the road. they gather information in advance where they could connect to free Wi-Fi, where they would find shelter, food and where they could receive or exchange money and the like. When it comes to knowing how to organize a trip, the journey of irregular migrants is most often planned and organized, that it involves a network of smugglers and irregular migrants. Organized crime groups in recent years have also recruited

---

[38] *European Migrant Smuggling Centre 4th Annual Report*, Europol, 2020, <https://www.europol.europa.eu/publications-documents/emsc-4th-annual-activity-report-%E2%80%93-2020> (04/21).

[39] The price of each individual ticket for these users was 25 euros, ie 3.5 times higher than the regular ticket price which is around 7 euros. All this events higher the risk for finding alternatives for transiting the country.

[40] *FIELD REPORT 2020, April - May – June,* Macedonian Young Lawyers Association, 2019, p.3 < Field Report Apr-May-June 2020 Daniel (myla.org.mk)> (04/21).

[41] *Nova Makedonija* <https://www.novamakedonija.com.mk/makedonija/hronika/%D0%BF%D1%80%D0%BE%D0%BD%D0%B0%D1%98%D0%B4%D0%B5%D0%BD%D0%B8-44-%D0%BC%D0%B8%D0%B3%D1%80%D0%B0%D0%BD%D1%82%D0%B8-%D1%81%D0%BE%D0%BA%D1%80%D0%B8%D0%B5%D0%BD%D0%B8-%D0%B2%D0%BE-%D0%BA%D1%83%D1%9C%D0%B0/> (02/21).

juveniles to transport migrants - they do not have driver's licenses and can not be convicted.[42] It is cheapest via Macedonia and Bulgaria. Smugglers always give several options to their customers.[43] We must be aware that the organization of the trip is mostly planned, so it is known who provides logistics, who transits, who the whole trip, who accepts migrants in the next country, etc. So, it is logical that this communication must take several days with constant communication between smugglers and migrants. Good part of the communication between them is happening by using the internet cafes in every city,[44] because it does not leave a digital trace, so the user can not be located via GPS. When communicating with migrants, if they use a telephone, that telephone number is no longer available after the call, they use it only once. For Balkans in general, smugglers are not needed for the entire trip. They usually contact migrants in Turkey, trough Facebook. When selecting smugglers, refugees and migrants also trust the judgment of fellow countrymen who have already travelled. They are aware that smugglers are lying about the dangers but have no other choice and try to choose "the least bad ones".[45]

Smuggling offers can also be found on the internet. They are using Facebook to put out legal or illegal offers.[46]

The accent is put on smuggling migrants for one reason only – thin line between the crimes and not proper recognition on human trafficking by authorities in practice. Testimonies of migrants says that it is impossible to find smugglers who are not traffickers.[47] Also, some cases in practice, in Macedonia were not properly resolved mainly because of the ping - pong procedure at the time.[48] Or, very

---

[42] G. Lefkov, *Searching for Illegal Routes: Human trafficking Carries Millions For Smugglers*, Center for Investigative Journalism SCOOP, 2017, <https://scoop.mk/%D0%BF%D0%BE-%D1%82%D1%80%D0%B0%D0%B3%D0%B8%D1%82%D0%B5-%D0%BD%D0%B0-%> (03/21).

[43] Transport by truck from Thessaloniki to Kumanovo Lojane costs around 1,300 euros, but the price can go up and down depending on the intermediaries. It's a little more expensive with a car. The most expensive option for refugees is to procure false documents through smuggling channels, most often Bulgarian, and to leave the airport in Thessaloniki for the requested European destinations. For the two-hour flight from Thessaloniki to Munich, migrants pay up to 7,000 euros, Ibid.

[44] *Migrants in local communities in Serbia*, Athens - Association of Citizens for Combating Trafficking in Human Beings and All Forms of Violence against Women, Belgrade, 2014, <http://www.atina.org.rs/sites/default/files/Migranti%20i%20migrantkinje%20u%20lokalnim%20zajednicama%20u%20Srbiji.finalno.pdf> (02/21).

[45] *From a refugee perspective. Discourse of Arabic speaking and Afghan refugees and migrants on social media from March to December 2016*, UNHCR – The UN Refugee Agency, 2016, p.43

[46] Ibid. p.17.

[47] "All smugglers are also human traffickers. I heard, you pay the smuggler and he later exploit and abuses you." "If someone doesn't have the money, make an agreement with the smuggler, they choose one Somali woman who becomes his property so that the man can continue his journey from Turkey, Greece or Macedonia." *Atina* <http://www.atina.org.rs/sites/default/files/Migranti%20i%20migrantkinje%20u%20lokalnim%20zajednicama%20u%20Srbiji.finalno.pdf> (04/21).

[48] *Republica online* <https://republika.mk/vesti/crna-hronika/nema-ni-krivichna-za-zgrizuvachot-na-81-migranti-vo-vaksince-mvr-i-ojo-si-prefrlaat-odgovornost/> (04/21).

often, the charges ended up with an easier qualification for the perpetrators because of the lack of collaboration by the migrants themselves. Our Criminal Code[49] provides severer punishment for the perpetrators of migrant smuggling, if they were treated in an inhumane way, were tortured, or held in conditions that were endangering their health. So, while the migrants were staying in the country, information that was spread about the same crime for example, was that there is no such treatment,[50] so that later, when migrants arrived in the EU, they admit that they were held hostage, extorted money, and treated inhumanely[51]. But the question that arises is – is there a severe treatment in those cases, combined with torture, forced labor etc., or was that the main intention of the smugglers at the first place, so that trafficking with persons was their initial intention?

4. The Job Offers - A Common Bait and a Path to Further Labor Exploitation

As mentioned above, migrants often start their journey with a pre-arranged plan for future employment and accommodation. Most often, they trust some kind of "agencies" that offer the whole packages. However, refugees often do not have the desired time to plan their journey in advance. Nor do all migrants have it. Therefore, every place through which they transit in order to reach their desired destination is an opportunity to get in touch with potential "intermediaries" who can provide them with documents, work and accommodation in the country of destination. As labor exploitation is the second most common form of human trafficking exploitation (immediately after sexual exploitation)[52] and having in mind that human trafficking works on the principle of supply and demand (push – pull effect), we would call the migrant crisis particularly favorable for the perpetrators, because the demand is very high. Identified cases of labor trafficking across Europe suggest that victims may be recruited through advertisements for nannies, waitresses or jobs in cleaning, construction, transportation, and agriculture.[53] Some authors however distinguish trafficking for forced labour, trafficking for labour exploitation and labour trafficking.[54]

---

[49] Article 418-b(3), Criminal Code, Republic of North Macedonia.

[50] *Akademik* <https://akademik.mk/mvr-nitu-eden-od-migrantite-vo-vaksintse-ne-posochil-deka-e-zhrtva-na-prisilba-zakana-ili-utsena-3/, (04/21).

[51] *Channel 4 News* <http://www.channel4.com/news/tracking-down-macedonias-migrant-kidnap-gang> (04/21).

[52] *Situation Report: Trafficking in Human Beings in the EU,* Europol, Hauge, 2016, <https://www.europol.europa.eu/publications-documents/trafficking-in-human-beings-in-eu (03/21).

[53] A. Volodko, E. Cockbain & B,Kleinberg, "*Spotting the signs" of trafficking recruitment online: exploring the characteristics of advertisements targeted at migrant job-seekers. Trends in Organized Crime*, Springer, 2019.

[54] N. Ollus, A. Jokinen, & M. Joutsen, *Exploitation of Migrant Workers in Finland, Sweden, Esto-*

We assume that labor exploitation is most prevalent among traffickers targeting migrant victims, for two main reasons:

- job offers along with accommodation are the most sought after by migrants, so they could easily be tempted and
- the group of migrants and refugees may be heterogenic, but is mostly composed of adult males[55], so it is easier for traffickers to detect victims from this wide group that would benefit the most if they exploited them several times. By physiognomy, men are more resilient to pain, more persistent in their quest to reach their destination, and often have other people dependent on their arrival at the desired destination, which makes them ideal victims for traffickers.

Forced Labor Convention[56] defines forced or compulsory labor as: "all work or service which is exacted from any person under the threat of a penalty and for which the person has not offered himself or herself voluntarily." According to the International Labor Organization there are specific indicators that point to forced labor like.[57] United Nations office on drug and crime[58] says that people who have been trafficked for the purpose of labor exploitation are typically made to work in sectors such as: agriculture, construction, entertainment, service industry and manufacturing. People who have been trafficked for labor exploitation may: live in groups in the same place where they work and leave those premises infrequently, if at all, live in degraded, unsuitable places, such as in agricultural or industrial buildings, not be dressed adequately for the work they do, be given only leftovers to eat, have no access to their earnings, have no labor contract, work excessively long hours, depend on their employer for a number of services, including work, transportation and accommodation.

Macedonian NGO La Strada aware about this kind of fake job offers that could be found online in Macedonia, and explains how to recognize one. They

---

nia and Lithuania: Uncovering the Links Between Recruitment, Irregular Employment Practices and Labour Trafficking, European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI), Helsinki, 2013, p.13 - They said that forced labour does not necessarily entail trafficking. Forced labour may exist without trafficking, but many jurisdictions require that for the crime of labour trafficking to be fulfilled, there must be exploitation that amounts to forced labour (or equivalent exploitation). Trafficking for forced labour hence exists where trafficking in human beings and forced labour overlap. Overall, both crimes can be seen to take place in the context of exploitation of (mainly migrant) labour.

[55] The most common irregular migrants transiting through the territory of Macedonia in the period 2016-2019 are adult males - *Human trafficking and smuggling migrants in North Macedonia - report*, Macedonian Young Lawyers Association, 2019, p.40

[56] Forced Labour Convention (No. 29), International Labour Organization, 1930, <https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C029 > (03/21)

[57] *Operational indicators of trafficking in human beings. Results from a Delphi survey implemented by the ILO and the European Commission*. International Labour Organization, Geneva, 2009, <http://www.ilo.org/sapfl/Informationresources/Factsheetsandbrochures/lang- - en/docName--WCMS_105884/index.htm> (03/21).

[58] Human Trafficking Indicators, untitled (unodc.org).

suggest, before applying for a certain job, that we need some time to research the agency or the company that offers the job - to visit the website, to search how professional they are. They emphasis that serious bidders usually have their own domain and do not send emails and bids from public domains such as Gmail, Outlook, Hotmail, Yahoo, etc. Bidders who have their headquarters usually also have a landline phone, not just a mobile phone. La Strada suggests if a foreign phone numbers is given, first to check the number or email address on Google or another browser. During our little research on web mentioned under, we found a lot of advertisements that use same phone number for selling products and offering jobs abroad.

The websites 419scam.org or scamnbers.info, can be used to check if any of the listed phone numbers have been used for fraud before. After searching for the phone number, the name of the person that is communicated with should be researched profoundly. Authors of fake companies are trying to make everything look convincing, but some details can be revealed. Their advertisements often contain pictures that can be find on the Internet, for their Skype profile, or to submit them through a website or Facebook. La Strada strongly recommends avoiding job advertisements abroad that are urgently looking for workers. If the offer does not require special education, experience or knowledge of the language and offers a very high salary, be careful because it may be fraud or an attempt at abuse or exploitation.

Having in mind this (post) indicators, we set some of the potential indicators that could point to possible trafficking for labor exportation, or just labor exploitation in their advertisement phase. Online advertisements that could be created by perpetrators, probably include several constants that are attempting for migrants at first place like: country of destination, accommodations included, help in arranging documents, previous experience not required, also knowledge of the language of the country of destination is not required, transportation to the desired destination included, transportation to workplace too, indefinite duration of work engagement, etc.[59] With this in mind, we searched through Macedonian internet sites, Facebook profiles and Instagram profiles for sites that offer employment. Although the ads are mostly in Macedonian language, the site itself offers English translation, so are reachable. Offers for work abroad (EU countries in mind) that are posted on the pages of companies for which contacts can be found in the yellow pages, are usually legitimate and registered[60]. However, there are also some adds on other websites that are quite symptomatic and look darker.[61] Several ads that date from March and April 2021, say: "Possibility to work in Germany for more workers (m / h) in warehouse (packaging). Hourly rate 10.50 Euros, gross. It works in 3 shifts. The hourly rate for the 3rd

[59] N. Ollus et al., cit. *supra* note 54, p.17.

[60] *Yellow pages* <https://zk.mk/vrabotuvanje-vo-stranstvo-agencii-za-posreduvanje> (04/21).

[61] For example – *Pazar 3* <https://www.pazar3.mk/oglasi/rabota-biznis/rabota/rabota-vo-stranstvo> (04/21).

shift is 50% higher. Accommodation provided, 150 Euros per month. Provided transportation to work and back to accommodation, 150 Euros per month. Transport to Germany, provided. All you need to apply is a passport photo." and refer to additional communication on WhatsApp or Viber. Another add titled as "work abroad" says that all the parameters are irrelevant – documents, gender, language skills, education, skills… and refers also for further e-mail or phone communication.[62] There is one add that asks for translator for Iranian language, for refugee camp. This add is not advertised officially, the site is suspicious by itself, but also is very attempting for migrants/refugees who are stuck in the country or in need for money. Without any specifications, it refers to further phone communication.[63] There are plenty adds like these that could be attempting for everyone, but especially for migrants that urge to get to the countries in EU even in the condition of global pandemic. Because of the pandemic, borders were closed, smuggling migrant cases went higher than in previous year, and in the period of October, November, and December it was noticed increased number of refugees/migrants coming or returning from Serbia.[64] Over the past few months, (2021), the flow of migrants along the Balkan route has intensified with thousands of refugees from Central Asia and the Middle East taking that route to reach Western Europe.[65] So, the number of migrants that are searching for a way out of Macedonia went up in the past months.

Supported by the EU and Council of Europe Horizontal Facility Programme and implemented by the NGO Open Gate, member of the international anti-trafficking network La Strada, started a campaign "Opportunity or exploitation" that explains the perils of human trafficking for labour exploitation to young and unemployed persons. The awareness aims to prevent trafficking of human beings through warning the public and vulnerable groups about the existence of fake offers / recruitment through fraud or deception with the aim of exploitation. Focus of the campaign is to recognize fake offers when searching for a job within the country and abroad. This action is part of the joint European Union/Council of Europe program "Horizontal Facility for the Western Balkans and Turkey 2019 – 2022".[66]

We must emphasize that these indicators (provision of accommodation, transport to work, transfer to destination country and help with settling in..) are not necessarily indicative of criminal activity or exploitative conditions. Ac-

---

[62] *Reklama 5* <https://reklama5.com.mk/AdDetails?ad=2668591> (04/21).

[63] *Pazar 3* <https://www.pazar3.mk/oglas/rabota-biznis/rabota/drugo/se-nudi-rabota/kumanovo/kumanovo-opstina/se-bara-preveduvac-za-iranski-farsi-jazik/2455151> (04/21).

[64] *FIELD REPORT 2020, October-November-December*, Macedonian Young Lawyers Association, 2019, pg.4 available at <Q4 Field Report October - November - December (myla.org.mk)> (04/21).

[65] *Migrants: Hungarian police at Serbia-Macedonia border, February*, 2021 <Migrants: Hungarian police at Serbia-Macedonia border - General news - ANSAMed.it> (04/21).

[66] *Council of Europe* <https://www.coe.int/en/web/skopje/-/-opportunity-or-exploitation-a-new-public-awareness-campaign-on-human-trafficking-for-labour-exploitation-in-north-macedonia> (04/21).

cording to UNDOC and ILO they could indicate trafficking but could also be present in legitimate work relations. Such services might be provided by employers in jobs that recruit migrant workers, who sometimes do not speak the language of the destination country or might require assistance navigating a new system. In fact, certain sectors in Western Europe are now dependent on relatively cheap migrant labor, so it seems reasonable that employers (including employment agencies) seeking migrant labor would also be willing to provide additional support.[67] However, that deception is said to be more common than outright coercion as a means of recruiting people – online included - into situations of labor trafficking,[68] and low payments (under the minimum) and other indicators point to the certain further labor exploitation.[69]

5. Instead of a Conclusion

Technology is increasingly important for organized criminals, and the new forms of organized crime managed to use it in their favor. And yet, legislator reacts slowly to technological change, with the result that the use of some technologies for criminal purposes, is not incriminated. It can be difficult and resource-intensive to identify victims of trafficking, smuggled migrants with protection need), and other potential victims of abuse and exploitation. However, victims of abuse and exploitation avoid seeking protection and assistance because they fear deportation on account of their irregular status. Similarly, the services available are still too often dependent on factors such as age, sex, nationality, migration status, type of exploitation, location of exploitation and who identified the victim.[70]

Cyber trafficking is firstly covered by the respective international anti-trafficking instruments, - Palermo Protocol from 2000[71], and the three Protocols against Trafficking in Persons, Smuggling of Migrants, and Illicit Manufacturing of and Trafficking in Firearms.[72] Then UN Convention against Transnational Organized Crime, the 2005 Council of Europe's Convention on Action

[67] N. Ollus et al., cit. *supra* note 54, p. 25.

[68] E. Cockbain, & K, Bowers, *Using Data Science Techniques Better to Understand Human Trafficking,* The United Nations 4th International Conference on Governance, Crime and Justice Statistics, Lima, June 2018.

[69] <https://lastrada.org.mk/labor-exploitation/?lang=en> (04/21).

[70] *Issue Brief #5, Smuggling of migrants, trafficking in persons and contemporary forms of slavery, including appropriate identification, protection and assistance to migrants and trafficking victims,* United Nations, < https://refugeesmigrants.un.org/sites/default/files/ts5_issue_brief.pdf > (04/21).

[71] Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, Adopted and opened for signature, ratification and accession by General Assembly, resolution 55/25 of 15 November 2000.

[72] A. Guterres, *Greater cooperation urged worldwide as criminals seek to profit from COVID-19*, 2020, <https://news.un.org/en/story/2020/10/1075182>.

against Trafficking in Human Beings,[73] Convention on Cybercrime.[74] European Court of Human Rights has also recognized vast positive obligations of States towards victims of human trafficking under Article 4 of the European Convention of Human Rights.[75] So, we could see that when it comes to trafficking in human beings, from the point of recruitment, until the destination – it is not only one country's problem. The Internet Referral Unit of Europol[76] monitors online content and referring pages linked to migrant smuggling criminal networks. Republic of Macedonia, in 2016, has developed specific "Indicators for Initial/Preliminary Identification of Presumed and Potential Victims of Trafficking in Human Beings in the Context of Mixed Migration Flows".[77]

As countries have closed their borders due to the pandemic, some victims are unable to return home. Others face delays in legal proceedings, as well as a reduction in the support and protection they rely on. Some are also in danger of further abuse or neglect by their captors.[78] Traffickers may become more active and prey on people who are even more vulnerable than before because they have lost their source of income due to measures to control the virus.[79] All movement restrictions have made migrants more vulnerable to exploitation and trafficking. Organized crime groups are selling substandard and falsified medical products, targeting individuals, health facilities and public agencies through internet scams. Falsified COVID vaccines will soon be a lethal reality and governments need to be prepared to counter this threat.

[73] Full list (coe.int).
[74] Convention on cybercrime, Concil of Europe, 2001.
[75] L.E. v Greece, J. and others v. Austria, Chowdury and others v. Greece….
[76] *Europol* <https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru> (04/21).
[77] *Council of Europe* <https://rm.coe.int/16806ed5a5> (04/21).
[78] *United Nations* <https://news.un.org/en/story/2020/05/1063342> (04/21).
[79] Mr. Chatzis, Chief of the agency's Human Trafficking Section.

DIRITTI UMANI FRA CAPITALISMO DELLA SORVEGLIANZA ED ETICA HACKER

Maria Chiara Vitucci

1. Premessa

Quando si parla di hacker o hacking occorre anzitutto sgomberare il campo da un equivoco di fondo. Secondo i media *mainstream* l'hacker è un pirata informatico, cioè qualcuno che sfrutta le vulnerabilità dei sistemi informatici per rubare o manomettere dati. Il termine corretto per definire la figura di chi si dedica al furto o alla manomissione di dati è invece *cracker*, ma la confusione ha fatto breccia nell'immaginario collettivo, tanto che anche secondo la definizione del vocabolario Treccani con il termine hacker si designa "chi, servendosi delle proprie conoscenze nella tecnica di programmazione degli elaboratori elettronici, penetri abusivamente in una rete di calcolatori per utilizzare dati e informazioni in essa contenuti, per lo più allo scopo di aumentare i gradi di libertà di un sistema chiuso e insegnare ad altri come mantenerlo libero ed efficiente".[1] Almeno da questa voce emergono lo scopo "alto" che muove l'azione di hacking e il rapporto fra questa e la nozione di libertà. Vengono in rilievo la libertà di espressione, la libertà di informazione, ma anche il diritto a una vera e propria autodeterminazione informativa, garantito nella Dichiarazione dei diritti in internet, approvata in Italia nel luglio del 2015, e strettamente connesso con il diritto alla privacy.[2] Se di pirati si vuole parlare, anche in omaggio all'altro spazio navigabile di cui tratta il volume, dobbiamo pensare a capitan Harlock, cioè un pirata con un altissimo senso della giustizia.[3]

In realtà l'hacker vuole garantire i *cyber rights*, cioè il diritto alla privacy e all'autodeterminazione informativa, a sé stesso e ai membri della comunità di cui fa parte e con la quale instaura un rapporto di profonda collaborazione, secondo lo spirito della condivisione dei saperi e della libertà della ricerca fondata su autentica curiosità e desiderio di divertirsi.[4] La consapevolezza del fatto che la tecnologia non è neutra, sulla scia tracciata da Orwell, che vede nella tecnologia la chiave di volta per la costruzione di una società totalitaria, rischia di rendere l'hacker un paranoico. Gran parte dei suoi sforzi è quindi dedicata a convincere gli altri dei rischi insiti nel-

[1] Treccani voce "hacker" <https://www.treccani.it/vocabolario/hacker/ > (06/21).

[2] https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf. A livello internazionale, v. la Carta dei diritti umani e principi di internet, su cui *infra* nota 26.

[3] F. Pennacchi, *Fammi volare capitano. Viaggio nell'universo di Harlock e Matsumoto Leiji*, CR edizioni (https://cannibaliere.blomming.com), 2020.

[4] Cfr. la voce "Pedagogia hacker", in Ippolita, *Tecnologie del dominio. Lessico minimo di autodifesa digitale*, Meltemi, Milano, 2017, pp. 197 ss.

la tecnologia, rischi che solo se conosciuti, possono essere arginati. C'è chi ha pagato e sta ancora pagando un prezzo molto alto a livello personale per aver voluto condividere col mondo la conoscenza delle violazioni dei diritti umani compiute dai governi di alcuni paesi, con la scusa di proteggere la sicurezza nazionale.[5] Mi riferisco a Edward Snowden, cui una recentissima decisione della Corte europea dei diritti umani sembra aver dato finalmente ragione.[6] La sentenza ha infatti affermato che le intercettazioni di massa del Regno Unito, di cui alle doglianze degli attori (diverse ONG – organizzazioni non governative – e alcuni individui), non sono state effettuate in modo tale da garantire i privati contro i rischi di abuso. Di conseguenza si è verificata una violazione dell'art. 8 (e anche dell'art. 10) della Convenzione europea.

2. Digital rights

All'inizio del mese di giugno 2021 si è verificato un problema tecnico che ha causato il blocco di moltissimi siti internet in tutto il mondo, tra cui alcune delle principali testate giornalistiche mondiali.[7] Il blocco è durato solo 40 minuti, ma le *home page* dei siti hanno comunque sperimentato rallentamenti per parecchie ore. Il problema tecnico riguardava il sistema di Fastly, una delle aziende più utilizzate (da qui la capillarità del problema) per i servizi di *content delivery managment*, cioè la rete di server che fornisce servizi di cloud a tutti i siti che hanno subito il blocco.

Non richiamo questo episodio per dire che in un primo momento si è parlato di un attacco hacker su grande scala, bensì per evidenziare i problemi che, in una società iperconnessa come la nostra, simili eventi possono causare: a prescindere dal blackout informativo, che tutto sommato non rappresenta un danno troppo significativo, penso alle persone che non hanno potuto imbarcarsi a bordo di aerei perché non era arrivato loro in tempo il risultato del tampone, oltre al blocco di piattaforme di commercio elettronico o siti di pagamento. Al tempo stesso l'episodio contribui-

[5] Cfr. E.J. Snowden, *Permanent Record*, Metropolitan Books, New York, 2019.

[6] European Court of Human Rights, *Big Brother Watch et al. v. the United Kingdom* Applications Nos. 58170/13, 62322/14 and 24960/15) Grand Chamber, sentenza del 25 maggio 2021. Lo stesso giorno la Grande Camera ha reso anche una seconda sentenza, sempre in tema di sorveglianza di massa: European Court of Human Rights, *Case of Centrum för Rättvisa v. Sweden* Application No. 35252/08 Grand Chamber, sentenza del 25 maggio 2021. Per la precedente giurisprudenza della Corte, cfr. A. Stiano, "Il diritto alla privacy alla prova della sorveglianza di massa e dell'intelligence sharing: la prospettiva della Corte europea dei diritti dell'uomo", *Rivisita di diritto internazionale*, 2020, p. 511 ss.

Occorre rilevare che la Grande Camera, pur avendo ritenuto violati *nel caso concreto* i diritti dei ricorrenti, non ha giudicato i sistemi di sorveglianza di massa *di per sé* contrari alla Convenzione, ponendo così le basi per una loro "normalizzazione": in questo senso, v. M. Milanovic, "The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa" <https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/> (06/21).

[7] <https://www.agi.it/estero/news/2021-06-08/internet-inaccessibili-migliaia-siti-tutto-mondo-12842518/> (06/21).

sce a esemplificare plasticamente uno dei diritti digitali, il diritto di accesso a internet: tale diritto va oltre il mero diritto a essere tecnicamente connessi alla rete, ma deve essere inteso come condizione di accesso a una cittadinanza digitale. Rodotà ha scritto efficacemente che il diritto di accesso "si presenta ormai come sintesi tra una situazione strumentale e l'indicazione di una serie tendenzialmente aperta di poteri che la persona può esercitare in rete".[8] La circostanza che oggi il diritto di accesso alla rete rappresenta uno strumento indispensabile per rendere effettivo un gran numero di diritti fondamentali e quindi, sostanzialmente, per il mantenimento della democraticità del sistema è confermata da un rapporto presentato all'Assemblea generale delle Nazioni Unite.[9]

2.1. Big data, privacy e anonimato

Compiendo un passo ulteriore rispetto al mero diritto di accesso, possiamo introdurre il diritto all'anonimato in rete, che rappresenta una precondizione all'esercizio della libertà di manifestazione del pensiero. L'ondata securitaria e di controllo, che ha avviluppato la rete e non solo, ha fatto dimenticare l'esistenza del diritto all'anonimato, che può certamente essere limitato quando si devono proteggere altri diritti (ad esempio la tutela di una persona dalle diffamazioni in rete), ma che deve comunque essere garantito contro lo strapotere di alcuni giganti della rete quali Google o Facebook che, al pari di alcuni Stati autoritari come la Cina, subordinano l'accesso alla cosiddetta *real name policy*, ovvero la dichiarazione della propria identità. In questo caso è necessaria l'elaborazione di nuove strategie che consentano l'identificazione della persona in caso di effettiva necessità, senza tuttavia imporre un generalizzato obbligo di trasparenza assoluta. Anche perché spesso chi impone questo obbligo è un soggetto privato, che vuole ottenere i dati a fini di profilazione, per poi utilizzarli a scopi pubblicitari. Una delle reazioni a tali pretese è rappresentata dalla scelta individuale di non utilizzare i social network o sostituire Google con altri motori di ricerca che garantiscano il diritto alla privacy degli utenti, come ad esempio Qwant.[10] Un'altra reazione sta nella creazione di soggetti collettivi quale Anonymous, che fa dell'anonimato una battaglia politica.[11] I meccanismi di autodifesa digitale presentano comunque vari livelli di protezione, in funzione del livello di consapevolezza e di conoscenza tecnica dell'utente.[12] È curioso che mentre la reazione sociale a un'attività così pervasiva compiuta a scopi politici suo-

[8] Cfr. S. Rodotà, *Il diritto di avere diritti*, Laterza, Bari, 2012, p. 384.

[9] *Report of the Special Rapporteur on the promotion and protection of the right of freedom of opinion and expression*, UN Doc. A/HRC/17/27 del 16 maggio 2011, p. 22. Cfr. anche le risoluzioni dell'Assemblea Generale 68/167 del 18 dicembre 2013, 69/166 del 18 dicembre 2014, 71/199 del 19 dicembre 2016, 73/179 del 17 dicembre 2018 e 75/176, del 28 dicembre 2020 dal titolo *The right to privacy in the digital age*.

[10] Questo almeno è il suggerimento del docufilm del 2020 *The Social Dilemma*, di Jeff Orlowski.

[11] <https://anonitaly.blackblogs.org> (06/21).

[12] Oltre alla voce già richiamata *supra* alla nota 4, cfr. anche la voce "Digital labour", in Ippolita, *Tecnologie del dominio. Lessico minimo di autodifesa digitale*, cit., p. 88.

le suscitare reazioni indignate (si pensi allo scandalo sollevato dal caso Prism negli Stati Unti),[13] l'analoga operazione compiuta da soggetti privati (che poi talvolta vendono i dati forniti più o meno volontariamente dagli utenti) non ha prodotto analoghi movimenti di protesta.

Coloro che sono favorevoli alle misure di sorveglianza che ledono la privacy degli individui sono soliti sostenere, a sostegno della loro posizione, che chi non fa niente di male non ha nulla da temere. Si può agevolmente replicare che proprio perché non si sta facendo nulla di male non c'è alcun bisogno di essere sorvegliati e che la privacy non ha nulla a che fare con il nascondere qualcosa di sbagliato.[14] Il diritto alla privacy, chiamato in alcuni ordinamenti diritto alla riservatezza, è invece un diritto umano garantito in numerose convenzioni internazionali.

Data la struttura della rete, è evidente che il diritto alla privacy online deve essere adeguato ad essa. Già nel mondo reale si è passati dal tradizionale diritto a "essere lasciato solo" a una nuova e più ampia nozione di sfera privata. Il nuovo significato sociale della privacy non è più ancorato al criterio di esclusione dell'altro, ma comprende anche il diritto a seguire le proprie informazioni ovunque esse si trovino.[15] Il passaggio dall'originaria nozione di privacy alla protezione dei dati personali, elaborato soprattutto in ambito europeo, riflette il profondo e strutturale mutamento avvenuto nelle modalità di invasione della sfera privata. Oggi quindi, quando si parla di privacy in rete, si deve intendere quell'insieme di poteri che consentono forme di controllo sui diversi soggetti pubblici e privati che esercitano la sorveglianza su tutte le nostre azioni in rete.[16]

Nel 2013 Snowden ha svelato al mondo che la National Security Agency (NSA) statunitense stava intercettando, registrando e analizzando le comunicazioni digitali del paese, estraendone ogni tipo di informazioni. Tale massa di informazioni, i cosiddetti *big data*, permette di influenzare i comportamenti umani, da cosa acquistare a cosa votare; si parla infatti al riguardo di capitalismo della sorveglianza.[17] Emerge quindi la necessità di elaborare una visione più ampia di privacy, che si distacchi dal mero rispetto alla vita privata e familiare. Questo può essere fatto in via normativa in sistemi altamente evoluti: ad esempio, la Carta dei diritti fondamentali dell'Unione europea, accanto all'art. 7 che prevede il diritto al rispetto della vita privata e familiare, comprende anche l'art. 8, che riconosce un diritto separato alla protezione dei dati personali. In altri sistemi l'evoluzione è giurisprudenziale: la Corte di Strasburgo, nel caso richiamato sopra, ha considerato il diritto alla protezione dei dati personali ricompreso in altri diritti previsti nella Convenzione europea dei diritti umani, che era stata elaborata nel 1950, quando intrusioni nella sfera

[13] <https://www.valigiablu.it/tutto-quello-che-devi-sapere-sullo-scandalo-prism/> (06/21).

[14] Questo è l'incipit di un saggio seminale sulla privacy: cfr. B. Schneier, "The Eternal Value of Privacy", *Wired*, 18 maggio 2006, <https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html> (06/21).

[15] Cfr. S. Rodotà, *Il diritto di avere diritti*, cit., p. 394 ss., p. 396.

[16] Ibidem, p. 397.

[17] Cfr. S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York, 2019.

personale come quelle compiute dalla NSA erano descritte solo nei libri di fantascienza.

Sempre in Europa, secondo la più recente legislazione, la raccolta dei dati è legittimata non solo dal consenso dell'interessato (tutti noi sappiamo bene quante volte questo consenso sia solo fittizio) ma anche da un soggetto pubblico che ha valutato preventivamente l'ammissibilità della raccolta di alcuni dati da parte di soggetti privati e le limitazioni nella raccolta e nella conservazione.[18] Il problema è che troppo spesso, a livello globale, i dati personali e il loro utilizzo sono gestiti non da persone, bensì da algoritmi che compiono processi automatizzati di cui non si capisce chi possa essere responsabile, perché spesso è ignota o non conoscibile la logica applicata dalle macchine.[19] La questione presenta risvolti inquietanti anche perché oramai è stato evidenziato quanto gli algoritmi non siano neutri. A mero titolo esemplificativo può essere richiamato il recente documentario sull'intelligenza artificiale *Coded bias*, che illustra in maniera emblematica i pregiudizi (razziali e di genere) degli algoritmi di riconoscimento facciale.[20]

3. La protezione dei diritti digitali nella società sorvegliata

Vari organi delle Nazioni Unite si sono occupati dell'impatto dei sistemi di sorveglianza sui diritti umani. Vi è in particolare un rapporto del Relatore speciale per la promozione e protezione del diritto alla libera manifestazione di opinione e di espressione dedicato alla sorveglianza su obiettivi specifici (*targeted surveillance*); in genere si tratta di giornalisti, difensori dei diritti umani e dissidenti,[21] mentre altri rapporti analizzano il problema della sorveglianza di massa.

In tali rapporti si mettono in rilievo gli obblighi in materia di diritti umani che

[18] V. <https://protezionedatipersonali.it/regolamento-generale-protezione-dati> (06/21).

[19] Occorre tener presente, al riguardo, che a livello europeo (sia nell'ambito dell'Unione europea che del Consiglio d'Europa) è stato affermato il diritto del portatore di dati personali a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona (v. l'art. 22 del Regolamento europeo per la protezione dei dati personali, e il nuovo articolo 9 della Convenzione n. 108 del Consiglio d'Europa del 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, così come modificato dal Protocollo di emendamento del 10 ottobre 2018). V. anche l'art. 14 della proposta di Regolamento sull'intelligenza artificiale, che stabilisce l'obbligo di assicurare una "sorveglianza umana efficace" sui sistemi di intelligenza artificiale ad alto rischio, tra i quali possono senz'altro rientrare gli algoritmi di riconoscimento facciale), <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206&from=IT> (06/21).

[20] Per il trailer del film documentario *Coded bias*, del 2020, del regista Shalini Kantayya, cfr. <https://www.imdb.com/video/vi181780761?ref_=nv_sr_srsg_1> (06/21). Più in generale, sul problema relativo alle discriminazioni operate dagli algoritmi, cfr. <https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html> (06/21).

[21] *Report of the Special Rapporteur on the promotion and protection of the right of freedom of opinion and expression*, UN Doc. A/HRC/41/35 del 28 maggio 2019.

incombono sugli Stati e che sono violati da simili meccanismi.[22] Vi sono anzitutto l'art. 19 della Dichiarazione universale dei diritti umani e del Patto delle Nazioni Unite sui diritti civili e politici che garantiscono a ogni individuo il diritto a non essere molestato per le proprie opinioni e il diritto alla libertà di espressione, che comprende la libertà di cercare, ricevere e diffondere informazioni e idee di ogni genere. Vi è poi l'art. 17, par. 1 del Patto sui diritti civili e politici ai sensi del quale: "nessuno può essere sottoposto a interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza". Nel mondo digitale la privacy è strettamente connessa alla libertà di opinione e di espressione poiché le garantisce. Ogni restrizione nei diritti appena enunciati deve rispondere a precisi requisiti: deve essere prevista dalla legge ed essere necessaria al rispetto dei diritti o della reputazione altrui e alla salvaguardia della sicurezza nazionale, dell'ordine pubblico, della salute o della morale pubbliche.[23]

Altro strumento che può essere utilizzato è l'Accordo di Wassenaar relativo ai controlli delle esportazioni di armi convenzionali e beni e tecnologie a duplice uso. Infatti nel 2013 gli Stati parti hanno aggiunto tra i beni della lista il software e le reti di comunicazione che permettono la sorveglianza.[24]

Visto che spesso le violazioni sono compiute da aziende private, vengono in rilievo anche i Principi guida su imprese e diritti umani, una serie di direttive elaborate nel 2011 dalle Nazioni Unite e che devono guidare le azioni delle imprese, garantendo il rispetto dei diritti umani.[25] Si tratta di uno strumento giuridicamente non vincolante; deve rilevarsi che al momento attuale, anche quando le compagnie adottano delle politiche in materia, spesso si tratta di politiche assai vaghe.

Si deve infine porre in rilevo l'azione coordinata dei vari attori della società dell'informazione, diretta alla riflessione e alla elaborazione di regole per la *governance* di internet. In tale contesto occorre menzionare il dialogo che si svolge nell'ambito dell'*Internet Governance Forum*, piattaforma istituita dal Segretario dell'ONU nel 2006 come risultato del summit mondiale sulla società dell'informazione (WSIS) e che è diventata negli anni il punto di riferimento per la discussione globale sui temi della *governance* di internet;[26] deve inoltre essere richiamato il Panel di alto livello sulla cooperazione digitale, creato anch'esso dal Segretario generale delle Nazioni Unite nel luglio 2018.[27]

---

[22] Per un'analisi di tali norme cfr. G. Della Morte, Big data *e protezione internazionale dei diritti umani. Regole e conflitti*, Editoriale scientifica, Napoli, 2018, p. 71 ss.

[23] Cfr. art. 19 del Patto sui diritti civili e politici; cfr. *Report of the Special Rapporteur on the promotion and protection of the right of freedom of opinion and expression*, UN Doc. A/HRC/41/35, cit., par. 24.

[24] <https://www.wassenaar.org/app/uploads/2020/12/Public-Docs-Vol-II-2020-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-20-3.pdf.> (06/21).

[25] V. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.

[26] Cfr. <https://www.intgovforum.org> (06/21). All'interno del forum è stata elaborata la Carta dei diritti umani e principi di internet: <https://internetrightsandprinciples.org/charter> (06/21).

[27] Cfr. *Report of the Secretary General, Road Map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation*, UN Doc. A/74/821 del 29 maggio 2020.

Nonostante tale quadro normativo di hard e soft law, non può non rilevarsi una pressoché totale assenza di rimedi per i casi in cui si verifica la sorveglianza: molto spesso la vittima non riesce a citare in giudizio né lo Stato dietro il progetto di sorveglianza né la società privata che ha materialmente fornito la tecnologia. Gli ostacoli che si frappongono a tali azioni sono l'immunità dello Stato e l'eccezione della sicurezza nazionale. Quest'ultima fa sì che l'autorizzazione giudiziale all'uso di tecniche di sorveglianza, ancorché necessaria, si riveli nei fatti insufficiente, dal momento che i giudici sono soliti concedere l'autorizzazione quando questa viene domandata per motivi di sicurezza nazionale. Non si è riusciti finora neanche a trovare strade alternative che portassero, ad esempio, a commissioni di verità.[28] Occorre comunque rilevare il forte ruolo a tutela della privacy svolto da parecchie organizzazioni non governative, anche mediante il loro coinvolgimento diretto in azioni legali, come è avvenuto, da ultimo, nel caso *Big Brother Watch*.[29]

Per quanto riguarda l'azione di *advocacy* delle ONG, richiamiamo ad esempio l'appello, redatto da *Access Now*, *Amnesty International*, *European Digital Rights*, *Human Rights Watch*, *Internet Freedom Foundation* e *Instituto Brasileiro de Defesa do Consumidor*, in cui si chiede la messa al bando delle tecnologie di riconoscimento biometrico che permettono la sorveglianza di massa, appello che è stato condiviso da più di 175 organizzazioni rappresentative della società civile.[30] Non bisogna ritenere che tali sistemi di controllo operino solo in paesi totalitari come la Cina: nell'appello viene richiamato espressamente il caso di Como, in Italia, dove il Comune ha installato sistemi di videosorveglianza con riconoscimento facciale nonché di rilevamento automatico di bighellonaggio e di oggetti rimossi.[31] Tale iniziativa volta, nella mente delle autorità locali, a rafforzare la sicurezza cittadina, ha richiamato l'attenzione del Garante per la protezione dei dati personali, che il 26 febbraio 2020 ha emanato un provvedimento in cui ingiungeva al Comune di conformarsi alle previsioni normative che subordinano la raccolta di dati biometrici a specifiche condizioni e garanzie, presupposti di ammissibilità, non presenti nel caso di specie.[32]

Può essere interessante rilevare che nell'appello delle ONG si ripete quanto già da noi osservato circa la differenza di attenzione riservata dal grande pubblico alle intrusioni nella privacy effettuate da autorità pubbliche, che da sempre attraggono attenzione e critiche, e l'uso di analoghe tecnologie da parte di privati, spesso su incarico di agenzie governative, che passa invece generalmente inosservato.[33]

A prescindere dai problemi di privacy che queste tecniche, adottate sulla base

---

[28] Cfr. *Report of the Special Rapporteur on the promotion and protection of the right of freedom of opinion and expression*, UN Doc. A/HRC/41/35, cit., par. 55.

[29] Cfr. *supra* nota 6.

[30] <https://www.accessnow.org/ban-biometric-surveillance/> (06/21).

[31] <https://www.wired.it/internet/regole/2020/06/09/riconoscimento-facciale-como/?refresh_ce=> (06/21).

[32] <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9309458> (06/21).

[33] <https://www.accessnow.org/ban-biometric-surveillance/> (06/21), p. 2.

del presupposto della loro necessità ai fini di rafforzare la sicurezza pubblica, possono comportare, si pongono anche questioni etiche più delicate. Si è parlato di *chilling effect* sulla libertà di espressione e si è già messo in rilievo l'alto rischio di discriminazione che deriva dai dati con cui sono stati "nutriti" gli algoritmi di riconoscimento facciale. Ma il vero problema è costituito dagli aspetti etici connessi al fatto che una società democratica introduca tecnologie così intrusive.[34] Da questo punto di vista è assai significativa la circostanza che la decima conferenza sui diritti digitali, RightsCon,[35] che si è tenuta all'inizio del mese di giugno del 2021, si sia conclusa, tra l'altro, con un comunicato congiunto da parte di ben 13 relatori di procedure speciali del Consiglio dei diritti umani delle Nazioni Unite.[36]

Ci piace mettere in relazione questa conferenza con un altro evento che dal 1993 si tiene tutti gli anni a Las Vegas, la Defcon, il più grande incontro di hacker, che riunisce vari professionisti del mondo della sicurezza, giornalisti, giuristi, agenti federali statunitensi (FBI, dipartimento di difesa e dipartimento sulla sicurezza nazionale non mancano mai), ricercatori in materia di cybersecurity, studenti e hacker con interesse nel software, nell'architettura della rete, nell'hardware, nei badge e in ogni cosa che può essere "hackerata".

4. Hacker e *hacktivism*

Senza la pretesa di tracciare qui la storia degli hacker,[37] ci limitiamo a dire che essi rappresentano gli eredi della controcultura degli anni settanta, che ha espresso personalità importantissime tanto per la creazione dei computer, dei software e della rete, quanto per le battaglie a favore dell'eticità della società informatica.

Ma l'hacking ha origine negli anni cinquanta tra i membri del Thec Model Railroad Club del MIT, dove un gruppo di studenti si dedicavano a smontare e rimontare di continuo un sistema ferroviario miniaturizzato. Dai binari si passa ai bit e la cultura hacker continua a crescere nello spirito libertario tipico della generazione cresciuta negli Stati Uniti dopo la seconda guerra mondiale.[38] In un volume decisa-

[34] Così Ioannis Kouvakas, consigliere giuridico di *Privacy International*, nell'articolo che può leggersi su *Wired*, <https://www.wired.it/internet/regole/2020/06/09/riconoscimento-facciale-como/?refresh_ce=> (06/21).

[35] <https://www.rightscon.org> (06/21). La prima riunione, la Conferenza sui diritti umani della Silicon Valley, era stata organizzata nel 2011. Da allora ogni anno RightsCon riunisce leader di imprese tecnologiche, difensori dei diritti umani, rappresentanti degli Stati, esperti di informatica e tecnologia e giornalisti da tutto il mondo per affrontare le questioni connesse all'interazione fra diritti umani e tecnologia.

[36] Per il testo del comunicato, nonché per la lista dei singoli esperti cfr. <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27140&LangID=E> (06/21).

[37] Rinviamo a F. Tavassi la Greca, "Per comprendere l'*hacking*: storia e valori di una cultura attuale", in Idem, Hacking *e criminalità informatica*, 2003, e alla bibliografia ivi citata. Il saggio può leggersi al seguente indirizzo: <http://www.adir.unifi.it/rivista/2003/tavassi/index.htm> (06/21).

[38] R. Mattera, "Al largo dei bastioni di Orione. Cyberpunk e cultura hacker," *Zapruder*, 45, 2018, p. 11 ss, p. 20.

mente agiografico, Steven Levy definisce gli hackers quali eroi della rivoluzione informatica.[39] Nel periodo pionieristico, tra gli anni settanta e novanta del secolo scorso, si è verificata una strettissima collaborazione tra hacker e scienziati, che ha poi fatto posto anche alla cultura cyberpunk e all'antagonismo sociale. Lo spirito comunitario che è nato da questo strano incontro ha generato l'etica hacker. Inoltre gli hacker hanno sempre sostenuto la necessità che le reti si sviluppassero nel rispetto di due valori fondamentali: la libertà di espressione e la privacy. Sono state soprattutto le azioni repressive condotte alla fine degli anni ottanta nei confronti delle reti telematiche amatoriali basate su BBS (bullettin board system),[40] prima negli Stati Uniti poi in Italia, a destare la preoccupazione che il ciberspazio potesse essere regolamentato in modo totalitario, mettendo a rischio questi diritti.[41] Da qui la nascita di numerose organizzazioni a loro tutela. E di qui anche l'interesse del diritto internazionale dei diritti umani per la vicenda.

Separando la vicenda statunitense da quella italiana e concentrandoci su quest'ultima, occorre rilevare come gli hacker italiani siano stati quasi subito connotati da una forte politicizzazione: almeno a partire dagli anni novanta hanno infatti riflettuto sull'uso sociale delle nuove tecnologie digitali, mostrando un particolare interesse per i nuovi mezzi ai fini di una (contro)informazione il più possibile libera e indipendente.[42] E chi fa politica si relaziona necessariamente con uno spazio di condivisione che non è solo virtuale. Di qui la nascita degli hackmeeting, il primo dei quali, nel 1998, è stato animato dal collettivo Strano Network, nato nel centro sociale ex-Emerson di Firenze.[43] Il passaggio dall'hacker all'*hacktivism* può dirsi dunque compiuto. Nella prima fase del movimento, i dieci anni che vanno dal 1990 al 2001, cioè dal movimento universitario della pantera al G8 di Genova, si assiste a un cambio di passo tecnologico, di cui il movimento si accorge e si appropria. Dapprima ci crea la European Counter-Information Network (ECN), uno strumento utilizzato dai vari gruppi per mettersi in comunicazione, poi si passa a CyberNet e infine nel 1993 al CERN si inventa il Web. Il rapido avanzare di internet si riflette nel modo di comunicare: dalle BBS si passa alle mailing list e nel 1996 Isole nella rete, un'associazione nata come BBC e appoggiata alla ECN, si sposta online e fornisce

[39] S. Levy, *Hackers: Heroes of the Computer Revolution*, 1984, Garden City, Doubleday.

[40] Si tratta di un software che, permettendo agli utenti di scambiare messaggi e file attraverso la rete telefonica, è il precursore delle comunicazioni telematiche. Gli scambi avvenivano a tarda notte attraverso il modem e i singoli utenti lasciavano che le persone si collegassero alla propria BBS. In un momento successivo nacquero network di BBS, spesso su base tematica, a volte anche internazionali. Intuendone l'enorme potenziale comunicativo e la sua indipendenza, le varie realtà di movimento iniziano ad utilizzare questo mezzo nelle loro attività politiche, cfr. Autistici & Inventati, + *kaos. 10 anni di hacking e mediattivismo* (a cura di L. Beritelli), Agenzia X, 2012, p. 31.

[41] Per le caratteristiche dello spazio cibernetico v. A. Sardu, "L'international cybersecurity law: lo stato dell'arte", *La Comunità internazionale*, 2020, pp. 5-42, p. 8. Per il giro di vite contro gli hacker, cfr. B. Sterling, *The Hacker Crackdown, law and disorder on the electronic frontier*, Tredition, 2013, disponibile online, <https://www.mit.edu/hacker/hacker.html> (06/21).

[42] I. Rossi, I. Severi, "Prove tecniche di trasmissione. Mediattivismo e 'paranoia'", *Zapruder*, 45, 2018, p. 2 ss., p. 3.

[43] Autistici & Inventati, + *kaos. 10 anni di hacking e mediattivismo*, cit.

agli utenti italiani il primo anonymous remailer, cioè un server che riceve messaggi di posta elettronica e li ritrasmette senza rivelare la loro provenienza originaria. All'interno del movimento comincia a diffondersi l'uso di server che non memorizzano i dati identificativi degli utenti; si invitano gli utenti all'uso della crittografia e si pubblicano manuali sulla privacy nelle comunicazioni online. Già prima, diverse BBS, come ad esempio Avvisi Ai Naviganti (AvANa),[44] nata all'interno del centro sociale Forte prenestino, ponevano una grande enfasi sull'uso della crittografia e sulla sua rivendicazione come strumento politico di sottrazione (dei dati) al controllo delle multinazionali e degli Stati. Nel 2000 nasce Indymedia Italia, un mezzo di informazione organizzato ma condiviso e trasversale, che avrà un ruolo fondamentale nella circolazione delle notizie a Genova.[45]

Sembra dunque che i temi sin qui affrontati si uniscono e contribuiscono a delimitare i confini dell'etica hacker.

A questo si deve aggiungere un forte impulso alla condivisione del sapere e alla educazione critica. Tali nodi vanno sotto il nome di pedagogia hacker e di esso si occupano molte realtà dell'hacktivismo. Gli hacktivisti si collocano in una linea ideale che nasce dalle proteste contro la guerra in Vietnam e dalle denunce della politica statunitense nel giardino di casa e che utilizza la tecnologia come mezzo per raggiungere gli obiettivi della propria azione politica.

Prima della rivoluzione digitale, la critica allo *status quo* era affidata a volantini e dazebao, fanzine e manifestazioni di piazza, ora invece la rete diventa una grande arena per discutere e contestare i rapporti ufficiali e i silenzi della stampa. Le azioni sulla rete possono essere suddivise, in linea di massima, in tre ampie tipologie: le campagne di informazione, le iniziative di protesta e il sabotaggio informatico. Ad accompagnare tutte queste azioni c'è comunque lo sforzo di smuovere le coscienze e di creare consapevolezza critica. Con il passaggio ai social network, infatti, la rete sta diventando sempre più un luogo di intorpidimento delle coscienze, amplificazione delle *fake news*,[46] e una grande piattaforma commerciale. Riteniamo che l'esperienza dell'hacktivismo possa svolgere un ruolo importante per arginare questo fenomeno.

E se il *Denial of Service*, consistente nel rendere temporaneamente inaccessibili dall'esterno alcuni siti governativi o commerciali, è un'azione di protesta, l'analoga azione compiuta dai governi merita una più attenta riflessione. Da qualche anno si è infatti diffusa la pratica degli Stati di oscurare internet e bloccare l'accesso a piattaforme quali Twitter o Facebook durante le proteste contro il governo. Un esempio

[44] "Avvisi ai naviganti (@forteprenestino.net)" (a cura di F. Mazzini), *Zapruder*, 45, 2018, p. 152 ss.

[45] Il portale Indymedia Italia era parte di una rete internazionale, l'Independent media center <www.indymedia.org> (06/21), nata grazie a diversi gruppi di attivisti che cercavano media alternativi e indipendenti per raccontare le proteste contro il WTO a Seattle. Per approfondimenti, cfr. *Millennium bug. Una storia corale di Indymedia Italia* (a cura di E. Del Frate, S. Menafra, P. Noschese, F. Urijoe e F. Vite), Alegre, Roma, 2021.

[46] In un recentissimo rapporto di Irene Khan, Special Rapporteur delle Nazioni Unite per la promozione e protezione del diritto alla libertà di opinione e espressione ci si concentra sulla "disinformation", cfr. *Disinformation and freedom of opinion and expression*, A/HCR/47/24 del 13 aprile 2021.

tra i tanti[47] può essere offerto da quanto avvenuto in Togo durante le proteste contro il prolungamento del mandato presidenziale. In occasione delle manifestazioni, il governo, oltre a reprimere brutalmente gli oppositori, ha interrotto l'accesso a internet nel paese, in palese violazione dell'art. 9 della Carta africana dei diritti dell'uomo e dei popoli, che garantisce il diritto all'informazione, e da altri strumenti internazionali che vincolano lo Stato. Il caso è stato portato davanti alla Corte di Giustizia della Comunità degli Stati dell'Africa Occidentale,[48] che il 25 giugno del 2020 ha condannato le autorità togolesi per la violazione del diritto alla libertà di espressione, di cui l'accesso a internet è presupposto indispensabile.[49] Il tribunale non ha considerato come esimente le giustificazioni fondate sulla sicurezza nazionale addotte dallo Stato. Anche se il diritto alla libera manifestazione del pensiero può essere limitato, le limitazioni devono essere previste dalla legge e tale non può essere considerato quello che all'epoca dei fatti era solo un disegno di legge sulla cybersecurity che permetteva simili shutdown.[50]

Nel corso del 2021, forse grazie anche alla massiccia campagna contro gli shutdown della rete lanciata nel 2016 e che oggi sostenuta da 243 associazioni,[51] il numero dei casi si è ridotto, ma possiamo ugualmente ricordare il blocco di internet nella fase più acuta della guerra del Tigray in Etiopia, l'analoga azione della giunta militare in Myanmar, la deliberata distruzione delle infrastrutture dedicate alle telecomunicazioni a Gaza durante l'intervento israeliano del mese di maggio 2021, nonché l'intermittente accesso alla rete telefonica in Kashmir o in India durante la recente protesta degli agricoltori. Si è poi diffusa la pratica di sospendere alcuni servizi internet (quali l'accesso alle piattaforme e ai servizi di messaggistica) a ridosso delle elezioni in molti paesi tra cui Uganda, Repubblica democratica del Congo, Nigeria, Bielorussia e Myanmar.[52] Infine durante le proteste in diversi paesi sono stati rilevate difficoltà di accesso alla rete o veri e propri blocchi: questo produce l'effetto di mettere a tacere le denunce sulla violazione dei diritti umani durante le proteste. Peraltro in paesi nei quali quasi tutta la connettività passa attraverso le reti mobili (come avviene in molti paesi in via di sviluppo) il blocco di queste ultime equivale a una interruzione pressoché assoluta del traffico in rete. Contro queste pratiche di disinformazione mosse dagli Stati, il Consiglio per i diritti umani delle Nazioni Unite non ha esitato a levare la propria voce di condanna.[53]

---

[47] Chi si volesse rendere conto dell'evoluzione, può guardare il sito <https://avana.forteprenestino.net> (06/21).

[48] <http://prod.courtecowas.org/wp-content/uploads/2020/07/JUD-ECW-CCJ-JUD-09-20-AMNESTY-INTERNATIONAL-TOGO-7-ORS-V.-REPUBLIC-OF-TOGO-of-6-july-2020.pdf.> (06/21).

[49] Ibidem, par. 38, dove si legge "access to internet is not *stricto sensu* a fundamental human right but since internet service provides a platform to enhance the exercise of freedom of expression, it then becomes a derivative right that is a component to the exercise of the right to freedom of expression".

[50] Ibidem, par. 43 e par. 45.

[51] <https://www.accessnow.org/keepiton/> (06/21).

[52] Cfr. il rapporto *Disinformation and freedom of opinion and expression*, A/HCR/47/24, cit., par. 50.

[53] Risoluzione del Consiglio dei diritti umani 44/12 del 16 luglio 2020, *Freedom of opinion and expression*.

L'azione delle numerosissime organizzazioni coinvolte nella campagna #KeepItOn è stata capillare. Sono state preparate linee guida per le compagnie di telecomunicazioni e gli internet provider nelle quali si richiama l'attenzione sull'importanza di eseguire solo ordini legittimi e si spiega come limitare gli effetti dirompenti di tali blocchi. Al tempo stesso le organizzazioni internazionali sono invitate a mantenere alta la pressione sugli Stati che hanno imposto le misure restrittive. Appare evidente – anche se purtroppo non si tratta di un'azione molto conosciuta dal grande pubblico – l'importanza di questa e di analoghe campagne promosse dalle ONG.

5. Conclusioni

Anche se è indubbio che i nuovi mezzi offerti dalla tecnologia possono fungere da volano all'azione a difesa dei diritti umani, gli stessi strumenti sono potenzialmente in grado di nuocere gravemente alla tutela dei diritti umani: come aveva intuito Orwell, la tecnologia non è neutra.

Nel corso dell'indagine abbiamo (consapevolmente) descritto talvolta con toni manichei un quadro che tale non è. Non ci sono solo hacker buoni e hacker cattivi, società private desiderose di fare profitti vendendo i nostri dati al miglior offerente e Stati dediti alla sorveglianza globale per reprimere le minacce alla sicurezza. Spesso però l'esagerazione ha il vantaggio di mostrare ciò che ci ostiniamo a non vedere, pur avendolo costantemente sotto gli occhi. Proprio nei giorni in cui scrivevo questo lavoro, le pagine dei quotidiani erano piene di notizie (spesso contraddittorie) sulle modalità di somministrazione e l'efficacia dei vaccini, sull'importanza del cosiddetto *Green pass* e sui rischi di violazioni della privacy, pare verificatesi in concreto, relative ai dati sensibili contenuti nel nostro fascicolo sanitario elettronico. Sempre negli stessi giorni il governo italiano ha ridefinito, ampliandolo, l'elenco dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica delineato nelle disposizioni di attuazione della Direttiva NIS[54] e ha emanato disposizioni urgenti per la creazione dell'Agenzia per la cybersicurezza nazionale.[55] Io stessa, in vista di un viaggio all'estero e non avendo ancora a disposizione il *Green pass*, che entrerà in vigore il prossimo 1° luglio, ho scaricato sul mio cellulare una serie di app, alle quali ho concesso molti privilegi che non sono solita concedere: pur senza arrivare al riconoscimento facciale, ho acconsentito all'invio di notifiche nonché alla comunicazione tra siti. Non mi posso certo definire una complottista paranoica, ma cerco di fare buon uso di tutte le informazioni in mio possesso. Opero sempre la critica delle fonti, so che prima dell'emanazione delle disposizioni sul

[54] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L1148&from=EN> (06021).

[55] Per ulteriori dettagli v. <https://www.governo.it/it/articolo/cyber-aggiornato-l-elenco-dei-soggetti-del-perimetro-di-sicurezza-cibernetica-nazionale e https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/sg> (06/21).

Green pass vi è stato un intenso e proficuo scambio tra il Ministro per l'innovazione tecnologica e la transizione digitale e il Garante per la protezione dei dati personali,[56] so di vivere in uno Stato democratico, dotato di garanzie e contrappesi. Ma sono anche una internazionalista che ha studiato a fondo le violazioni dei diritti umani che derivano direttamente o indirettamente dalle misure messe in atto per la lotta al terrorismo.[57] Auspicando che queste righe possano essere utili a un aumento di consapevolezza in chi legge, non posso che concludere con un plauso agli hacker dotati di etica[58] e a tutte le ONG che si battono per la tutela dei nostri diritti, nella certezza che le seconde sono le degne eredi dei primi.

[56] V. <https://innovazione.gov.it/notizie/comunicati-stampa/app-io-ok-dal-garante-privacy/> (06/21).

[57] Sia consentito, per ulteriori indicazioni bibliografiche, il rinvio ai volumi *La tutela dei diritti umani nella* lotta *e nella* guerra *al terrorismo* (a cura di P. Gargiulo e M.C. Vitucci), Editoriale scientifica, Napoli, 2009 e *Seguridad y derechos. Análisis de las amenazas, evaluación de las respuestas y valoración del impacto en los derechos fundamentales* (J.L. Gonzáles Cussac, F. Flores Giménez coordinadores), Tirant Lo Blanch, Valencia, 2018.

[58] Cfr. i protagonisti della serie *Mr. Robot* e dei film tratti dalla trilogia *Millennium* di Stieg Larsson.

DISPOSITIVO PANDEMICO E GOVERNAMENTALITÀ DIGITALE

Gianvito Brindisi - Paolo Vignola

1. Introduzione

L'attuale governo biopolitico della pandemia ha fatto un uso massiccio, a fini di sicurezza sanitaria, di tutta una serie di tecnologie digitali per il governo dei comportamenti, la cui origine non risale al contesto pandemico, ma la cui articolazione presenta l'inedita volontà di assorbire e metabolizzare in tutti i suoi aspetti un fenomeno globale come la pandemia per farlo esistere nelle e attraverso le piattaforme digitali[1]. Il livello di cattura, di estrazione e di riconfigurazione del reale è stato ritenuto tale da poter governare e frenare la pandemia con l'isolamento fisico e sociale dei corpi mediante la quarantena e la securizzazione algoritmica, e al tempo stesso permettere la continuità dei flussi di energia, materia, informazione, capitale.

Lo spazio giuridico-politico e sociale pandemico ha rappresentato in questo senso un laboratorio di sperimentazione di forme di governo digitale in cui il controllo sembra fondersi con un nuovo potere disciplinare: da un lato le tecnologie di induzione di comportamenti stanno trasformando la nostra psiche in uno spazio di conquista da parte dei nostri ectoplasmi digitali, dall'altro la tracciabilità e l'estrazione di dati da ogni nostro comportamento stanno disegnando un futuro in cui le nostre case diventeranno "le nostre scuole, i nostri studi medici, le nostre palestre e, su decisione dello stato, le nostre carceri"[2], insomma uno spazio eterotopico plurifunzionale. In altre parole, la soluzione informatica all'angoscia prodotta dal virus, e cavalcata dal capitalismo della sorveglianza, è stata un modo per trasformare il luogo dell'esposizione e della circolazione per eccellenza, ossia la rete, in un rifugio iperdomestico in cui, parallelamente alle soluzioni offerte dal digitale per non interrompere lavoro, informazione, istruzione e mercato, si sperimentano nuove forme di governo dei comportamenti.

Al di là delle strategie sanitarie macropolitiche e delle relative forme di socializzazione del virus, il governo digitale della pandemia non è infatti mai stato messo in discussione in quanto tale, ma solo rispetto alle sue possibili varianti,[3] che riflet-

---

[1] Sulla gestione biopolitica e le misure di risposta all'emergenza sanitaria, cfr. J.J. Sylvia, "The Biopolitics of Social Distancing", *Social Media + Society*, 2020, <https://journals.sagepub.com/doi/10.1177/2056305120947661> (06/21).

[2] N. Klein, "Screen New Deal", *Dinamo Press*, 21 maggio 2020, <https://www.dinamopress.it/news/screen-new-deal/> (05/21).

[3] Per un'analisi critica dell'implementazione dei dispositivi di sorveglianza e tracciamento nello spazio digitale pandemico e delle loro ripercussioni giuridiche e politiche, cfr. S. Pietropaoli, "La scia dell'untore: privacy, ICT e virus non informatici", *La fionda*, 10 apr. 2020, < https://www.lafionda.org/2020/04/10/la-scia-delluntore-privacy-ict-e-virus-non-informatici/> (05/21);

tono in fondo lo scontro tecnologico tra i giganti della Silicon Valley e la Cina. Quest'ultima ha rappresentato sin da subito l'avanguardia tecnologico-politica rispetto alla quale i primi, che ne hanno invidiato l'"infrastruttura normativa relativamente lassista" e il "suo appetito senza fondo per la sorveglianza"[4], rischiavano di perdere il loro vantaggio competitivo. Il già rodato sistema di credito sociale cinese, unito alla condivisione dei dati tra fornitori di servizi di telefonia mobile e ministeri degli interni e della salute, ha permesso un tracciamento e una valutazione senza precedenti di qualsiasi attività umana, tanto da portare Byung Chul Han a sostenere, facendo eco a Carl Schmitt, che la pandemia dovrebbe indurre a rivedere il concetto stesso di sovranità: "Sovrano è chi possiede i dati".[5] Definizione problematica, questa, a cui, per le ragioni che mostreremo, andrebbero preferite le altre, pure proposte da Han, di "biopolitica", "psicopolitica" o "stato di polizia"[6] digitali, nonostante una certa confusione, storica e concettuale, delle sue analisi.

Ad ogni modo, Han sostiene che il sistema cinese difficilmente potrebbe convivere con il liberalismo occidentale, benché riconosca che le piattaforme digitali come *Google* o *Facebook* hanno un accesso illimitato alla sfera privata e che la procedura di valutazione del credito sociale cinese si basa sugli stessi algoritmi di valutazione del credito come *FICO* negli Stati Uniti o *Schufa* in Germania.[7] Volendo sciogliere la problematicità di questa tesi, immaginiamo che quando parla di liberalismo Han faccia riferimento allo stato liberale e allo stato (costituzionale) di diritto e non alla governamentalità liberale, dotata invece massicciamente delle più varie procedure di controllo. Se il cosiddetto *platform capitalism* è già di per sé un sistema che (al di là dell'emergenza sanitaria e a fini di accumulazione finanziaria e di anticipazione degli scenari sociali e dei comportamenti) permette forme di controllo dei dati che conducono a violare sistematicamente la privacy, allora lo stato costituzionale liberale può conservare una pertinenza critica in rapporto alla codificazione autoritaria di matrice cinese dei meccanismi di controllo digitali. Non può dirsi lo stesso, però, rispetto al problema politico principale rappresentato a nostro avviso dalla biopolitica e dalla psicopolitica digitali, vale a dire il loro innescare meccanismi di potere direttamente funzionali alla modifica comportamentale attraverso software predatori. Il modello degli stati costituzionali occidentali convive infatti

---

S. Milan, E. Treré, S. Masiero (eds.), *COVID-19 from the Margins. Pandemic Invisibilities, Policies and Resistance in the Datafied Society*, Institute of Network Cultures, Amsterdam, 2021; L. Taylor, G. Sharma, A. Martin, Sh. Jameson (eds.), *Data Justice and COVID-19: Global Perspectives*, Meatspace Press, London, 2020; *Surveillance & Society*, 2021, Dialogue section on "Surveillance and the COVID-19 Pandemic" <https://ojs.library.queensu.ca/index.php/surveillance-and-society/issue/view/890> (05/21).

[4] N. Klein, "Screen New Deal", cit.

[5] B.-Ch. Han, "La emergencia viral y el mundo de mañana", *El Paìs*, 20 marzo 2020, <https://elpais.com/ideas/2020-03-21/la-emergencia-viral-y-el-mundo-de-manana-byung-chul-han-el-filosofo-surcoreano-que-piensa-desde-berlin.html> (05/21).

[6] *Ibid*.

[7] ID., "Il fattore X contro la pandemia è il senso civico", *Domani*, 31 ottobre 2020, <https://www.editorialedomani.it/idee/cultura/il-fattore-x-contro-la-pandemia-il-senso-civico-a45w7rf0> (05/21).

con l'estensione massiccia delle tecnologie di controllo tanto quanto lo stato legislativo del XIX secolo ha convissuto con le tecnologie disciplinari e di regolazione. D'altronde, se molti Stati occidentali hanno addirittura inteso promuovere all'inizio della pandemia un governo a distanza, volto a gestire i comportamenti attraverso tracciamenti, nudges e incitazioni comportamentali al fine di evitare ricadute sull'economia, queste tecnologie sono state implementate a dismisura ovunque nonostante i legittimi dubbi sull'efficacia nel contrasto alla diffusione del virus.

In queste pagine non sarà ovviamente possibile svolgere un'analisi storicamente dettagliata di un simile ordine di fenomeni, ma ci proponiamo di renderlo parzialmente intelligibile interrogando la genesi della condizione bioipermediale della pandemia[8] e delineando la simbiosi di due dinamiche caratterizzanti quello che potremmo definire il *dispositivo pandemico*, la cui articolazione governamentale è tuttora in via di definizione: il *data mining* o estrattivismo dei dati, e la captologia, nel senso delle tecnologie di persuasione e d'induzione comportamentale. Queste riattualizzano a nostro avviso il dispositivo di potere moderno e le relative funzioni di estrazione e cattura.

2. Il dispositivo tra sovranità, disciplina e controllo

Prima di arrivare a sostenere la nostra ipotesi, sono necessarie alcune precauzioni di ordine storico e metodologico intorno al dibattito degli ultimi trent'anni sui dispositivi di potere e sulle relative forme di società, che ha spesso sollevato il problema delle successioni storiche o delle discontinuità tra due dispositivi, piuttosto che analizzare le loro sovrapposizioni o le rifunzionalizzazioni dei loro meccanismi. Quest'ultima opzione ci sembra al contrario meglio suscettibile di restituirci in modo storicamente significativo tanto le linee di continuità tra due dispositivi quanto i caratteri inediti della razionalità politica in cui siamo.

Intorno alle nostre *società di controllo*, per come definite da Gilles Deleuze all'inizio degli anni Novanta, si è infatti generalmente considerato che esse avessero storicamente fatto seguito alle *società disciplinari* analizzate da Foucault e prodotto una desuetudine del relativo potere a favore di una nuova configurazione di potere avente un carattere preventivo e modulatore, basato sull'utilizzo sistematico e sistemico dell'informatica e in grado di articolare controllo continuo e circolazione istantanea dell'informazione e della comunicazione, tracciando ogni azione o flusso per prevedere probabilisticamente rischi e fenomeni. Non si trattava più, per Deleuze, di segmentare lo spazio e normalizzare gli individui come nelle società disciplinari, ma di fluidificare i ruoli e le soggettività, di trasformare i comportamenti, gli affetti e le relazioni che formano le trame dei processi di soggettivazione, indirizzandole e adattandole ai bisogni immediati del mercato o di uno Stato.[9] L'elemento

[8] G. Griziotti, *Neurocapitalismo. Mediazioni tecnologiche e linee di fuga*, Mimesis, Milano, 2016.

[9] G. Deleuze, "Poscritto sulle società di controllo", in Id., *Pourparler*, Quodlibet, Macerata, 2000, pp. 234-241.

problematico di questa diagnosi è però la tesi per la quale le società di controllo avrebbero sostituito senza resti quelle disciplinari succedendo loro storicamente, ciò che rende difficile dare conto dell'irriducibilità del potere disciplinare alle istituzioni chiuse e della rifunzionalizzazione delle tecnologie disciplinari in altri dispositivi di potere. Questo è in particolar modo il caso di Han, che volendo sottolineare la radicale discontinuità, per non dire l'assenza di qualsiasi relazione storica, tra lo psicopotere che caratterizza le attuali società di controllo e il potere disciplinare, non solo evita di analizzare i dispositivi di potere e le relative tecnologie nel loro lungo periodo, ma si costruisce una nozione di potere disciplinare "dominato dalla negatività"[10] (perché *vieta*, *impedisce*, *esclude*, *reprime*). Vale a dire esattamente l'opposto di quello che sosteneva Foucault in *Sorvegliare e punire*, dove si esaltava la dimensione produttiva del potere disciplinare, tanto dal punto di vista corporeo e psichico quanto dal punto di vista sociale.

Ora, un dispositivo è per Foucault un complesso eterogeneo di poteri e saperi che si articolano a partire da un imperativo strategico e in funzione di una serie di urgenze specifiche.[11] Il legame tra questi elementi eterogenei (ad es. misure e norme giuridiche e mediche, enunciati scientifici, invenzioni architettoniche o tecnologiche, etc.) delinea una forma altrettanto specifica di razionalità politica e produce una certa forma di soggettività. Foucault ha così spesso distinto un dispositivo legale, un dispositivo disciplinare e un dispositivo di sicurezza. Riducendo al minimo le distinzioni, il potere giuridico sovrano si esercita sul territorio, ha una funzione di prelievo e repressiva e si esprime nel linguaggio della legge o della regolamentazione; la disciplina si esercita sul corpo e l'anima degli individui, ha una funzione di prescrizione di normalità e si esprime nei saperi relativi al normale e al patologico; la sicurezza si esercita sulla popolazione nella sua natura dinamica come elemento fluttuante, ha una funzione gestionale e preventiva la cui forma privilegiata di sapere è l'economia politica. Ciò tuttavia non significa che i meccanismi dell'uno non sussistano nell'altro, che ad esempio la sicurezza non faccia uso di tecniche giuridiche e disciplinari. Il caso della gestione dello spazio epidemico e del controllo politico delle molteplicità umane è esemplare: l'esclusione dei lebbrosi nel Medioevo era determinata da leggi e regolamenti e da un apparato rituale di ordine religioso, ed era funzionale a effettuare una partizione binaria tra i malati e i sani. Nel caso della peste, invece, anche se regolamentata giuridicamente, si tratta di includere gli individui all'interno di uno spazio minuziosamente regolato, come nella quarantena, in cui si ha l'obbligo di restare in casa e si è sotto il controllo di un potere di sorveglianza e di ispezione continuo. Infine, nel caso del vaiolo, corrispondente alle tecnologie di sicurezza, sono ancora presenti tecniche giuridiche e disciplinari, ma il tentativo di bloccare un'epidemia è caratterizzato dall'immunizzazione della popo-

[10] B.-Ch. Han, *Psicopolitica. Il neoliberalismo e le nuove tecniche del potere*, Nottetempo, Milano, 2016, p. 24.

[11] M. Foucault, "Il gioco di Michel Foucault", in ID., *Follia e psichiatria. Detti e scritti 1957-1984*, a cura di M. Bertani e P.A. Rovatti, Cortina, Milano, 2005, p. 156. Per un uso della nozione in grado di coniugare efficacemente Deleuze e Foucault, cfr. O. Razac, *Avec Foucault Après Foucault. Disséquer la société de contrôle*, L'Harmattan, Paris, 2008.

lazione tramite l'inoculazione del virus e attraverso il calcolo statistico della mortalità, delle infezioni, etc.[12]

La ripartizione delle molteplicità umane nello spazio in funzione di un certo dispositivo non segna la scomparsa o la desuetudine degli altri meccanismi di potere, ma la loro rifunzionalizzazione, per cui bisogna comprendere i dispositivi come "edifici complessi in cui ciò che cambia, oltre alle stesse tecniche, destinate a perfezionarsi e a divenire sempre più complicate, è soprattutto la dominante o, più esattamente, il sistema di correlazione tra i meccanismi giuridico-legali, disciplinari e di sicurezza".[13] Benché non sia sempre possibile e forse neanche necessario individuare con esattezza una dominante, va rilevato che un dispositivo è sempre strategico, nella misura in cui le tecnologie hanno una lunga durata, essendo oggetto di spostamenti che conferiscono loro una portata ogni volta differente all'interno dei quadri e dei rapporti di forza in cui sono utilizzate.

Pertanto si potrà fare una storia di come le tecnologie di potere e i meccanismi giuridici e disciplinari vengono riconfigurati strategicamente in un quadro securitario o di controllo, senza assolutizzare nessuno di questi meccanismi, essendo le tecnologie funzionalmente fungibili, come proprio la pandemia in corso ci mostra. Ma prima di affrontare questo problema, ve n'è un altro di non poco conto da sollevare.

Molto si è scritto nel corso dell'ultimo anno sulla città appestata, per rendere intelligibili l'esercizio del potere durante la quarantena e l'uso degli strumenti di coercizione in funzione di uno stato d'eccezione. Molto si è scritto anche sul nostro muoverci all'interno della soglia di modernità biologica simboleggiata dalla nozione di biopolitica. Molto meno però si è scritto sull'automatismo del potere e sul rapporto tra disciplina e controllo al riguardo, probabilmente perché, identificando la sorveglianza disciplinare con la città appestata, si è avuto l'effetto di non comprendere il carattere di novità del panoptismo nel XIX secolo, oltre al fatto che anch'esso ha rappresentato una forma di controllo esercitantesi al di là delle istituzioni chiuse.

Fermo restando che le tecnologie disciplinari si incrociano storicamente con tecniche giuridiche, securitarie e di regolazione, se si legge attentamente *Sorvegliare e punire* si vedrà che il dispositivo disciplinare non è un tutto unitario, e che il panoptismo ha dei tratti che non sono affatto estranei a ciò che Deleuze definisce come controllo. Il modello della città appestata non coincide con il modello della sorveglianza del XIX secolo, simboleggiato dal panopticon, né con il panoptismo, inteso da un lato come forma di potere-sapere estesa in tutta la società, e dall'altro come carattere specifico di una governamentalità più complessa del semplice esercizio della sorveglianza.

La città appestata rappresentava la "messa in opera globale" delle discipline elaborate nelle istituzioni di età classica, ed era tutto sommato un modello disciplinare d'eccezione, perché aveva la funzione di "neutralizzare dei pericoli, di stabiliz-

[12] M. Foucault, *Sicurezza, territorio, popolazione. Corso al Collège de France 1977-1978*, a cura di M. Senellart, Feltrinelli, Milano, 2005, pp. 20-22.

[13] *Ibid* 19.

zare popolazioni inutili o agitate, di evitare gli inconvenienti di assembramenti troppo numerosi"[14], e valorizzava contro il pericolo del contagio la sovrana minaccia di morte, un potere dunque ingombrante e visibile. Si trattava di una *disciplina-blocco* avente una funzione prevalentemente negativa. Il panopticon, diversamente, ha il ruolo di amplificare e intensificare un potere anonimo che deve al tempo stesso accrescere le forze sociali e l'utilità degli individui al livello della produzione, dell'istruzione, dell'apparato bellico, della morale pubblica.[15] Per farlo, deve esercitarsi in modo continuativo, meccanico e infinitesimale sulla società, al di là delle forme legate all'esercizio della sovranità. Una *disciplina-meccanismo*, la definisce Foucault, certamente in continuità con l'estensione delle discipline nel corso del XVIII secolo, ma anche in discontinuità, perché il carattere principale della sorveglianza panoptica è che essa tende verso un esercizio incorporeo del potere.

Sinteticamente, il panopticon è uno strumento di governo funzionale all'assoggettamento delle volontà che si esercita sul corpo e sulla mente degli individui, nella misura in cui sono sede di abitudini. Si tratta di un potere istituzionalmente polivalente, per la sua capacità di integrarsi a una funzione qualunque (economica, produttiva, terapeutica, educativa) e di potenziarla. La differenza con le discipline di età classica risiede nel funzionamento meccanico e automatico del potere e nel fatto che l'efficacia di quest'ultimo si trasferisce sulla sua superficie di applicazione[16], nel senso che gli individui sottoposti a sorveglianza sono presi in una situazione di potere di cui diventano i portatori attivi.

Il panoptismo, invece, rappresenta una società caratterizzata dall'estensione massiccia delle tecnologie disciplinari, che sono un tipo di potere avente il fine di governare la molteplicità umana agendo positivamente sugli individui per far acquisire loro abitudini e trasformarli moralmente, costituendo soggettività economicamente utili che vengono fatte decrescere in quanto massa politica di contestazione. Se queste tecniche sono volte all'estrazione di forze e di tempo dai corpi per trasformare la vita in forza lavoro – per cui Foucault poteva affermare che l'abitudine è ciò attraverso cui gli individui sono legati all'apparato di produzione[17] –, lo stesso effetto può essere ottenuto anche al di fuori delle istituzioni chiuse e con procedure differenti dalla sorveglianza in senso stretto, come i libretti operai in funzione della contabilizzazione della vita dell'individuo, o le casse di risparmio, che individualizzano i risparmi e impediscono che siano versati in un fondo comune.

Ma in *Sorvegliare e punire* Foucault sostiene anche che al di là della moltiplicazione delle istituzioni disciplinari, i meccanismi che le caratterizzano tendono nel XIX secolo a disinternarsi e a disistituzionalizzarsi e a circolare allo stato libero nel corpo sociale per svolgere funzioni di controllo generalizzato, automatico e anonimo della popolazione sul versante penale, medico, educativo etc.[18] E ancora, che è

[14] ID., *Sorvegliare e punire. Nascita della prigione*, Einaudi, Torino, 1995, p. 229.
[15] *Ibid* 227.
[16] Cfr. *ibid* 221.
[17] ID., *La società punitiva. Corso al Collège de France 1972-1973*, a cura di B.E. Harcourt, Feltrinelli, Milano, 2016, p. 248.
[18] ID., *Sorvegliare e punire*, cit., p. 230.

come meccanismo di potere, e non come apparato, che va inteso il potere poliziesco, in quanto "sguardo senza volto che trasforma tutto il corpo sociale in un campo di percezione".[19]

Foucault riprende infine il problema del panopticon nel 1979, sostenendo che esso non rappresenta un meccanismo limitato a delle istituzioni, bensì la formula politica generale del governo liberale in rapporto alle sue funzioni di sorveglianza e di intervento sulla meccanica naturale dei comportamenti e della produzione.[20] In questo senso, come ha sostenuto Christian Laval, il panoptismo configura l'ipotesi di un controllo a distanza che consente di condurre le condotte strutturando il campo di azione degli altri attraverso tutti i modi di influenzare le rappresentazioni che determinano il calcolo d'interesse, ciò che presuppone di conoscere gli individui, i loro interessi, i motivi che presiedono ai comportamenti per orientarli verso l'interesse generale.[21]

3. Il dispositivo pandemico e la captologia

Ora, assumendo la nozione di dispositivo come una rete di elementi discorsivi e non discorsivi che si articolano in un certo momento storico e in funzione strategica per rispondere a un'urgenza, si tratta innanzitutto di capire qual è l'urgenza cui l'articolazione di questi elementi nella pandemia ha inteso rispondere. Il *dispositivo pandemico* è un insieme tecnologico-politico che ha articolato diverse tecniche (legali, mediche, securitarie, digitali, statistiche, etc.) per rispondere all'urgenza dell'imperativo contraddittorio del contenimento del contagio e del mantenimento della produzione e della competitività tecnologica, occasione per intrecciare un legame tra attori governamentali differenti che intendono altresì strategicamente evitare la messa in discussione dei meccanismi di produzione attraverso la responsabilizzazione individuale e al tempo stesso accelerare la digitalizzazione dell'esistenza.[22]

L'intreccio tecnologico-politico che caratterizza il governo della pandemia conferma che la società di controllo non rende obsolete le tecniche giuridiche e disciplinari, ma le sovrappone e le estende facendole funzionare in tutto lo spessore della società. Il governo dello spazio di movimento degli individui e delle popolazioni ha infatti realizzato una inedita articolazione delle tre modalità di gestione dello spazio

[19] *Ibid* 233.

[20] ID., *Nascita della biopolitica. Corso al Collège de France 1978-1979*, a cura di M. Senellart, Feltrinelli, Milano, 2005, p. 69.

[21] Ch. Laval, "Ce que Foucault a appris de Bentham", *Revue d'études benthamiennes*, 2011, <https://journals.openedition.org/etudes-benthamiennes/259> (05/21).

[22] Cfr. Sul punto A. Rouvroy, "COVID-19: Antoinette Rouvroy: "Le capitalisme numérique colonise tous les lieux que nous dés-habitons", *Etopia, revue d'écologie politique*, 2020, <https://etopia.be/wp-content/uploads/2020/06/REVUE15_Le_Virus_du_Changement_WEB.pdf> (06/21); V. Dubal, "The expansion of mass surveillance to stop coronavirus should worry us all", *The Guardian*, 18 apr. 2020, <https://www.theguardian.com/commentisfree/2020/apr/18/mass-surveillance-coronavirus-technology-expansion> (06/21).

e delle molteplicità umane sopra richiamate: esclusione da determinati luoghi (modello della lebbra), inclusione/reclusione in casa (modello della città appestata), controllo degli spostamenti sulla base del calcolo statistico dei rischi (modello del vaiolo), con una netta prevalenza degli ultimi due. Ha rifunzionalizzato in tal senso l'esercizio del potere sovrano e di quello disciplinare a fini di controllo e sicurezza sanitaria.

Tuttavia, ci sembra che una delle funzioni caratterizzanti la nuova configurazione strategica non sia stata semplicemente il controllo, quanto piuttosto una sorta di iper-controllo, ossia un controllo automatizzato che riattiva un governo disciplinare degli individui e delle popolazioni tramite estrazione, cattura e induzione comportamentale nell'intero spazio digitale. E che pertanto la discontinuità dell'iper-controllo rispetto al panoptismo sia molto relativa, perché le sue funzioni di condizionamento e produzione di abitudini permangono intatte. Peraltro, in tempi non sospetti Jonathan Crary, prendendo posizione nel dibattito tra Foucault (società di sorveglianza) e Debord (società dello spettacolo), ha mostrato come i dispositivi ottici elaborati nel XIX secolo fossero, come il panopticon, "techniques for the management of attention"[23] finalizzate a imporre l'omogeneità, isolare gli individui e ridurne la forza politica.

Tra i tanti esempi che sarebbe possibile fare intorno alla strategia digitale di gestione della pandemia, ne segnaliamo alcuni che ci sembrano piuttosto significativi di quest'ordine di fenomeni, in quanto mostrano come l'emergenza sanitaria sia stata colta quale occasione imperdibile per una comprensione pragmatica dei fattori di trasformazione del comportamento che è possibile replicare in laboratorio.

L'Accademia Scientifica Nazionale degli Stati Uniti (*National Academies of Sciences, Engineering, and Medicine*) ha elaborato una serie di strategie di cambiamento comportamentale rivolte ai governi, al fine di produrre nuove abitudini sanitarie in funzione della protezione della salute (ad es. rendere i comportamenti facili da svolgere e gratificanti, agganciarli alle abitudini esistenti, etc.), nonché una strategia di comunicazione del rischio che sostiene esplicitamente che l'enunciazione della verità del Covid-19 non è sufficiente a produrre un cambiamento comportamentale, ragion per cui bisogna modulare persuasivamente il messaggio in funzione dei target specifici di popolazione.[24] Lo stesso approccio è stato considerato in funzione della vaccinazione, e tra i vari esperimenti al riguardo[25],

---

[23] J. Crary, *Techniques of the Observer. On Vision and Modernity in the Nineteenth Century*, MIT Press, Cambridge, 1990, p. 18.

[24] D. Brossard et al., *Encouraging Adoption of Protective Behaviors to Mitigate the Spread of COVID-19: Strategies for Behavior Change*, The National Academies Press, 2020, <https://www.nap.edu/catalog/25881/encouraging-adoption-of-protective-behaviors-to-mitigate-the-spread-of-covid-19#> (05/21).

[25] Cfr. W.-Y. Sylvia Chou et al., *COVID-19 Vaccination Communication: Applying Behavioral and Social Science to Address Vaccine Hesitancy and Foster Vaccine Confidence*, National Institutes of Health, 2020; Ch.J. Bechler, Z.L. Tormala, "Misdirecting Persuasive Efforts during the COVID-19 Pandemic: The Targets People Choose May Not Be the Most Likely to Change", *Journal of the Association for Consumer Research*, January 2021, pp. 187-195.

quello del *Behavior Design Lab* dell'Università di Stanford[26] ci sembra piuttosto significativo, non solo perché si propone esplicitamente di raccogliere la sfida della vaccinazione a livello globale, agendo sui "psychological factors for vaccine acceptance and hesitancy", ma anche perché è stato ideato da uno degli psicologi che più hanno influenzato la progettazione di software per il cambiamento comportamentale, ossia Brian Jeffrey Fogg.

Fogg ha coniato nei primi anni Duemila la nozione di captologia,[27] indicando con essa la progettazione di strumenti informatici persuasivi mirati all'automatizzazione del cambiamento comportamentale, che hanno peraltro trovato un'immediata applicazione nell'ambito della protezione sanitaria.[28] Per Fogg non c'è alcun dubbio che "*applying computing technology to observe others' behavior increases the likelihood of achieving a desired outcome*",[29] ma nella sua autocomprensione la sorveglianza non solo è concepita come un fattore tra gli altri per modificare il comportamento, bensì anche come una tecnologia debole in relazione alla produzione di abitudini[30], perché non incide efficacemente sulle motivazioni intrinseche ed estrinseche dei comportamenti. Sostiene così che "if a suggestion technology can produce the desired behavior, that approach should be used rather than surveillance technology".[31]

Com'è stata giustamente definita da Nick Seaver, che la iscrive nell'antropologia della cattura, la captologia non è altro che un sistema di trappole per l'attenzione, in cui i confini tra persuasione e coercizione sono piuttosto sfumati. Si tratta di un paradigma comportamentista che trova uno dei suoi fondamenti teorici nel comportamentismo skinneriano e che ha segnato una svolta recente nella progettazione dei software, nella misura in cui incita le aziende che vogliono acquisire utenti a inculcare loro delle abitudini attraverso un insieme di misure che Seaver definisce "*captivation metrics*".[32]

Shoshana Zuboff ha dunque perfettamente ragione nel sostenere che il mercato dei comportamenti del capitalismo della sorveglianza può finalmente "imporre la tecnologia del comportamento di Skinner nei vari ambiti della vita quotidiana, fino al nostro intimo". Tuttavia sbaglia quando sostiene che "prima dell'ascesa del capitalismo della sorveglianza, l'idea di un potere strumentalizzante era solo un sogno

---

[26] *Behavior Design Lab. Models and Methods For Behavior Change*, <https://behaviordesign.stanford.edu/vaccination> (05/21).

[27] Cfr. B.J. Fogg, *Persuasive Technology: Using Computers to Change What We Think and Do*, Morgan Kaufmann, San Francisco, 2003.

[28] Cfr. O.E. Pinzon, M.S. Iyengar, "Persuasive Technology and Mobile Health: A Systematic Review", *Linköping Electronic Conference Proceedings*, issue 68, 2012, pp. 45-48; A.S. Chan, "Health captology - application of persuasive technologies to health care", *Studies in Health Technology and Informatics*, 2004, pp. 83-91.

[29] B.J. Fogg, *Persuasive Technology*, cit., p. 256.

[30] *Ibid* 46-48.

[31] *Ibid* 53-54.

[32] N. Seaver, "Captivating algorithms: Recommender systems as traps", *Journal of Material Culture*, 2019, pp. 1-16.

confuso, un'illusione".[33] Non si trattava infatti di un sogno confuso, ma di un'utopia concreta. È vero che in questo dispositivo pandemico l'estrazione di dati e la cattura dei comportamenti tramite condizionamento avvengono non solo con un occhio digitale, ma mediante un'elaborazione algoritmica, ma le funzioni di sorveglianza, estrazione e cattura non sono così lontane dal panoptismo. Pure tralasciando la moltiplicazione inaudita della videosorveglianza su scala globale nel corso della pandemia, possiamo dunque dire che le nostre non sono delle società di mero controllo smaterializzato, ma delle società di controllo che articolano tecnologie a carattere giuridico, disciplinare e securitario, dove la funzione dominante resta certamente la sicurezza, caratterizzata però da un iper-controllo che, strutturando l'ambiente digitale, riattualizza con nuove tecniche una funzione panoptica. Realizzando in tal modo uno psicopotere che fa della psiche lo spazio di conquista da parte della psicologia comportamentale. Tale psicopotere effettua infatti un'azione selettiva sugli affetti, le passioni, le preferenze, etc., che è a un tempo individualizzante e totalizzante, esercitandosi sugli individui e sui target di popolazione, e producendo una forma di soggettività che si è data artificialmente e preliminarmente in laboratorio, facendo coincidere gli individui con il loro ectoplasma digitale.

4. Il nostro passato e futuro prossimi: l'iper-controllo

Veniamo dunque ad approfondire gli aspetti più significativi di questo iper-controllo come nuova forma di gestione politica degli individui e delle popolazioni, a confrontarla con le recenti ipotesi di aggiornamento della società di controllo e a definire infine la nostra ipotesi, ossia che i confinamenti, i tracciamenti digitali e il distanziamento sociale, accompagnati dalla migrazione alle modalità on line di buona parte della vita quotidiana, stiano contribuendo alla realizzazione di un disciplinamento massivo, ai fini di ciò che potremmo definire un'immunizzazione algoritmica. L'effetto più evidente di questa immunizzazione affidata a calcoli, statistiche, tracciamenti e correlazioni per ridurre il pericolo da contagio fisiologico, pare darsi in quelle sfere dell'ecologia che Guattari ha definito sociale e mentale,[34] ossia non solo a livello delle istituzioni sociali ma nelle relazioni interpersonali a 360 gradi, nonché sul piano fisiopsicologico degli individui, ai quali vengono forniti sempre più stimoli e strumenti di autoestrattivismo di dati, percezioni ed emozioni. Reindirizzando molte attività alla modalità online, nel caso dei consumi (smart shopping e smart entertainment) come nel caso della produzione (smart working), ci troviamo costantemente connessi a schermi, dispositivi e piattaforme che non solo ci monitorano ed estraggono dati dalle nostre attività, ma definiscono anche le condizioni di possibilità dell'esperienza mediatizzata. Strumenti che, mediante il calcolo intensivo su tali dati e la capacità di catturare attenzione e tempo mentale dispo-

[33] Sh. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, LUISS University Press, Roma, 2019, pp. 452-453.

[34] Cfr. F. Guattari, *Le tre ecologie*, Sonda, Casale Monferrato, 2013.

nibile, producono profili calcolabili e prevedibili, come sostengono Antoinette Rouvroy e Thomas Berns nella loro teoria della governamentalità algoritmica[35], che da un punto di vista filosofico politico viene ad aggiornare il concetto deleuziano di società di controllo e quello foucaultiano di governamentalità.

Con "governamentalità algoritmica" Rouvroy e Berns intendono un modo di governo alimentato da basi di dati grezzi e metadati i cui flussi attraversano ogni aspetto della vita umana, che opera attraverso correlazioni e procedure, e si indirizza ai cittadini attraverso i loro profili digitali, ossia modelli comportamentali prodotti su base unicamente induttiva. Se l'obiettivo è anticipare, prevedere e prevenire le relazioni sociali e i comportamenti individuali, questa operazione di modulazione automatica e a priori del comportamento mira a «separare i soggetti dalla loro abilità di fare o non fare certe cose», secondo «il modo condizionale della formula "cosa *potrebbe* un corpo", laddove questo modo condizionale è definitorio della *facoltà* come tale»[36]. Queste ultime parole di Rouvroy trovano oggi, nella condizione pandemica, una concretizzazione decisamente calzante. L'espressione "Cosa potrebbe un corpo", estrapolata dal piano etico politico, nella governamentalità algoritmica descrive una serie di operazioni probabilistiche e correlazioniste, fatte su e a riguardo dei corpi individuali e collettivi, che con il biennio pandemico hanno occupato sempre più spazio nella vita di chiunque a livello globale.

Dal punto di vista cibernetico, se il controllo dipende dall'estrazione e veicolazione delle informazioni, l'incremento della circolazione dei flussi informativi e comunicativi all'interno di un sistema aumenterà necessariamente la capacità, il volume e la precisione del controllo che vi si potrà esercitare. Questo aspetto è centrale per comprendere il concetto di governamentalità algoritmica in quanto frutto della necessità di evidenziare una tappa successiva ma anche in totale continuità con le società di controllo deleuziane. Con la governamentalità algoritmica infatti, il controllo, per dirla con Stiegler, diviene iper-controllo, nel senso di un controllo che si esercita «alla velocità della luce», totalmente automatizzato, nutrito dai dati personali auto-prodotti, auto-captati e autopubblicati dagli utenti in funzione del calcolo anticipatorio dei comportamenti.[37]

Tuttavia, la fase attuale, e in relazione alle misure di tracciamento, datificazione e proiezione dell'andamento pandemico, sembra contraddistinguersi anche per un significato ulteriore di iper-controllo, cui sopra abbiamo fatto riferimento, come produzione di una nuova forma di sorveglianza disciplinare, che opera nello (cyber)spazio della governamentalità algoritmica senza però limitarsi al controllo per così dire impassibile o ineffabile, ma inducendo comportamenti, posture ideologiche, desideri, agendo sul piano che Deleuze e Guattari definiscono micropolitico, nel senso che concerne i flussi materiali e semiotici che attraversano – e costitui-

[35] Cfr. T. Berns e A. Rouvroy, "Gouvernementalité algorithmique et perspectives d'émancipation", *Réseaux*, 2012, pp. 163-196.

[36] A. Rouvroy, "The end(s) of critique: data-behaviourism vs. due-process", in M. Hildebrandt, & E. De Vries (eds.), *Privacy, Due Process and the Computational Turn. Philosophers of Law Meet Philosophers of Technology,* London, Routledge, 2013, p. 152.

[37] Cfr. B. Stiegler, *La società automatica I. L'avvenire del lavoro*, Meltemi, Milano, 2019, p. 76.

scono – i soggetti in un campo sociale e strutturano gli enunciati (macro)politici, sociali e sanitari.[38] Si tratta perciò di una dimensione letteralmente molecolare, quella nella quale opera l'iper-controllo, dal momento che tali enunciati e comportamenti in forma di dati si cristallizzeranno algoritmicamente in segmenti identitari che rappresentano l'intero campo sociale sull'altro piano, quello macropolitico delle istituzioni, dei partiti e delle rappresentazioni sociali. Se il controllo cibernetico prefigurato da Deleuze avrebbe dovuto limitarsi appunto a controllare la dimensione micropolitica modulandola, l'iper-controllo del dispositivo pandemico giunge a modellarla tout court. Il controllo è perciò molecolarizzato in una microgestione ingerente e plastica, che forma stampi disciplinari e segmenti identitari che si sommano a quelli delle grandi divisioni binarie (classe, sesso, etnia, ecc.), promuovendo l'insicurezza, la precarietà, il panico del contagio, così come la paranoia complottista, i negazionismi e le arcaicità di ogni genere. L'iper-controllo che si attua con la piattaformizzazione della vita nella pandemia rappresenta quindi la forma ottimale di gestione micropolitica non solo dell'emergenza sanitaria ma di tutti i suoi effetti secondari in ambito sociale: "una macropolitica della sicurezza a favore e per mezzo di una micropolitica dell'insicurezza",[39] ovvero l'organizzazione di una sicurezza molare fondata su una produzione e somministrazione costante di piccole insicurezze molecolari.

È sullo sfondo di queste miriadi di piccole insicurezze programmate e oggi precalcolate e anticipate, che secondo Paul B. Preciado si verifica il precipitare della biopolitica delle popolazioni sul corpo individuale, sull'anatomopolitica. Più in particolare, quando Preciado afferma "il nuovo confine necropolitico è passato dalla costa della Grecia alla porta della casa privata. […] La nuova frontiera è la tua pelle. La nuova Lampedusa è la tua pelle"[40] mostra il dispositivo pandemico in atto a livello micropolitico, per cui i corpi diventano sempre più i luoghi di riproduzione delle macropolitiche di confine già applicate a migranti e rifugiati. Ciò poiché le misure di distanziamento, isolamento, ma anche di evidenziazione dei sintomi e di delazione, adottate in risposta alla pandemia, esasperano una logica discriminatoria nei confronti dell'altro (come straniero, diverso, anomalo, sconosciuto) tendenzialmente già in atto e comunque sempre sotto traccia, spingendo a interiorizzarla, cioè ad assumere su di sé il pericolo dell'invasione, in questo caso rappresentata dal possibile contagio. È la stessa logica di segmentazione identitaria che, su un'altra scala, ha portato a forme di polarizzazione sistematica dell'ordine del discorso, basate cioè su di una logica dualistica atavica, che tende a costituire rigide cornici oppositive entro le quali ricomprendere gli enunciati pubblici sul virus e sulla sua gestione

[38] Cfr. G. Deleuze, F. Guattari, *Mille piani. Capitalismo e schizofrenia II*, Orthotes, Napoli-Salerno, 2017, pp. 299-330. Un'interessante lettura micropolitica della gestione della pandemia è offerta da L. S. Rossi, "Pandemia y plataformas: capitalismo, controlatorios y coronavirus", *Reflexiones Marginales*, numero especial 8, 2020: <https://revista.reflexionesmarginales.com/pandemia-y-plataformas-capitalismo-controlatorios-y-coronavirus/> (06/21).

[39] G. Deleuze, F. Guattari, *Mille piani*, cit., p. 309.

[40] P. B. Preciado, "Aprendiendo del virus", in *Sopa de Wuhan*, editoriale ASPO, 2020, p. 175.

sanitaria, sociale, economica e politica.[41] Potremmo così giungere ad affermare che le menti dell'iper-controllo pandemico sono indotte ad adagiarsi all'interno di tali cornici captologiche, lasciandovisi modellare.

Possiamo concludere questa digressione sulle differenze di grado e di natura tra il controllo e l'iper-controllo, affermando che quest'ultimo è iper non solo perché dipende dall'algoritmizzazione, dall'automazione generalizzata e dai sistemi di geolocalizzazione, bensì anche perché aggiunge una dimensione in più al concetto di controllo deleuziano, ossia una sorta di disciplina dell'immunizzazione con tendenze totalizzanti. Si tratterebbe di una totalizzazione soft, ma micropolitica e onnipervasiva, nel senso di una mobilitazione totale richiesta agli individui per contrastare il virus, dunque un'induzione al cambiamento dei comportamenti in funzione dell'immunizzazione, che fa di ogni persona un soldato, dalla sentinella ai colonnelli e i generali, passando per tutti coloro che stanno in "prima linea". Un soldato potenzialmente incarnato da ciascuno di noi – proprio come per Foucault c'era qualcosa dell'incarnazione dell'imprenditorialità da parte degli individui – attraverso una nuova forma di sorveglianza disciplinare.

Detto altrimenti, e riprendendo gli argomenti sviluppati nel paragrafo precedente, piuttosto che al controllo in purezza, sembriamo essere di fronte a una forma spuria, un ibrido di controllo e sorveglianza disciplinare, nella misura in cui, attraverso l'insieme di interazioni quotidiane con i dispositivi di informazione e comunicazione, vengono introdotte o favorite segmentazioni e norme ad hoc di comportamento di fronte non solo e non tanto al virus in quanto tale, bensì agli elementi che ne compongono il contesto: istituzioni, professioni, associazioni, saperi, attori sociali, ecc. Questa spinta alla segmentazione, con la conseguente polarizzazione delle posizioni, appare sin dalla radice dell'informazione, rimbalza per ogni angolo delle reti sociali, fino ad essere riflessa da ogni sguardo, e fa sì che si irrigidiscano ancor più i segmenti e le polarizzazioni. Sebbene non rientri direttamente nella nostra analisi, occorrerebbe riflettere anche su quanto tutto ciò sia cinicamente l'effetto collaterale della logica mercantile alla base del *platform capitalism*, come testimoniano tanto gli scandali di vendita di pacchetti immensi di dati micropolitici da parte dei grandi colossi del web (di cui Cambridge Analitica è la metonimia) per scopi macropolitici, quanto gli studi di marketing e neuromarketing volti a catturare il plusvalore che emerge dal rapporto tra le architetture della profilazione algoritmica e le azioni, emozioni e relazioni degli utenti.

Per questo crediamo che la captologia assuma un ruolo importante proprio nel passaggio dal controllo all'iper-controllo del dispositivo pandemico. Il concetto e le pratiche della captologia, in cui la cattura dell'attenzione mediante trappole algoritmiche è già finalizzata alla modificazione dei comportamenti e delle decisioni[42], mostrano infatti con sufficiente chiarezza l'intreccio di sorveglianza e controllo che innerva l'iper-controllo della governamentalità algoritmica in epoca pandemica. In quest'ottica, si può giungere a sostenere che l'obiettivo della disciplina digitale non

[41] Cfr. S. Baranzoni, P. Vignola, "Etats d'exception micropolitiques", *Lignes*, n. 65, 2021.
[42] Cfr. N. Seaver, "Captivating algorithms", cit.

sia più quello di fabbricare "corpi docili" per la produzione, come nel caso delle società disciplinari. Il lavoro algoritmico delle varie captologie, tanto pubbliche e sanitarie quanto private e commerciali, sembra semmai puntare a modellare "menti docili", ossia non critiche, non solidali, bensì asociali, paurose, calcolabili, prevedibili, nonché predisposte a incardinarsi nei segmenti identitari e nelle polarizzazioni discorsive. Queste sono quindi le menti che le società di iper-controllo mirano a catturare e disciplinare, trovando nella transizione alla modalità smart un terreno assolutamente idoneo per poter concretizzare l'immunizzazione algoritmica della pandemia: prendere le distanze dagli altri corpi, dai luoghi della condivisione fisica, ma anche separarsi dai propri desideri – da quello che *avrebbe potuto fare* il proprio corpo – e dalla *vita activa* del pensiero critico, verso un'esistenza monadologica legata all'intelligenza digitale (smart working, smart city, e-learning, ecc.). È così che sulle basi di forme di governamentalità sempre più automatizzate, capaci di anticipare e prevenire, si sviluppano e si esercitano forme di biopotere e psicopotere disciplinari, ingerenti nella modificazione dei comportamenti individuali e sociali.

5. Conclusioni

Nel sostenere che l'iper-controllo è una forma di psicopotere che riattiva l'utopia panoptica, possiamo concordare con Han nel ritenere che le forme contemporanee di potere sono prevalentemente psichiche e legate alla sfera della produzione immateriale. Ne rigettiamo tuttavia la tesi relativa alla loro radicale discontinuità con il dispositivo moderno, perché questa non solo manca di riconoscere i caratteri di novità dello psicopotere, per come messi in luce ad esempio da Stiegler in relazione all'economia dell'attenzione,[43] ma anche le sue continuità tecnologiche sul piano storico in relazione alla produzione di abitudini. Al contrario di Han, riteniamo che il panopticon sia già concepito come un potere della mente sulla mente, che il panoptismo non sia vincolato al medium ottico, che il potere disciplinare abbia a che fare con la produzione di soggettività e con l'estensione sociale dei saperi psicologici, e che la specificità dello psicopotere non risiede nel suo accesso ai "pensieri o bisogni intimi" degli individui[44]. Il problema non è infatti quello di un potere che ha accesso alla sfera dell'intimità e dell'affettività, come se queste fossero indipendenti dallo stesso esercizio del potere, ma è esattamente un potere che si esercita producendo soggettività.

Se riteniamo di poter sostenere che lo psicopotere contemporaneo è in un rapporto di continuità e discontinuità con il potere disciplinare, è perché valorizziamo la produzione di psichicità legata alla funzione disciplinare. La normatività prodotta dallo psicopotere attraverso l'elaborazione algoritmica dei dati, la predizione e l'influenza del comportamento si fonda infatti su tutta un'arte del condizionamento

[43] Cfr. B. Stiegler, *Prendersi cura. Della gioventù e delle generazioni*, a cura di P. Vignola, Orthotes, Salerno-Napoli, 2014, pp. 209-234.

[44] B.-Ch. Han, *Psicopolitica*, cit., p. 30.

ambientale e della caccia psichica che non è solo una semplice *tecnica di acquisizione di dati*, ma di *produzione di abitudini*. È vero che la governamentalità digitale è modellata sulle nostre classificazioni quotidiane (consapevoli e inconsce), ma queste si muovono in un ambiente costruito per persuaderle ad agire in un certo modo, progettato su un modello elementare di soggettività che viene dato come presupposto ma che è in realtà prodotto.

Modellando le nostre percezioni e la nostra affettività, questi meccanismi di potere producono una soggettività che ha bisogno a sua volta del dispositivo che la produce. Il governo algoritmico della pandemia genera un investimento psichico nel dispositivo digitale come dispositivo salvavita e protettore dall'angoscia che riproduce a sua volta la necessità materiale del governo che lo ha generato.

Nel contesto pandemico in cui stiamo vivendo ciò significa, tra le altre cose, sfruttare la nobiltà del sentimento di responsabilità per l'altro in una direzione utile a non porre la questione della responsabilità dei poteri dominanti nei confronti dell'origine della pandemia e delle sue modalità di gestione.

LA PREVENZIONE DEL CRIMINE ALLE FRONTIERE 2.0, UNA QUESTIONE DI DATI BIOMETRICI

Federica De Simone

1. Le nuove modalità di controllo

"*Nothing to declare? This is your passport, thank you and have a nice trip!*". Queste le frasi di rito al passaggio delle frontiere europee sino a qualche tempo fa cui corrispondeva un timbro sul passaporto, segno formale del travalicamento dei confini, esibito con orgoglio da ogni viaggiatore che si sentiva cittadino del mondo.

Sono passati poco più di 35 anni dagli Accordi di Schengen, ossia da quando il controllo delle frontiere dei paesi europei ha assunto una rilevanza sovranazionale, ma forse all'epoca le evidenti esigenze di mobilità delle persone e delle merci non erano traducibili nei numeri odierni. I dati, infatti, mostrano che ogni anno gli spostamenti alle frontiere interne sono quasi 50 milioni, mentre i passaggi alle frontiere esterne poco più di 200 milioni,[1] ma si calcola che entro il 2025 saranno 887 milioni le persone che visiteranno lo spazio Schengen.

I numeri sono considerevoli, ancor più rilevanti se incrociati con i dati relativi all'incremento della criminalità nell'area Schengen e che alcuni mettono in correlazione proprio con l'abolizione dei controlli interni.[2] Non solo immigrazione clandestina e terrorismo tra i delitti immediatamente contrastabili alle frontiere, ma anche altre ipotesi delittuose eterogenee che includono alcuni reati contro il patrimonio (in particolare, truffa, contraffazione, riciclaggio e ricettazione), contro la persona (tratta di persone) o la pubblica amministrazione (per lo più corruzione), oltre al traffico di sostanze stupefacenti o armi, solo per citarne alcuni.

Inevitabile, dunque, la ricerca di nuove modalità di controllo più efficaci e capaci di coniugare il difficile binomio sicurezza/fluidità, che ha portato nell'ultimo decennio all'implementazione delle tecnologie più moderne tra gli strumenti impiegati nel controllo delle frontiere. Nello specifico, il riferimento riguarda l'introduzione del sistema *Intelligent portable border control system*

---

[1] Cfr. <*https://www.europarl.europa.eu/doceo/document/TA-8-2017-0411_IT.pdf*>. Si prevede che nel 2025 il numero totale degli attraversamenti di frontiera regolari salga a 887 milioni, di cui circa un terzo sarebbe effettuato da cittadini di paesi terzi che si recano nei paesi Schengen per visite di breve durata. Sui flussi migratori negli spazi navigabili si veda M. Mastroianni, F. Schettino, *Human Security: Risk Indicators in Navigable Space*, in questo Volume.

[2] F. Longo, *Identità, sicurezza, frontiere. I paradigmi della lotta alla criminalità organizzata nell'Unione Europea*, Meridiana, 2002, p. 43.

meglio noto come *IBorderCtrl*,[3] che associa l'analisi di una grande quantità di dati (*big data, open data, personal data*) dei passeggeri in transito con uno strumento di intelligenza artificiale (IA) addestrato al riconoscimento facciale e che costituisce un punto di approdo rispetto a politiche già avviate dall'Unione europea in tema di controllo delle frontiere esterne.

Con l'abolizione delle frontiere interne si è reso ben presto evidente che la sicurezza dello spazio Schengen potesse essere garantita solo con il rafforzamento dei controlli alle frontiere esterne e che non fosse sufficiente investire del problema i paesi frontalieri. L'adozione di normative nazionali, infatti, ha spesso determinato difformità operative[4] tali da rendere necessaria nel 2004 l'istituzione dell'Agenzia *Frontex*[5] con compiti di armonizzazione delle pratiche di controllo e di coordinamento operativo. Tuttavia, un significativo cambio di passo nelle politiche europee in materia si è avuto nel 2016, con l'attribuzione alla stessa Agenzia di poteri co-decisionali nella gestione dei flussi migratori e con l'adozione della Direttiva 2016/681/UE relativa all'istituzione del codice di prenotazione[6]. Contestualmente, l'adozione di strumenti tra cui *Schengen Information System*, *Visa Information System* ed *Entry/Exit System*,[7] hanno posto l'accento sull'importanza del ruolo rivestito dalla raccolta dei dati dei visitatori nel controllo delle frontiere e al contempo nel contrasto del crimine. Nessuno di questi sistemi sin ora citati si era spinto oltre la raccolta e l'incrocio dei dati, seppure automatizzati grazie alle più recenti tecnologie, mentre *IBorderCtrl* mostra tutta la sua innovatività dal momento che associa l'uso dei dati con la disciplina dell'IA, sfruttandone le prestazioni e le potenzialità.

Quella della intelligenza artificiale è una disciplina relativamente nuova,[8] che alle difficoltà di definizione e di delimitazione dell'ambito di operatività[9] aggiunge non poche criticità quando la si coniuga con le categorie giuridiche. L'impiego di tali sistemi, infatti, si pone spesso in contrasto con il più generale

---

[3] V. <*www.iborderctrl.eu*>.

[4] V. Gasparini, G. Casari (eds.), *Il diritto dell'immigrazione. Profili di Diritto Italiano, Comunitario e Internazionale,* V quaderno de «Il diritto dell'economia», I, 2010, p. 65.

[5] Regolamento (CE) n. 2007/2004 del Consiglio del 26 ottobre 2004. V. <*https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2004R2007:20070820:IT:PDF*>. L'Agenzia è divenuta operativa il 3 ottobre 2005. Per approfondimenti sull'Agenzia Frontex si veda F. Vassallo Paleologo, *La finzione della zona* SAR *"libica": quale giurisdizione sulle acque internazionali?*, in questo Volume.

[6] Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio del 27 aprile 2016 *sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi*, in <*https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L0681&from=IT*>.

[7] <*https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders_en; https://www.europarl.europa.eu/factsheets/it/sheet/153/gestione-delle-frontiere-esterne*>.

[8] G. F. Italiano, "Intelligenza artificiale: passato, presente, futuro", in F. Pizzetti (eds.)*, Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018, p. 206 ss.

[9] G. Ubertis, "Intelligenza artificiale, giustizia penale, controllo umano significativo", *Sist. Pen*., 2020, p. 2; M. Ienca, *Intelligenza. Per un'unione di intelligenza naturale e artificiale*, Rosenberg & Sellier, Torino, 2019, p. 13.

tema della tutela dei diritti fondamentali e con i principi propri della scienza penalistica. Le ragioni di un interesse penalistico per le nuove tecnologie risiedono soprattutto nell'esigenza di ricondurre a razionalità il sistema rispetto ai differenti ruoli che l'IA può rivestire e che possono tradursi in benefici per la collettività ma – al contempo – anche in pregiudizi per i beni giuridici.

Quattro le categorie in cui è possibile riscontrare attività di *law enforcement* in capo all'IA: previsione e analisi, riconoscimento, esplorazione, comunicazione. In particolare, poi, i nuovi apparati possono assumere il ruolo ora di autori ora di vittime di reato, ovvero possono essere impiegati come strumenti di contrasto al crimine in funzione predittiva o anche a reato consumato.[10]

Nello specifico degli strumenti di controllo alle frontiere, le attività predittive che impiegano sia sistemi algoritmici di trattamento dei dati sia sistemi di riconoscimento facciale permetterebbero la profilazione dei possibili autori di reato prima che i delitti siano perpetrati. Ed è proprio nel solco della funzione predittiva che si inserisce il nuovo sistema *IBorderCtrl*,[11] di cui il presente contributo si prefigge lo scopo di illustrarne il funzionamento al fine di conoscerne i meccanismi e le potenzialità ma anche i limiti e le criticità.

2. *Iborderctrl*, un significativo cambio di passo

La crescente centralità dei temi legati alla sicurezza nell'agenda europea scaturisce sia da fattori contingenti e reali, sia dall'incremento generale e condiviso tra i popoli di un sentimento di paura e incertezza per il futuro. I maggiori indicatori sono, da un lato, l'affinamento delle strategie criminali per il superamento dei confini europei, l'aumento dei flussi migratori, la crescente consapevolezza circa le possibilità di manipolazioni e alterazioni dei dati e dei documenti anche grazie alla criminalità informatica. Dall'altro, il rafforzamento anche della stessa fobocrazia, che sin ora era stata contenuta nei singoli confini nazionali e grazie alla quale la sicurezza è divenuta un bene bilanciabile con gli altri diritti, ben oltre quanto gli stessi principi sovranazionali consentirebbero.

Le conseguenze tangibili sono duplici: il ripristino di fatto delle frontiere con la reintroduzione dei controlli anche ai cittadini europei ad opera del Regolamento 2017/458[12] e il ricorso massivo alle tecniche di riconoscimento facciale sin ora considerate sproporzionate rispetto agli obiettivi perseguiti.

---

[10] F. Basile, "Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine"*, Diritto Penale e Uomo-DPU*, 29 settembre 2019.

[11] H. Surden, "Artificial Intelligence and Law: An Overview", *Georgia State University Law Review*, 2019, p. 1333, secondo cui l'apprendimento automatico e in particolare gli strumenti di riconoscimento facciale possono aiutare a raccogliere dati sulla criminalità e orientare risorse dove è necessario.

[12] Il Codice Schengen, istituito con Regolamento (UE) 2016/399 del Parlamento europeo e del Consiglio del 9 marzo 2016 è stato sospeso numerose volte (si calcola siano 116. V. <*https://www.ispionline.it/it/pubblicazione/europa-blindata-25410*>), sia per esigenze connesse agli attacchi terroristici, sia recentemente per esigenza sanitarie connesse alla pandemia in atto.

Lo sviluppo tecnologico e l'implementazione dei sistemi di IA hanno, poi, costituito l'ulteriore spinta all'introduzione – seppure in via sperimentale – del nuovo sistema *IBorderCtrl*, che per le sue caratteristiche si inserisce nel terzo gruppo delle misure poste a controllo delle frontiere europee.

Se questo è il quadro di riferimento in cui si inserisce il nuovo strumento, il suo fondamento coincide con la considerazione che ogni singolo sistema è fallace, anche quello più avanzato[13]. L'impronta può essere sofisticata, la faccia camuffata, ma finanche lo *scanner* della vena del palmo della mano, sinora ritenuto più efficace del rilevamento delle impronte, può subire alterazione a causa dello sporco. Solo la combinazione di tutti gli strumenti a disposizione è capace di garantire un miglior risultato riguardo agli obiettivi di controllo e monitoraggio delle frontiere.[14]

La nuova procedura costituisce una novità assoluta rispetto al suo funzionamento, proprio perché sfrutta più tecniche contemporaneamente: dati personali, dati biometrici,[15] riconoscimento facciale, tecnica di rilevamento dell'inganno. Il sistema prevede due fasi consequenziali, una antecedente l'inizio del viaggio e una contestuale all'attraversamento della frontiera.

La prima si sostanzia in un triplice obbligo posto a carico del viaggiatore, il quale è tenuto ad allegare una semplice fotografia, a registrare sulla piattaforma digitale dedicata alcuni dati personali e, infine, a sottoporsi a una intervista allo scopo di accertare la veridicità delle sue affermazioni. Il protagonista di quest'ultimo momento è un sistema che erroneamente viene definito ora come una semplice forma di riconoscimento facciale, ora come un rilevatore automatico di inganno, ma che invece combina entrambi gli aspetti con una forma di IA addestrata, tramite le tecniche di *machine learning*, a svelare i raggiri elabo-

---

[13] *IBorderCtrl*, infatti, è solo l'ultimo di una serie di misure adottate dall'UE nel controllo delle frontiere, il cui comune denominatore è la rilevanza e il trattamento di dati, sia in termini quantitativi, sia in termini qualitativi e che sono raggruppabili in tre categorie a seconda se adottino sistemi tradizionali come la verifica dei documenti seppure automatizzata, tecniche innovative di trattamento dei dati o, infine, un'azione sinergica di nuove tecnologie. Non è questa la sede per illustrarne il funzionamento e sottolineare gli aspetti critici, ma basti sapere che nel primo gruppo rientrano la procedura nota come *Registered Traveller Programme* (RTP) e il *Visa Information System* (VIS). Diversamente, nella seconda categoria, invece, si inserisce il cd. *Passenger Name Record* (PNR), nonché *l'European Travel Information and Authorisation System* (ETIAS). Entrambi affiancano il già collaudato *Schengen Information System* (SIS II), mentre si inserisce nel terzo gruppo il sistema informativo centralizzato *Entry/Exit System* (EES), che sfrutta i dati raccolti dal VIS, le informazioni sulle impronte digitali provenienti dalla banca dati *European Dactyloscopie* (EURODAC) e infine i dati raccolti nell'*European Criminal Records information System* (ECRIS). Giova sottolineare che nel 2013 fu presentato il pacchetto *Frontiere intelligenti*, che non trovò all'epoca l'avallo dei tecnici per alcune criticità rilevate in merito alla tutela della privacy. Per una panoramica più dettagliata delle misure adottate, v. <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52016DC0205&from=EN> (06/21).

[14] K. CrocKett et al., "Do Europe's Borders Need Multifaceted Biometric Protection?"*, Biometric Technology Today Journal*, 2017, p. 1.

[15] L'art. 9 del Regolamento (UE) 2016/679, meglio noto come GDPR, include nei dati personali anche i dati biometrici, tuttavia in questa analisi li si tratta separatamente in considerazione del diverso momento in cui vengono trattati.

rando tutti i dati raccolti.[16] Nello specifico, il soggetto viene virtualmente accolto da un cd. *avatar* dalle sembianze umane che lo interroga in merito ai motivi del suo viaggio; tuttavia, non sono solo le risposte fornite e le eventuali contraddizioni verbali a permettere alla macchina di accertarne la verità, bensì il complesso del comportamento non verbale rilevato. A differenza delle comuni macchine delle verità *IBorderCtrl* si serve di uno strumento che non analizza gli indicatori fisiologici o le micro-espressioni, piuttosto l'apprendimento fondato sulla generalizzazione di esempi ingannevoli e indipendente da un modello esplicativo sottostante permette di esaminare i micro-gesti ed è in grado di combinare autonomamente i singoli indicatori. Il vantaggio consiste nella possibilità di decifrare le emozioni dell'intervistato tramite l'analisi della mimica facciale, senza che il soggetto riesca a correggere e controllare psicologicamente queste manifestazioni. A seguito di questa procedura sarà assegnato un punteggio di rischio[17] rispetto alla eventuale falsità dell'identità che sarà, poi, verificato dalla guardia di frontiera. Si tratta di una sorta di *screening* digitale pre-partenza che, in linea con gli scopi perseguiti dai sistemi illustrati in precedenza (ad esempio EES), permette di ridurre i tempi di attesa alle frontiere e migliorare il controllo. Tutte le informazioni così raccolte saranno messe in correlazione sia con quelle contenute nelle banche dati istituzionali poste in rete tra loro (come eventuali condanne penali, inserimento del nome in liste nere o segnalazioni di altro genere), sia con una serie di *open data* raccolti dal sistema nel *web*.

La seconda fase, a questo punto, risulta più veloce e incentrata effettivamente su un sistema di riconoscimento facciale volto ad accertare l'identità del soggetto che intende oltrepassare il cancello. La guardia di frontiera dispone di una unità portatile che gli permette di raccogliere tutti i dati biometrici utili alla verifica dell'identità, come il sensore di impronta digitale e palmare, la fotocamera e il lettore di documenti. Nello specifico, la sovrapposizione delle immagini raccolte con il dispositivo portatile alle immagini contenute nei documenti, l'abbinamento dell'immagine con il modello biometrico della persona e le sequenze video permettono la verifica della corrispondenza dell'identità di colui che ha effettuato la registrazione nella prima fase con la persona che si trova al valico, determinando il suo riconoscimento come un utente *IBorderCtrl*.

Gli studi condotti circa l'efficacia dello strumento riportano un *true positive rate* pari al 95,3%, un *false positive rate* dello 0,1% e un'accuratezza complessiva del 99,5%, risultati che soddisfano pienamente i requisiti richiesti nelle linee guida elaborate per il sistema *Frontex*.

La sperimentazione è durata tre anni ed è stato impiegato ai controlli fronta-

[16] Il sistema adotta la tecnologia elaborata dal Dipartimento di Calcolo Computazionale e Matematica della *Manchester Metropolitan University* denominata *Silent Talker*, in <https://www.mmu.ac.uk/news-and-events/news/story/?id=77>.

[17] L'intelligenza artificiale rivolge all'utente sedici domande semplici circa i suoi dati e il viaggio che intende intraprendere. Per comprendere le motivazioni del punteggio di rischio assegnato è possibile rivolgere una richiesta di accesso agli atti a *EuroDynamics*, la società capofila del progetto, in <https://www.eurodyn.com/?s=iborderctrl>.

lieri di Ungheria, Lettonia e Grecia da settembre 2016 ad agosto 2019, grazie al finanziamento di 4,5 milioni di euro stanziati dal programma di ricerca della Commissione europea *Horizon 2020*.

3.1. Alcuni profili di criticità: i possibili contrasti con i principi fondamentali

Negli ultimi tre anni le istituzioni sovranazionali hanno mostrato di esser ben consapevoli dei rischi significativi in termini di lesione sia dei principi fondamentali sia dei diritti umani, tanto da gettare le basi di una regolamentazione futura adottando alcuni importanti provvedimenti, di cui la Proposta di Regolamento sull'approccio europeo all'IA del 21 aprile scorso costituisce solo l'ultimo atto.[18]

I maggiori pericoli derivano soprattutto dal problema della qualità[19] dei dati utilizzati nei sistemi di apprendimento che alimentano le macchine, nonché dai rischi connessi all'impiego di tecniche di tracciamento a mezzo degli strumenti di riconoscimento facciale.

Sebbene alla base del sistema *IBorderCtrl* operi esplicitamente una presunzione di favore secondo cui tutti i viaggiatori sottoposti alla misura sono considerati in buona fede, questa potrebbe ridursi a una mera enunciazione di principio. Sottesa allo strumento, infatti, opera anche una presunzione implicita di irregolarità, che scaturisce dall'impiego di dati biometrici (in particolar modo informazioni riguardanti la razza, l'etnia, il genere) viziati dai pregiudizi[20] che l'operatore riversa nelle macchine per il tramite delle tecniche di apprendimento automatico e i cui effetti distorsivi possono determinare forme di disuguaglianza e discriminazione.[21] Elevati i rischi di criminalizzazione che si autoavverano, nella misura in cui se il sistema è alimentato da dati viziati *ab origine*, il pregiudizio si alimenta ancora di più, inducendo a cercare il crimine in determinate tipologie di soggetti con gravi pericoli di distorsione del sistema.[22]

---

[18] Le tappe più significative di questo approccio sono costituite dapprima dalla Strategia europea sull'intelligenza artificiale resa pubblica nel 2018, poi dalle linee guida emanate nel 2019 e, infine, il Libro Bianco sull'intelligenza artificiale pubblicato dalla Commissione nel 2020. In questo arco temporale si sono susseguite anche altre iniziative (ad esempio, in ambito civilistico si segnala la *Risoluzione del Parlamento europeo del 16febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*). V.<*https://temi.camera.it/leg18/post/OCD15_14416/il-nuovo-approccio-europeo-all-intelligenza-artificiale.html*>.

[19] D. Piana, L. Verzelloni, "Intelligenze e garanzie. quale governance della conoscenza nella giustizia digitale?", *Quaderni Scienze Politiche*, 2019, pp. 372 ss.

[20] H. Surden, *Artificial intelligence*, cit., p. 1335.

[21] S. Quattrocolo, "Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente riflessione tra scienze penale e informatiche", *La legislazione Penale*, 2018, p. 6; S. Signorato, "Giustizia penale e intelligenza artificiale. Considerazioni in tema di algoritmo predittivo", *Rivista Diritto Procedura Penale*, 2020, p. 612; A. Simoncini, "L'algoritmo incostituzionale: intelligenza artificiale e il futuro della libertà", *BioLaw Journal – Rivista BioDiritto*, 2019, p. 84.

[22] W. Thomas, D. Thomas, *The child in America: behavior problems and programs, Alfred A. Knopf, Inc.,* New York, 1928; R.K. Merton, *La profezia che si autoavvera*, *Teoria e Struttura Sociale*,

Questioni di discriminazione algoritmica si pongono anche a seguito dell'impiego degli strumenti di riconoscimento facciale più o meno evoluti, che possono tradursi in ipotesi di violazioni dei diritti umani e più genericamente di lesioni del principio di uguaglianza.[23]

Al contempo, però, la valutazione dei dati inseriti dal viaggiatore ad opera di un sistema unico e un procedimento di apprendimento automatico che utilizza gli stessi *data set* sembrerebbe risolvere i casi di disparità di trattamento rispetto alle modalità di controllo esperite dal singolo paese di confine.[24]

Come in tutte le ipotesi in cui la politica criminale anticipa il momento della tutela optando per strategie di prevenzione, si pone il tema delle garanzie. In questi termini il controllo alle frontiere, infatti, si colloca in un'area grigia che esula dalle tutele proprie del diritto penale sostanziale e processuale, avallando il convincimento che il crimine vada prevenuto ancorché non si sia prodotto nessun fatto e nessun danno. Ne consegue un rovesciamento di prospettiva, nella misura in cui non rileva più l'oggetto della tutela, bensì il soggetto con uno slittamento sempre più accentuato del diritto penale verso ipotesi di responsabilità d'autore, aggravate dal ritorno a forme di determinismo biologico strisciante,[25] che trovano un terreno fertile nel legame proprio tra i dati biometrici analizzati e i pregiudizi di cui si è detto innanzi.

La prevenzione dei fatti criminosi, poi, è un concetto che – a primo acchito – si pone facilmente in correlazione diretta con le nozioni di predizione e prevedibilità, ma che risulta essere distopico rispetto agli stessi; pur rinviando a un'idea di previsione basata su calcoli scientifici, infatti, non si può non considerare che il sistema *IBorderCtrl* restituisce un risultato in termini di inferenza statistica. Si tratta di un *modus operandi* ben noto al diritto penale, tuttavia è cosa ben diversa dedurre da una percentuale il nesso causale che lega un fatto accaduto a una condotta posta in essere, rispetto all'utilizzo di una percentuale probabilistica nella valutazione di un generico rischio criminale. Tutt'al più la

---

II, Il Mulino, Bologna, 1971.

[23] Il rischio è particolarmente elevato per le discriminazioni a danno delle minoranze etniche, come sembrerebbe succedere in Cina, dove è in corso di sperimentazione un *software* di riconoscimento facciale che invia un segnale di allarme nel caso in cui il soggetto faccia parte della popolazione degli Uiguri. Cfr. <*https://www.agendadigitale.eu/sicurezza/privacy/sorveglianza-di-massa-in-cina-cosi-funziona-il-modello-che-spaventa-loccidente/*>. V. anche <*http://gendershades.org/overview.html*>, che mette in correlazione i rischi di discriminazione per le minoranze etniche rispetto agli errori prodotti dai sistemi di riconoscimento facciale. Invero, il 4 aprile 2021 un tribunale cinese ha riconosciuto il diritto dei cittadini alla cancellazione dei propri dati acquisiti con le tecniche biometriche di rilevamento facciale, ponendo così un freno all'abuso di questi sistemi. In <*https://www.wired.it/attualita/tech/2021/04/14/cina-riconoscimento-facciale-causa/*>. Anche le discriminazioni di genere trovano terreno fertile, v. <*http://gendershades.org/*>.

[24] La questione fu sollevata in riferimento alla Direttiva 2016/681/UE introduttiva del sistema di *Passenger name record*. I dati dei viaggiatori, infatti, sono contenuti nelle banche dati dei singoli paesi, i quali utilizzano modalità di analisi e trattamento diversi, tale che potrebbe essere difficile garantire una uniformità di applicazione. Si veda <*https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_executive_summary_en.pdf*>.

[25] Quattrocolo, *Intelligenza,* cit., *supra* note 21, p. 10.

questione potrebbe essere superata ove il punteggio di rischio assegnato al viaggiatore non sia determinante in maniera esclusiva rispetto alla decisione di ammettere o meno l'ingresso del soggetto, ma residui un margine di valutazione in capo alla guardia di frontiera.[26]

Altri profili di criticità si pongono rispetto all'impiego di questo sistema. Sino ad ora esso è stato testato in via sperimentale e su base volontaria, ma allorquando dovesse essere annoverato tra i legittimi e ordinari strumenti di controllo alle frontiere esterne, si evidenzieranno questioni di responsabilità e colpevolezza per i casi in cui il viaggiatore si rifiuti di fornire i propri dati personali e biometrici. Gli sarà impedito il transito? Sarà automaticamente considerato un soggetto ad alto rischio? La condotta potrebbe integrare gli estremi di una fattispecie penale alla stessa stregua del *rifiuto di indicazioni sulla propria identità personale* prevista nel nostro ordinamento dall'art. 651 c.p.?[27]

L'evidenza dei contrasti che il ricorso a queste tecniche di controllo e prevenzione possono determinare rispetto ad alcuni principi fondamentali dell'ordinamento sovranazionale e nazionale – a partire proprio da quelli di non discriminazione, di uguaglianza, di colpevolezza e di offensività – è tale da trovarne traccia in tutti i documenti europei dedicati alla regolamentazione delle nuove tecnologie.[28]

Finanche i principi di equità e proporzionalità soffrono al cospetto dei nuovi strumenti, dal momento che si tratta di concetti che sfuggono ad una praticabilità algoritmica e che richiedono un'attività interpretativa che solo l'uomo può garantire.[29]

Allo stesso modo il principio di stretta necessità non trova una piena rispondenza rispetto agli scopi di gestione delle frontiere, ma sembra piuttosto una adeguatezza forzata, posto che già per le misure contenute nel pacchetto *Frontiere Intelligenti* e per il sistema *Entry/Exi*t la Commissione di esperti le aveva ritenute sproporzionate e l'obiettivo non raggiunto.[30]

---

[26] Tale considerazione è stata recepita sia nella citata Carta etica sia nella Proposta di Regolamento e richiama quanto affermato anche dalla Corte Suprema del Wisconsin in America nel noto caso *Loomis* relativo ai risultati prodotti dal *software* predittivo *Compas* in uso alla polizia locale.

[27] Potrebbe trovare applicazione l'art. 4 *Testo Unico sulle leggi di pubblica sicurezza* (T.U.L.P.S.) e art. 294 del relativo regolamento rispetto all'ipotesi di mancata esibizione di un documento di identità.

[28] Sui rischi di discriminazione e conseguente violazione del principio di uguaglianza, ad esempio, il Regolamento UE 679/2016 prevede al *Considerando* n. 71 che siano *impediti gli effetti discriminatori nei confronti delle persone fisiche base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello* status *genetico, dello stato di salute o dell'orientamento* sessuale*, ovvero che comportano misure aventi tali effetti.* Il dettato è di ampia portata e va riferito non solo alle attività di profilazione dei dati personale, quanto piuttosto a tutte le attività anche di tipo predittivo come il riconoscimento facciale. A. Simoncini, *L'algoritmo*, cit., p. 84. Anche la Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia penale e nei relativi ambienti stilato dalla Cepej nell'ambito del Consiglio d'Europa ne dà conto al secondo principio, prevedendo il divieto *di creare o accentuare discriminazioni tra gruppi e individui.* Quattrocolo, *Intelligenza*, cit., *supra* note 21, p. 5.

[29] Signorato, *Giustizia penale*, cit., *supra* note 21, p. 611.

[30] Il Gruppo di Lavoro istituito in virtù dell'articolo 29 della Direttiva 95/46/CE aveva ritenuto che

3.2. Alcuni profili di criticità: dati e diritti fondamentali

Violazione dei principi fondamentali e lesione dei diritti umani rappresentano un'endiadi inscindibile, soprattutto quando alla base della questione si pone l'impiego dei dati di qualunque specie essi siano, con i quali – invece – si ravvisa un rapporto quasi antinomico. In particolare, i dati possono assumere una dimensione attiva o passiva, a seconda se costituiscono uno strumento di tutela dei diritti fondamentali o contribuiscano alla restrizione o lesione degli stessi, ovvero siano l'oggetto della tutela qualora impiegati in maniera illegittima, fraudolenta o senza il consenso del titolare.

Rispetto alla prima ipotesi, nell'impiego di *IBorderCtrl* i dati costituiscono le due facce di una stessa medaglia. Da un lato, essi contribuiscono a garantire la dignità umana, dal momento che un miglioramento nell'efficienza dei controlli alle frontiere esterne facilitano anche l'ingresso nell'Unione di coloro che ne hanno il diritto e contribuiscono a garantire la sicurezza di tutti.[31] Dall'altro invece, ci si interroga sull'opportunità che dalla raccolta dei dati dei viaggiatori possa dipendere in via esclusiva l'autorizzazione all'ingresso nell'area Schengen e se questo non possa tradursi piuttosto in una violazione dei diritti di libertà.

Diversamente, in relazione alla misura passiva dei dati, non si pone né un problema di *privacy*, né di titolarità del trattamento dei dati personali e biometrici.[32] Nella maggior parte delle ipotesi in cui i dati personali sono utilizzati come strumento di prevenzione, infatti, la persona non ne è a conoscenza e non può esercitare il diritto di tutela. Tuttavia, nel caso dell'impiego di *IBorderCtrl* il soggetto accede volontariamente alla piattaforma e ha conoscenza sin da subito delle finalità di impiego, esprimendo un consenso in fase di registrazione.[33] Semmai la questione si riduce alle sole ipotesi di conservazione o trasferimento a soggetti terzi dei dati così raccolti, ipotesi che sono oggetto di specifiche disposizioni nella regolamentazione degli altri sistemi di ingresso già in uso in Europa, per i quali è previsti che i dati siano conservati in archivi per un limitato periodo di tempo e che possano essere ceduti solo in ipotesi tassative, e che si

---

"il valore aggiunto di un sistema di ingressi/uscite ai fini del conseguimento di tali obiettivi non è un elemento sufficiente per dimostrarne la necessità e la proporzionalità in termini di ricadute sui diritti fondamentali, in particolare il diritto alla protezione dei dati e alla vita privata. Le ingerenze nella vita privata devono essere "necessarie in una società democratica" e il mero valore aggiunto non soddisfa il criterio di necessità in tale contesto", in <*http://ec.europa.eu/justice/policies/privacy/index_en.htm*>.

[31] Nel Codice Schengen al *Considerando n. 7* si afferma che le verifiche e i controlli frontalieri *dovrebbero* essere effettuati nel pieno rispetto della dignità umana; l'uso del verbo al condizionale lascia intendere che le difficoltà di gestione siano note e che, dunque, questo non sempre è garantito. Proprio il ricorso alle nuove tecnologie potrebbe appunto contribuire a un miglioramento di tali condizioni.

[32] E. Sacchetto, *Face to face: il complesso rapporto tra automated facial recognition thecnology e processo penale*, *La Legislazione Pen*ale, issue 10, 2020, p. 2. V. la Proposta di Regolamento del 21 aprile 2021, pp. 21 e 45.

[33] Certo potrebbero non mancare rischi di scarsa informazione e comprensione rispetto al trattamento dei dati. Cfr. <*https://www.iborderctrl.eu/The-project*>.

immagina saranno adottate anche nel caso in cui *IBorderCtrl* divenisse operativo in maniera definitiva.[34]

I dati posti alla base del funzionamento di *IBorderCtrl* non sono solo quelli forniti dal viaggiatore, ma si pongono questioni anche rispetto ai *data set* che sono utilizzati per alimentare l'apprendimento automatico del sistema di IA. Garantire la qualità e la trasparenza di questa tipologia di dati, infatti, significa garantire la sicurezza del sistema; purtuttavia, si tratta di condizioni che difficilmente possono essere assicurate.[35] Se è vero, infatti, che in documenti come la Carta etica del Cepej e la Proposta di Regolamento ultima è esplicitamente previsto un principio di trasparenza tecnica,[36] è altrettanto vero che tecnicamente non è possibile soddisfare tale previsione, dal momento che neanche i programmatori riescono a mantenere il controllo su tutto il procedimento di formazione.[37] La mancanza di trasparenza e accessibilità dei dati, allora, si traduce nella possibile lesione anche del diritto a un equo processo, qualora il visitatore a cui è stato negato l'attraversamento dei confini europei decida di impugnare il provvedimento di diniego e la lesione è ancora più significativa ove si consideri che il risultato ultimo dell'intero procedimento è una previsione di rischio.[38]

Tutt'al più si può incidere sulla qualità dei dati iniziali utilizzati per l'addestramento dell'IA, chiamati a soddisfare stringenti criteri di qualità secondo quanto previsto anche dall'art. 10 della citata Proposta di Regolamento.

Il tema dell'accuratezza dei dati acquisisce un'importanza ancora maggiore ove si consideri che essi costituiscono il fondamento anche degli stessi sistemi di riconoscimento facciale.

3.3. Alcuni profili di criticità: il riconoscimento facciale

Dalla lettura di tutti i più recenti documenti prodotti dall'Unione europea sulle nuove tecnologie si evince che le preoccupazioni degli esperti rispetto alle criticità rilevate per l'impiego di strumenti di riconoscimento biometrico sono maggiori delle considerazioni in termini di vantaggi e benefici. È così, ad esem-

[34] Nell'attuale fase sperimentale è previsto che le informazioni raccolte siano cancellate dal sistema immediatamente dopo l'effettuazione del controllo.

[35] C. Barabas, *Beyond Bias: "Ethical AI" in Criminal Law*, in M.D. Dubber et al., *The Oxford Handbook of Ethics of AI*, Oxford University Press, Oxford, 2020, pp. 1-21.

[36] Il mito della trasparenza e neutralità è ancora largamente diffuso: l'art. 13 della Proposta di Regolamento del 21 aprile 2021 è rubricato *Trasparenza e fornitura di informazioni agli utenti.* Per la Carte etica del Cepej, si veda <*https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348*>. Persino il Consiglio di Stato del nostro paese ha invocato un *principio di trasparenza rafforzato* come fondamento degli algoritmi. Così C. di S. Sez. IV, sentenza 8 aprile 2019 n. 2270.

[37] S. Signorato, *Giustizia penale*, cit., pp. 611 ss.

[38] D.F. Engstrom et al., *Government by algorithm: artificial intelligence in Federal ADministrative Agencies,* in <*https://www.acus.gov/sites/default/files/documents/Government%20by%20Algorithm.pdf, 2020, 10/2020*>.

pio, per il Comitato consultivo della cd. Convenzione 108+,[39] secondo cui gli strumenti preposti al riconoscimento facciale possono entrare in conflitto con i valori propri dell'Unione europea, a cominciare dalla dignità umana, dal principio di non discriminazione e dalla libertà di espressione.[40] Ancora, il Comitato europeo per la protezione dei dati ha pubblicato il 29 gennaio 2020 delle Linee guida sul trattamento dei dati attraverso dispositivi video, in cui si citano anche le tecniche di riconoscimento facciale, foriere di maggiori rischi per i diritti delle persone e consentite solo se rispettano i principi di liceità, necessità, proporzionalità e minimizzazione dei dati (così come previsto anche dal GDPR del 2016); il loro impiego, poi, deve essere preceduto da valutazioni di impatto sui diritti e sulle libertà fondamentali.[41]

I timori per i rischi prospettati si amplificano ulteriormente, quando si analizza la tecnologia posta alla base del sistema *IBorderCtrl*. L'aspetto più controverso riguarda proprio il sistema di riconoscimento affettivo, che non si limita ai dati biometrici, bensì analizza le emozioni delle persone tramite l'analisi dei micro-gesti facciali non verbali. L'IA cd. emozionale riesce a cogliere i livelli di stress e ansia, esaminando i biomarcatori di inganno e permettendo, così, di distinguere i viaggiatori in buona fede e quelli non in buona fede.

Seppure già impiegato in Inghilterra e negli Stati Uniti,[42] il sistema ha suscitato molte critiche e destato perplessità,[43] sia in ordine al suo fondamento scientifico sia in termini di proporzione rispetto alle finalità di prevenzione del crimine. In riferimento a quest'ultimo punto, infatti, si profilerebbe una violazione del principio di autodeterminazione della persona e la possibile lesione della libertà morale[44] non giustificabile neanche con le esigenze di ordine pubblico e sicurezza della collettività.[45]

Invero, nella specifica ipotesi di *IBorderCtrl* la questione potrebbe subire un ridimensionamento, ove si verificassero alcune condizioni.

La prima coincide con il soddisfacimento del principio di trasparenza e co-

---

[39] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale del Consiglio d'Europa del 28 gennaio1981, modificata nel 2018.

[40] *Linee-guida in materia di intelligenza artificiale e protezione dei dati* del 25 gennaio 2919. V. <*https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3*>.

[41] <*https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_it.pdf*>.

[42] In Inghilterra il sistema è stato impiegato nel 2011 proprio per il controllo alle frontiere dal *Border Agency*. J.S. Monedero, L. Dencik, *The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl,* in *Information, Communication and Society*, issue 8, 2020, p. 1.

[43] D. Boffey, *EU border 'lie detector' system criticised as pseudoscience,* in <*https://www.theguardian.com/world/2018/nov/02/eu-border-lie-detection-system-criticised-as-pseudoscience*>, issue 1, 2018 e <*https://www.agendadigitale.eu/sicurezza/privacy/sorveglianza-di-massa-in-cina-cosi-funziona-il-modello-che-spaventa-loccidente/*>, issue 3, 2020. Cfr. <*https://iborderctrl.no/*>.

[44] R. Kostoris, *Genetica, neuroscienze e diritto penale*, in D. Provolo, S. Riondato, F. Yenisey (eds.), *Genetics, Robotics, Law, Punishment*, Padova University Press, Padova, 2014, p. 344.

[45] AAVV, *Artificial intelligence and robotics for law enforcement*, UNICRI-Interpol, Torino, 2019, p. 13.

noscibilità algoritmica già indicato genericamente per i dati e per il quale la Proposta di Regolamento del 21 aprile 2021 prevede un preciso obbligo in caso di sistemi di rilevamento biometrico.[46] A questo fanno seguito il necessario consenso del soggetto che accede al servizio e la possibilità che questi ne mantenga il controllo.

In particolare, rispetto al requisito del consenso, in alcuni paesi[47] è fatto divieto di utilizzare le tecniche di riconoscimento facciale diffuse indiscriminatamente nei luoghi pubblici, non potendo essere prestato di volta in volta il consenso dalle persone in transito.

Effettivamente, nel caso di *IBorderCtrl* non vi è dubbio che il consenso sia prestato all'atto della registrazione sulla piattaforma dedicata e, pertanto, il rispetto dell'autodeterminazione del singolo sarebbe assicurato almeno formalmente.[48] E, infatti, le Linee guida sul trattamento dei dati personali attraverso dispositivi video del 2020 ritengono fondamentale il consenso dell'interessato ma affermano che esso non debba costituire una condizione per l'accesso al servizio. Alla stessa stregua, anche le Linee guida sul riconoscimento facciale del Consiglio d'Europa del 2021 non mancano di osservare che il consenso non dovrebbe costituire la base giuridica per giustificare il riconoscimento facciale da parte della pubblica autorità, giacché tra questa e i soggetti privati ci sarà sempre uno squilibrio di poteri.[49]

Sul punto sarebbe opportuno capire cosa prevederà la disciplina normativa eventualmente adottata al termine della sperimentazione di *IBorderCtrl*, rispetto all'ipotesi in cui il viaggiatore neghi il suo consenso, se sarà prevista una soluzione alternativa ovvero gli sarà negato l'accesso all'area Schengen.

Infine, la garanzia del pieno rispetto del principio di autodeterminazione può essere assicurata solo se – oltre alla conoscibilità e al consenso espresso – l'utente possa mantenere sempre il dominio delle sue scelte, indipendentemente dalla complessità del sistema che sta utilizzando, così come è previsto anche dal quinto principio della Carta Etica del Cepej.[50] Le nuove tecnologie, infatti, devono costituire un'opportunità e un vantaggio per la collettività e per il singolo e non devono rappresentare in alcun modo un limite vincolante a carattere negativo.

A ben vedere, i timori che tutto questo possa non essere pienamente soddi-

---

[46] Titolo IV alla p. 73, recante *obblighi di trasparenza per determinati sistemi di AI.*

[47] In USA, il *Biometric Information Privacy Act dell'Illinois*, il *Washington's Biometric identifiers Act* e Il *Personal Identify Information Act* del Texas, ritengono il consenso elemento fondante delle tecniche di riconoscimento facciale. Cfr. R. Girasa, *Artificial Intelligence as a disruptive technology. Economic Transformation and Government Regulation*, Palgrave McMillan, Svizzera, 2020, pp. 1 ss.

[48] E. Currao, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?, Diritto Penale e Uomo-DPU*, 2021, p. 12.

[49] *Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, Convention 108, Guidelines on Facial Recognition Directorate General of Human Rights and Rule of Law, in* <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3>, p. 6.

[50] S. Quattrocolo, *Intelligenza artificiale*, cit., p. 9.

sfatto, in tema di riconoscimento facciale, permangono. Premesso che la maggior parte dei sistemi di IA sono considerati ad alto rischio,[51] dalla lettura della Proposta di Regolamento del 21 aprile 2021 emerge una doppia valutazione di impatto e di rischio.

Da un lato, al *Considerando* n. 39 si richiedono cautele ulteriori nell'impiego dei sistemi di intelligenza artificiali in materia di migrazione, asilo e controlli alle frontiere, potendo questi avere effetti su persone che si trovano spesso in una posizione particolarmente vulnerabile. Dall'altro, sono previste significative restrizioni all'uso dei sistemi di rilevamento biometrico, proprio perché considerati ad alto rischio, e consentiti solo per attività di *law enforcement* alle forze dell'ordine. Segnatamente, i sistemi di rilevamento biometrico remoto in tempo reale sono – in linea di principio – consentiti solo in tre ipotesi specifiche: per attività di contrasto per la ricerca mirata di potenziali vittime specifiche di reato, in caso di risposta a una minaccia imminente di attacco terroristico, per l'individuazione e l'identificazione degli autori di reati gravi. Si tratta di una casistica che, seppure tassativa, include anche le finalità di contrasto sottese ad *IBorderCtrl*, ossia il contrasto alla criminalità transfrontaliera.[52]

Sul fronte del formante giurisprudenziale, nonostante l'evidente coinvolgimento dei diritti fondamentali, ancora nessuna pronuncia si è avuta sul tema da parte della Corte europea e anche quelle ad opera delle Corti nazionali sono molto poche, oltre che di segno contrastante.

Una prima decisione, destinata a costituire un *leading case* piuttosto discusso, si è avuta ad opera dell'*High Court of Justice* di Cardiff. L'oggetto del procedimento è il sistema di riconoscimento facciale in uso in via sperimentale al corpo di polizia del Galles e ritenuto dal ricorrente lesivo del diritto alla riservatezza *ex* art. 8 Cedu, contrario alla Direttiva (UE) 2016/680 rispetto alla tutela del trattamento dei dati personali, nonché violativo dell'*Equality Act* del 2010 relativo al contrasto delle forme di discriminazione.[53] Contrariamente a tutte le aspettative, i giudici inglesi hanno respinto i motivi di doglianza del ricorrente e ritenuto il sistema di rilevamento biometrico lecito rispetto alla disciplina vigente, dal momento che la finalità di prevenzione dei reati perseguita a beneficio della collettività è proporzionata rispetto al sacrificio dei diritti del singolo, tanto più che non sarebbe stata raggiunta la prova circa la possibile influenza sul

[51] Consiglio europeo, Riunione speciale del Consiglio europeo (1° e 2 ottobre 2020) – Conclusioni EUCO 13/20, 2020.

[52] La Proposta al *Considerando* n. 23 chiarisce, altresì, che la disciplina ha valore di *lex specialis* rispetto alle maglie più larghe previste dall'art. 10 della Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla *protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.*

[53] J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice, Diritto Penale Contemporaneo*, 2020, pp. 231-247.

sistema di pregiudizi razziali o di genere. La Corte, inoltre, ha ritenuto lecito e trasparente il trattamento dei dati, poiché, in mancanza di corrispondenza tra le immagini catturate dal sistema e i nominativi inseriti negli elenchi in possesso delle forze dell'ordine, i dati raccolti sono cancellati immediatamente.

La giurisprudenza italiana non ha avuto ancora occasione di affrontare lo specifico tema del riconoscimento facciale, ma è significativa – ad avviso di chi scrive – una pronuncia relativa alla possibilità di introdurre nel processo penale delle prove fondate sulle nuove tecnologie. Il metodo *IAT*, indicato per provare la verità dei ricordi impliciti di una persona, è stato ritenuto dalla Corte di Appello di Brescia[54] contrario al dettato degli artt. 64 co. 2 e 188 c.p.p., in quanto capace di influenzare la libertà di determinazione o di alterare la capacità di ricordare e valutare i fatti, circostanza che non può essere ritenuta lecita nemmeno in presenza del consenso dell'interessato, non essendo la libertà morale un diritto disponibile o rinunciabile in alcun modo.

4. Rilievi conclusivi

Nel bilanciamento degli interessi coinvolti, la *società della sicurezza*[55] sembra acquisire una rilevanza preponderante, tanto da giustificare il sacrificio di alcuni beni giuridici, ancorché fondamentali, promuovendo forme di sorveglianza di massa dagli esiti incerti e rischiosi. Il controllo sociale affidato a sistemi tecnologici non ancora del tutto testati e conosciuti nel loro funzionamento destano molte perplessità quando ricadono su persone per le quali non ci sono prove di legami con reati gravi e sottintende un superamento della presunzione di innocenza a favore della presunzione di colpevolezza. Diversamente, ove i sistemi fossero impiegati su persone già in precedenza segnalate alle forze pubbliche con lo scopo di perseguire solo i reati più gravi, allora il loro uso potrebbe essere giustificato e la necessità di tutela della collettività potrebbe essere ritenuta prevalente rispetto a forme di responsabilità d'autore.

È pur vero che in tempi di forti migrazioni, rischi terroristici e finanche pericoli pandemici, non è più immaginabile che il controllo alle frontiere sia affidato solo al riscontro facciale effettuato da un agente rispetto a una immagine apposta su un passaporto o al suo istinto e *IBorderCtrl* potrebbe costituire non solo un rischio, ma anche un'opportunità. Le ricadute positive di questo strumento sull'efficacia in concreto dei controlli alle frontiere sono evidenti e si misurano in termini di velocità delle operazioni, uniformità nei controlli, scoperta delle false identità.

Tutto ciò a patto, però, che gli *standard* di verifica siano molto elevati, i ri-

[54] Corte App. Brescia, sez. II, sentenza 11 novembre 2020 n. 1683, in <file:///C:/Users/fdsde/OneDrive/Desktop/giorgia/sent%20brescia/1607551213_sentenza-corte-appello-brescia-test-iat.pdf>.

[55] M. Focault, *Sicurezza, popolazione e territorio, Corso al Collège de France* 1977-1978, Feltrinelli, Milano, 2005, pp. 15 ss.

sultati affidabili, i controlli continui e rigorosi,[56] perché la valutazione del rischio criminale e il *profiling* non necessariamente si traducono in attività violative dei diritti fondamentali, ma piuttosto è il rischio di valutazioni discriminatorie a contenere *in nuce* un pericolo di lesione.[57]

L'era della quarta rivoluzione[58] ci impone di non adottare posizioni di sfiducia algoritmica che portino a vietare *a priori* l'impiego dei nuovi strumenti, né a considerare i diritti delle persone in contrapposizione al progresso tecnologico come in un rapporto inversamente proporzionale. Piuttosto dovrebbe trovare ampia applicazione il principio di precauzione costituzionale,[59] nel continuo sforzo di bilanciamento tra progresso tecnologico e tutele. Potrebbe aiutare nell'intento anche una efficace regolamentazione rispetto alle ipotesi di responsabilità dei danni causati dalla scarsa qualità dei dati o dal loro errato trattamento, che non rimanga a livello di mera enunciazione di principio come nel caso dell'art. 25 GDPR.[60] Più in generale, è necessaria e non più rinviabile l'adozione di una normativa di dettaglio vincolante che regolamenti tutte le tipologie di strumenti e tutti i loro possibili usi.[61]

La previsione che l'uomo non affidi la verifica in via esclusiva ai nuovi strumenti e mantenga sempre un controllo sui risultati,[62] la possibilità di impugnativa del provvedimento e anche la previsione di un Garante,[63] sono misure che contribuiscono ad aumentare le garanzie rispetto all'impiego dell'intelligenza artificiale. Determinante potrebbe essere l'individuazione di parametri di validazione dei sistemi, sulla falsariga di quanto previsto nel 1993 dalla Corte Suprema degli Stati Uniti con i *Daubert standard* e che ha trovato l'avallo anche della Cassazione italiana nel 2010.[64]

Queste le misure di tutela, ma molto dipenderà dalla capacità di combinare

---

[56] S. Signorato, *Giustizia*, cit., p. 616.

[57] Commissione LIBE del Parlamento europeo, in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017DC0261&from=EN*.

[58] L. Floridi, *La quarta rivoluzione. Come l'infosfera sta rivoluzionando il mondo*, Raffaello Cortina Ed., Milano, 2017, *passim*.

[59] A. Simoncini, *L'algoritmo*, cit., pp. 86 ss., secondo cui si impone una tutela preventiva dei diritti fondamentali già in fase di progettazione dei nuovi sistemi (sia nel momento *by design*, sia *by default*). V. anche M.L. Gambini, *Algoritmi e sicurezza,* in *Giurisprudenza It*aliana, 2019, pp. 1726 ss. Sul principio di precauzione in diritto penale M. del Tufo, *Principio di precauzione e gestione del rischio: quali spazi applicativi per il diritto penale?,* in G. Carlizzi, G. Tuzet (eds.)*, La prova scientifica nel processo penale*, Giappichelli, Torino, 2018, pp. 137-177.

[60] Regolamento generale sulla protezione dei dati (UE/2016/679) Articolo 25 *Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita*.

[61] Currao, *Il riconoscimento*, cit., *supra* note 48, p. 23.

[62] La Proposta di Regolamento del 21 aprile 2021 dedica l'intero art. 14 al tema della sorveglianza umana rispetto alla progettazione e all'impiego delle nuove tecnologie. Il *Considerando* n. 65, poi, prevede che i sistemi considerati ad alto rischio siano valutati e certificati da soggetti terzi, estranei alla fase di progettazione. R. Girasa, *Artificial Intelligence*, cit., pp. 1 ss.

[63] Così è previsto anche per le attività di *Frontex*, per le quali è istituito un responsabile dei diritti fondamentali. Cfr. <https://frontex.europa.eu/it/cosa-facciamo/diritti-fondamentali/>.

[64] Cass. Pen. Sez. IV, 17 dicembre 2010, n. 43786.

la conoscenza causale, con la conoscenza scientifica e la conoscenza statistica, riconoscendo un ruolo preminente all'etica[65]. Dei ventitré *Principi di Asilomar*,[66] ben tredici sono dedicati all'etica e ai valori che devono ispirare l'intelligenza artificiale, tra cui l'allineamento dei valori di tali sistemi ai valori umani durante il loro funzionamento e la necessità che la loro progettazione e gestione sia compatibile con la dignità umana, i diritti, la libertà e la diversità culturale.

"Nonostante le fascinazioni della fisica quantistica, resta fermo che il comportamento umano non è prevedibile, essendo l'uomo un essere libero, sempre capace di autodeterminazione al netto dei condizionamenti esterni"[67] e neppure *IBorderCtrl* potrà aiutare a comprendere se un viaggiatore, pur mentendo, sia effettivamente in procinto di compiere un reato!

[65] T. Powers, J. Ganascia, *The Ethics of the Ethics of Artificial Intelligence*, in M. Dubber, F. Pasquale, S. Das (eds), Oxford Handbook of Ethics of AI, Oxford University Press, 2020, pp. 1 ss.

[66] I *Principi di Asilomar* sono stati stilati nel 2017 e sottoscritti dagli scienziati più autorevoli tra cui anche Stephen Hawking. Si tratta di un testo suddiviso in tre aree: la prima sulla *ricerca*, la seconda su *etica e valori*, la terza e ultima sui *problemi di scenario*.

[67] T.M. Powers, J.B. Ganascia*, Ethics*, cit., p. 64.

NEUROSCIENCE, ARTIFICIAL INTELLIGENCE AND PROTECTION FOR PERSONAL RIGHTS

Roberta Catalano

1. Legal Questions Regarding the Advent of Neuroscience

The advent and development of tomographic, eye-tracking and brain imaging techniques has opened up new fields of investigation to scientific research. These techniques, in fact, have made possible, for the first time, the observation and study of neural mechanisms that are activated in the human brain during the exercise of cognitive, decision-making and behavioural functions, and, therefore, have allowed scientists to investigate the correlation between mental activity and biological dimension of the individual. These researches, having as object the nervous system and, above all, the brain, are designated with the expression "cognitive neuroscience" and described as the study aimed at revealing how psychic functions emerge from neural circuits.[1]

In recent years, the number of neuroscientific studies has increased exponentially as their results are used to implement the technologies of robotics and artificial intelligence (AI), which are developed precisely on the basis of models of operation of neural circuits. The obvious breadth and complexity of the object of investigation leads to assess with great caution the results of these experiments. Nevertheless, philosophers, bioethicists and jurists have begun to reflect on these results and to ask if, and to what extent, the knowledge gradually acquired are able to challenge some traditional categories of philosophical, ethical and legal thought.[2] The attention of jurists, at a first moment, focused on the redefinition of the relationship between individual will and behaviour, since several neuroscientific studies, supported by research in behavioural genetics, have shown that decision-making processes oc-

[1] About cognitive neuroscience cf., among others, G. M. Edelman, *Darwinismo neurale*, Milan, 2018; B.R.Postle, G. Zoccoli, A. Sgoifo, *Neuroscienze cognitive. L'essenziale*, Giuffrè, Milan, 2016.

[2] See, among others, the analyses of L. TAFARO, *Neuromarketing e tutela del consenso*, ESI, Naples, 2018; S. Fuselli (ed.), *Neurodiritto. Prospettive epistemologiche, antropologiche e biogiuridiche*, Mimesis, Milan-Udine, 2016; ID., *Diritto, neuroscienze, filosofia. Un itinerario*, Feltrinelli, Milan, 2014, p. 11 ff.; D.J. Linden, *La bussola del piacere*, Codice edizioni, Turin, 2012; A. Santosuosso, *Diritto, scienza, nuove tecnologie*, Cedam, Padova, 2012; AA. VV., *Siamo davvero liberi? Le neuroscienze e il mistero del libero arbitrio*, Giuffrè, Milan, 2010; A. Santosuosso (ed.), *Le neuroscienze e il diritto*, Ibis, Pavia, 2009, p. 11 ff.; L.S. Khosbin - S. Khosbin, "Imaging the mind, Minding the image: an historical introduction to brain imaging and the law", *American Journal of Law and Medicine*, 2007, p. 171 ff.; J.R. Searle, "Libero arbitrio e neurobiologia", in J.R. Searle (ed.), *Libertà e neurobiologìa. Riflessioni sul libero arbitrio, il linguaggio e il potere politico*, Giuffrè, Milan, 2005, p. 31 ff.; O.D. Jones, "Law, evolution and brain: applications and open questions", *Phil. Trans. R. Soc. Lond. B*, 2004, p. 1700 ff.

cur partly below the threshold of awareness, and appear to be significantly influenced by the emotional and cultural component of the individual, as well as by his psychic and genetic framework.[3] In this regard, doctrine has questioned whether and to what extent traditional categories such as imputability and capacity to act can still be considered valid[4]; while some judges, by recognizing reductions in penalties based on the results of genetic and brain-imaging tests carried out on the person of the offender, have shown how revolutionary the consequences of applying cognitive neuroscience in the judicial field can be.[5] It was not long, however, before the issue of the limits to the use of neuroscience and AI to increase the suggestive effectiveness of commercial promotion messages also came to the attention of researchers.[6]

In fact, we have seen that the application of neuroscience and AI to advertising makes it possible to experiment with new persuasion techniques that are particularly subtle and effective, since they are capable of unconsciously stimulating that part of the psyche responsible for making purchasing decisions.[7] These new techniques of

[3] See *supra* notes 1 and 2. But see also C. Cappelletto, *Neuroestetica. L'arte del cervello*, Laterza, Roma-Bari, 2009, p. 5 ff., which says, today, in the context of recent neuroscientific discoveries, it must be affirmed that "rationality as such is emotional, the logical thinking of man who thinks, wants and chooses, is incarnate". These conclusions seem to be inspired by the observations, a few years earlier, of J.P. Changeux, P. Ricoeur, *La natura e la regola. Alle radici del pensiero*, Giuffrè, Milan, 1999, p. 141, they used the expression "neuronal man" to highlight the fact that man, also because of scientific discoveries and the tumultuous development of new technologies, is increasingly reduced to a mere center of imputation of events, with the consequent overcoming of the era of humanism and the advent of the so-called post-humanism. In this regard, in doctrine, see also P. Stanzione, *Biodiritto, postumano e diritti fondamentali*, in *Comparazione e diritto civile. Annali* 2010/2011, edited by P. Stanzione, I, Giappichelli, Turin, 2012, p. 85 ff., and B. Romano, *Fondamentalismo funzionale e nichilismo giuridico. Postumanesimo "noia" globalizzazione*, Torino, 2004, p. 18, he argues that neuroscience, leading to believe that even thought and emotions are the result of mere reactions of brain biochemistry, make man considered as *posthuman*, that is "without subjectivity, deprived of the dimension, creative and not calculable, the being me".

[4] See also M.T. Collica, "Gli sviluppi delle neuroscienze sul giudizio di imputabilità", *Dir. pen. contemp.*, fasc. 20 febbraio 2018; L. Tafaro, *Neuromarketing e tutela del consenso*, cit., p. 44 ff.; A. Santosuosso (ed.), *Neuroscienze e diritto*, cit., p. 11 ff.; S. Moccia, "I nipotini di Lombroso: neuroscienze e genetica nel diritto penale", *Dir. pen. proc.*, 2016, p. 681 ff.; C. Grandi, "Sui rapporti tra neuroscienze e diritto penale", *Riv. it. dir. proc. pen.*, 2014, p. 1249 ff.; L.S. Khosbin - S. Khosbin, "Imaging the mind, Minding the image: an historical introduction to brain imaging and the law", cit., p. 171 ff.; O.D. Jones, "Law, evolution and brain: applications and open questions", cit., p. 1700 ff.

[5] See Corte di Assise di appello of Trieste 1 October 2009, *Dir. e giur.*, 2011, p. 152 ff.; Gip Como 20 August 2011, *Guida al diritto (on line)*, 30 August 2011. In doctrine see I. Merzagora Betsos, "Il colpevole è il cervello: imputabilità, neuroscienze, libero arbitrio: dalla teorizzazione alla realtà", *Riv. it. med. leg*., 2011, p. 175 ff.; M.T. Collica, "Il riconoscimento del ruolo delle neuroscienze nel giudizio di imputabilità", *Dir. pen. contemp*, fasc. 15 February 2012; please also refer to R. Catalano, "Indagini genetiche, imputabilità e libero arbitrio: questioni giurisprudenziali e nuovi esigenze di tutela della persona", in L. Chieffi (ed.), *Bioetica pratica e cause di esclusione sociale*, Mimesis, Milan, 2012, p. 299 ff.

[6] Cfr. L. Tafaro, *Neuromarketing e tutela del consenso*, cit., p. 11 ff.

[7] Cfr. L. Ferrarella, "Neuroscienze e media", *Neuroscienze e diritto*, cit., p. 157 ff.; D. Ariely, G.S. Berns, "Neuromarketing: the hope and the hype of neuroimaging business", *Nature reviews neuroscience*, 2010. In Italy, the case of Thimus is well known. This company uses neuroscientific instruments (ECG, respiratory frequency measurement, electroencephalography, galvanic skin response, brain im-

persuasion, called neuromarketing or emotional marketing arouse in consumers new needs of protection in order to identify the most appropriate tools to deal with them adequately.[8]

2. New Protection Necessities Aroused by the Neuromarketing Phenomenon

In order to define these protection needs, it is useful, as a preliminary step, to explain in more detail the characteristics and practical applications of neuromarketing.

As mentioned, this is a branch of marketing that makes use of neuroscientific techniques aimed at studying and measuring the physiological variations produced by any stimulus, in order to provoke reactions in the individual that can propitiate and/or induce the decision to purchase. It consists of a set of persuasion tools that does not solicit the rational part of the mind of the potential consumer, but operates wholly or partly at an unconscious level and on an emotional level. The neuromarketing therefore aims to transmit to potential buyers of a product or a service a message suitable to induce in them needs and desires, as well as the increase of the propensity to purchase.[9]

The systems used to achieve this result are essentially two[10]: to detect in real time the behaviours and emotions of a single individual to make him reach[11], in a personalized way, the most suitable solicitations to hit him; to address to the public of potential users a uniform message containing stimuli usually suitable to arouse in people, in an unconscious way, a certain type of reaction.[12]

---

aging, etc.) to collect biometric data in order to analyze people's emotional and cognitive reaction to a product or an experience. By means of the electroencephalogram, Thimus records the waves naturally emitted by our brain, including alpha waves that indicate the presence of positive thoughts, serenity and appreciation; therefore, depending on the brain area in which they are detected, it is possible to understand which emotions the experience has aroused. The results of the surveys conducted in this way are then sold to companies interested in creating products in line with the interests or needs of consumers (see R. Travaglini, Thimus, quando la neuroscienza si tuffa nella natura, <www.verticalinnovation.it/it/top-stories/thimus-alto-adige-cervello-consumatori>, 3 June 2016). Along the same lines is the experience of Mazer srl, a start-up from Campania that, in collaboration with the Signal Processing and Communication Research Group of the University of Campania Luigi Vanvitelli, is working on a project aimed at creating a chatbot called Laila, i.e. a robot able to converse with people in chat and understand their emotions, so as to induce them to purchase a product by detecting their reactions in real time (see www.ilmattino.it).

[8] Cfr., tra gli altri, F. Gallucci, *Neuromarketing*, Hoepli, Milano, 2016; A. Saletti, *Neuromarketing e scienze cognitive per vendere di più sul web*, Webbook, Palermo, 2016; V. Russo (ed.), *Neuromarketing, comunicazione e comportamenti di consumo. Principi, strumenti e applicazioni nel food and wine*, Franco Angeli, Milan, 2015; F. Gallucci, *Marketing emozionale e neuroscienze*, Egea, Milan, 2014, p. 9 ff.

[9] Cfr. F. Gallucci, *Marketing emozionale e neuroscienze*, cit., p. 170 ff.; A. Miani, M. Tonielli, G. Virardi, *Il marketing dei sensi*, Lupetti, Milan, 2008, p. 2 ff.

[10] G. Zaffiro, *Neuromarketing: tecnologie e applicazioni*, aprile, 2010 <www.reserchgate.net>, describes some techniques of neuromarketing in use from enterprises.

[11] See the case of Thimus, to which note 7 above has already been devoted, to which we refer here.

[12] F. Gallucci, *Marketing emozionale e neuroscienze*, cit., pp. 170 ff. and 301 ff.

To the first type belong the recent experiments that, thanks to the use of AI, solicit each individual in a different way and depending on the results of the verification of his emotional state implemented by means of the detection of the tone of voice, face, gait or body temperature, web browsing options, etc.[13]. The second type includes, for example, the use of particular smells to scent environments or products; of colours, graphic styles or images for packaging or advertising messages; of sounds or music in the sales area, or to support commercial communication.

In both cases, we are talking about solicitations that are not simply aimed at illustrating and exalting the characteristics of a product or service in order to induce in the consumer a purchasing decision based on the evaluation of the quality or functionality of what is offered. Rather, these are messages which appeal to people's senses and arouse in them positive perceptions and emotions to be associated with the product regardless of its actual consistency. In other words, these messages solicit people's unconscious and emotional sphere to induce them to make a purchasing decision based on motivations that are not entirely rational.

Given the characteristics of neuromarketing, it is evident that it raises peculiar needs of protection in order to

- the processing of personal biometric data for commercial use;
- the correct pre-contractual information of the contracting parties to whom the type of commercial solicitation in question is addressed;
- the integrity of their negotiating intentions;
- the regular functioning of competitive mechanisms in the market segment within which use is made of the persuasive techniques in question.

There are no laws specifically dedicated to the protection of these needs from neuromarketing practices. There are only rules that, even though they do not concern neuromarketing, refer to cases that can be approached in some way to those investigated, so as to suggest new lines of research for the interpreters and intervention for the legislator[14]. Think, for example, of the traditional distinction between *dolus bonus* and *dolus malus* - depending, as we know, on the suitability of the means used to persuade[15] -, which could suggest, also with regard to neuromarketing, the need to distinguish between suggestions not suitable to impress people of normal wisdom, and persuasive techniques capable of misleading them[16]. Or con-

[13] Similar technologies, based on the real-time detection of biological parameters of individuals, are also used at the borders between States in order to prevent crimes; see, F. De Simone, *La prevenzione del crimine alle frontiere 2.0, una questione di dati biometrici,* in this Volume.

[14] L. Tafaro, *Neuromarketing e tutela del consenso*, cit., p. 63 ff., verifies whether and to what extent neuromarketing may represent a new form of aggression against contractual self-determination and evaluates, between rules of conduct and rules of validity, the civil law protections available to consumers.

[15] About *dolus bonus* and *malus* see, *ex multis*, C.M. Bianca, *Diritto civile*, 3, *Il contratto*, Giuffrè, Milano, 2000, p. 666 ff.; F. Criscuoli, "Il criterio discretivo tra dolus bonus e dolus malus", *Annali del Seminario giuridico della Università di Palermo*, XXVI, Palermo, 1957, p. 5 ff. See more G. Amadio, F. Macario (ed.), *Diritto civile. Norme, questioni, concetti, I, Parte generale*, Il Mulino, Bologna, 2014, p. 826 ff.

[16] If, in the future, persuasive techniques capable of coercing the will of individuals, similar to

sider the rules on unfair commercial practices, within which it would seem possible to include some manifestations of the persuasive techniques under consideration.[17] Or, finally, consider the discipline on competitive offences, which concerns conduct that can also be carried out by means of neuromarketing techniques.[18]

Here it is not possible to investigate all these issues both for their obvious complexity and because, probably, it would be a premature investigation. In fact, neuromarketing, as well as being born a few years ago, is evolving rapidly in dependence of the continuous progress of cognitive neuroscience and AItechnologies. Therefore, an analysis that aims, today, to identify legal actions to protect needs listed above, would risk coming to provisional results because they are subject to the tumultuous evolution of neuroscientific discoveries and AI technologies.

Nonetheless, in relation to the broad field of investigation outlined above, some more solid observations can be made regarding the protection of biometric personal data used for commercial purposes. In fact, in Italy, as in Europe, there is a recently updated regulation on the processing of biometric data that takes into account the latest technological advances and that, therefore, is suitable to offer several useful hints to the interpreter.

3. Current Legislation on the Processing of Biometric Personal Data

The regulatory context that we propose to analyse is rich in profiles relevant to the phenomenon of neuromarketing. It is mainly composed of provisions of the General Data Protection Regulation EU/2016/679 (GDPR), and of the legislative act August 10, 2018, no. 101, containing rules for the adaptation of the national discipline to the provisions contained in the aforementioned Regulation.[19]

---

hypnosis, were to emerge, it could be assumed that contracts concluded in this way would be null and void, similar to what happens in cases of absolute violence, traditionally defined as "material coercion that completely excludes the will of the subject with regard to the contract" C.M. Bianca, *Diritto civile, 3, Il contratto*, cit., p. 658.

[17] L. Tafaro, *Neuromarketing e tutela del consenso*, cit., pp. 77 ff. and 128 ff. About the rules on unfair commercial practices see F. DE Cristofaro (ed.), *Pratiche commerciali scorrette e Codice del consumo*, Giappichelli, Turin, 2008; F. DE Cristofaro, *Pratiche commerciali scorrette* (Voce), in *Enc. Dir.*, *Annali*, Giuffrè, Milano, 2009; F. DE Cristofaro, *Le conseguenze privatistiche della violazione del divieto di pratiche commerciali sleali: analisi comparata delle soluzioni accolte nei diritti nazionali dei Paesi UE,* in *Rass. diritto civile*, 2010, p. 880 s.; F. Di Cataldo, "Pratiche commerciali scorrette e sistemi di enforcement", *Giur. comm.*, 2011, p. 803 ff.; G. Grisi, "Rapporto di consumo e pratiche commerciali sleali", *Europa e dir. priv.*, 2013, p. 1 ff.; G. Marino, "Scorrettezza della pratica ed abusività della clausola nella disciplina del contratto del consumatore", *Contr. impr./Europa*, 2014, p. 137 ff.; G. Scognamiglio, "Le pratiche commerciali scorrette: disciplina dell'atto o dell'attività?", *Federalismi.it*, n. 19, 20 october 2010.

[18] See among others, F. Di Cataldo, "Pratiche commerciali scorrette e sistemi di enforcement", cit., p. 803 ff.

[19] About UE Reg. cf. F. Di Resta, *La nuova "privacy europea"*, Turin, 2018, p. 54 ff. About d.lgs. n. 101/2018 cf. V. Cuffaro, "Quel che resta di un codice: il d.lgs. 10 agosto 2018, n. 101, detta le disposizioni di adeguamento del Codice della privacy al Regolamento sulla protezione dei dati", *Corr. giur.*, 2018, p. 1181 ff.

The Regulation starts from the premise that biometric data are particularly sensitive from the point of view of fundamental rights and freedoms, since the context of their processing could create significant risks for fundamental rights and freedoms; they therefore should not be processed, unless processing is permitted in the specific cases referred to in this Regulation (51st recital). For the same reason, processing, where permitted, must be surrounded by specific security measures and be preceded by an "impact assessment" carried out in order to evaluate the particular probability and seriousness of the risk, taking into account the nature, scope, context and purpose of the processing and the sources of the risk. The impact assessment should address, in particular, the measures, safeguards and mechanisms provided to mitigate that risk while ensuring the protection of personal data and demonstrating compliance with this Regulation (91st recital).

Consistent with these premises, Article 9(4) of the GDPR prohibits the processing of genetic and biometric data intended to uniquely identify an individual, except where the data subject has consented, or the processing is necessary for compliance with a legal obligation or a task in the public interest (para. 2).[20] The provision also states that the processing must be proportionate to the purpose pursued, and respect the essence of the right to protection of personal data (particularly the principles established by art. 5) and security measures.

Article 22 of Regulation no. 679 specifies that the data subject has the right not to be subjected to "automated processing, including profiling", unless he/she has expressly consented to it[21]; while Articles 35 and 36 require prior impact assessment for processing operations which, like those under consideration, entail high risks for the rights and freedoms of individuals and the consequent prior consultation of the supervisory authority, which may impose the adoption of specific measures to mitigate the risk.

That said, the GDPR still allows member states to introduce additional and/or more restrictive conditions and limitations. In addition, Article 51 provides for the establishment of a Supervisory Authority in each member state to ensure the application of European standards.

---

[20] The Regulation was adopted by the Parliament and the Council on April 27, 2016. It repealed the former Directive 95/46/EC and provided that processing operations in progress on the date of its entry into force had to be adapted to the new rules within two years, i.e., by May 25, 2018. On the other hand, it has provided that the decisions of the Commission and the authorizations of the supervisory authorities adopted on the basis of Directive 95/46/EC shall remain in force until any new intervention aimed at amending, replacing or repealing them. In doctrine, in this regard, cf. F. Bravo, "Sul bilanciamento proporzionale dei diritti e delle libertà 'fondamentali', tra mercato e persona: nuovi assetti nell'ordinamento europeo?", *Contr. impr*., 2018, p. 190 ff.; E. Lucchini Guastalla, *Il nuovo Regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, *ivi*, 2018, p. 106 ff.; A. Mantelero, "Responsabilità e rischio nel Reg. UE 2016/679, *Nuove leggi civ. comm.*, 2017, p. 144 ff.; G. Granieri, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, *ivi*, p. 165 ff.

[21] Pursuant to Article 4(4) of EU Reg. 2016/679, profiling means "any form of automated processing of personal data consisting of the use of such personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects of that natural person's professional performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements". About profiling see C. Perlingieri, "La tutela dei minori di età nei 'social networks'", *Rass dir. civ.*, 2016, p. 1324 ff.

In order to comply with this provision and to harmonize the previous national discipline with that dictated by the Regulation, the Italian legislator approved Legislative Decree no. 101/2018. This decree clarified that the Supervisory Authority referred to in Article 51 of the Regulation is to be identified in the already existing Guarantor for the protection of personal data (art. 2, paragraph 1, letter e, introducing art. 2 bis in the Code for the Protection of Personal Data), and that in Italy the discipline of the processing of personal data has its source in the rules of the EU Regulation no. 679/2016 and in the Code for the Protection of Personal Data (Legislative Decree no. 196 of June 30, 2003) as amended by the same Legislative Decree no. 101/2018 in adaptation to the GDPR.

In effect, as far as the present investigation is concerned, it is worth recalling that the Italian Code for the Protection of Personal Data (Privacy Code), in a manner not dissimilar to the European Regulation of 2016 and since before its issuance, recognized that the mechanisms normally placed to guard the regularity of the processing of personal data are insufficient with respect to "data other than sensitive and judicial data, which present specific risks for the fundamental rights and freedoms, as well as for the dignity of the data subject, in relation to the nature of the data and the methods of processing or the effects that it may determine". Therefore, it established that, in order to process this kind of data, in addition to the consent of the owner and the notification to the Authority (art. 37, Privacy Code), a preliminary verification by the Guarantor was required in order to provide for any additional measures and precautions. In addition, the Italian Guarantor for the protection of personal data with Annex A of the General Prescriptive Measure on the subject of biometrics No. 513 of November 12, 2014, amended by Measure of January 15, 2015, made in implementation of EU Regulation No. 910/2014, dictated Guidelines on the subject of biometric recognition and graphometric signature.

Given this regulatory framework, Legislative Decree no. 101/2018 - in art. 2, co. 1, lett. e - deemed it possible to achieve the result of the harmonization of the internal discipline with the European one by making some changes and additions to the Privacy Code. In particular, art. 2 septies of the decree of 2018, headed *Guarantee measures for the processing of genetic, biometric and health-related data*, reiterates the general prohibition of processing enshrined in art. 9, par. 4, of the European Regulation. In these cases, the treatment becomes possible, but must be carried out in compliance with the safeguards imposed by the Guarantor, updated every two years (art. 2 septies, para. 1) after public consultation (art. 2 septies, para. 3).

It is assigned to the Supervisory Authority the task of defining the security measures and any additional conditions to be met for the various categories of personal data and for different purposes of treatment. He will have to identify the security measures, including the technical measures of encryption and pseudonymisation, the measures of minimisation, the specific modalities for the selective access to the data and for rendering the information to the data subjects, as well as any other measures necessary to guarantee the rights of the data subjects" (art. 9 septies, co. 5). In doing so, the Supervisory will take into account "the guidelines, recommendations and best practices published by the European Committee for Data Protec-

tion and best practices regarding the processing of personal data", "scientific and technological developments in the field covered by the measures" and "the interest in the free movement of personal data within the territory of the European Union" (art. 9 septies, co. 2).

Special provisions and precautions are established, then, for the processing of genetic or biometric data in the health sector (art. 2 septies, para. 6 and para. 4, lett. b and d) or to select the physical or logical access of authorized persons (art. 2 septies, para. 7).

At present, the Supervisory has not yet defined, with its own measure, the guarantee measures for the processing of biometric data. Therefore, in order to initiate this type of processing, it is necessary to comply with the following obligations, which can be deduced from the GDPR, from Legislative Decree no. 101/2018 and from the previous discipline:

- to acquire in advance the consent of the interested party, as a result of information containing the mention of the purpose of the acquisition of the information and the provisions of Articles 9 and 12 et seq. of the EU Reg./2016/679;
- process the data in compliance with the purpose stated in the informative report, or for other operations compatible with it (art. 6 of Reg. UE/2016/679);
- in the event that systems used are potentially suitable for the detection of biometric data without the cooperation of the data subject (as may be the case in some cases of facial or voice recognition), inform the latter, giving him/her the opportunity to choose whether or not to access the area subject to biometric controls (art. 4.5.1 Guidelines on biometric recognition and graphometric signature, Provv. Authority no. 513 of 2014). The information may be provided by means of appropriate signage in proximity to the areas subject to biometric detection, or may be provided by other means prior to the interaction of the data subject with the biometric system (e.g., voice recognition via telephone preceded by a warning) (art. 4.5.1 of the Guidelines)[22];
- in cases where the processing is carried out in synergy with another system (e.g. video surveillance), the information must be clear and appropriate to the means used (art. 4.5.1 of the Guidelines);
- in any case, the processing must be preceded by an impact assessment and prior consultation with the supervisory authority which, during the verification, may prescribe special precautions and security measures (Articles 35 and 36 Reg. UE/2016/679 and 2 septies d.lgs. n. 101/2018).

4. Neuromarketing and Commercial Processing of Biometric Data

The Italian and European laws just examined do not dictate rules specifically dedicated to the acquisition and processing of biometric data for commercial pro-

[22] On the use of video surveillance, see also the Guidelines of the European Data Protection Board, No. 3/2019, adopted on January 29, 2020, dealing with the processing of personal data through video devices.

motion purposes. It should be noted, however, that their scope of application is so broad that it also includes cases of biometric processing for neuromarketing purposes. To confirm this, it is sufficient to consider that Article 4(4) of Regulation EU/2016/679 extends the notion of "profiling" to include any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, in particular in order to analyse and predict aspects relating to the professional performance the economic situation, health, personal preferences, interests, reliability, behaviour the location or movements of that natural person; and that the subsequent no. 14 defines biometric data as personal data relating to hereditary or acquired genetic characteristics of a natural person which enable or confirm their unambiguous identification, such as facial image or dactyloscopic data.

To the affirmation according to which the field of application of the aforesaid laws is so ample as to also include the activities of neuromarketing carried out through biometric treatments, it can be objected that art. 9 of the European Regulation refers only to biometric data "intended to uniquely identify a person"; so that the protections provided therein would not apply to treatments aimed at commercial promotion, but only to those aimed at the univocal identification of persons (in order, for example, to regulate the access to a physical or logical space).[23]

This objection, however, is not convincing. First of all, because the result is that - unreasonable and incompatible with the ratio of Regulation 679 - to subject groups of personal data substantially coinciding to a different legal regime. Moreover, this objection is not persuasive because the phrase "intended to uniquely identify a person" does not seem to be aimed at limiting the scope of application of art. 9 only to treatments characterized by identification purposes, but rather to define the nature of the data considered. More precisely, with the phrase in question, art. 9, as does art. 4, n. 14, intends to clarify that biometric data, like genetic data, are distinguished from other personal data by their ability to identify each person in an unrepeatable way.[24]

In confirmation of this, it should be noted - and the observation seems decisive - that the criticized interpretation is incompatible with the dictate of art. 2 septies of the Privacy Code introduced by Legislative Decree no. 101/2018, since this rule, in addition to covering the processing of biometric data aimed at selecting the access of persons to physical or logical spaces (hypothesis expressly provided by co. 7), also refers to other types of treatment in which the detection of biometric data does not necessarily occur in order to identify and select individuals (see, in particular,

[23] In this sense, the Supervisory Authority for Privacy ruled on July 26, 2017 in the Preliminary Verification. Recognition via webcam of participants in live streaming training courses, which can be consulted in garanteprivacy.it, rendered, however, in accordance with the regulations prior to the GDPR.

[24] F. Di Resta, *La nuova "privacy europea"*, cit., p. 54 ff. correctly observes that the category of biometric data is characterized by its univocality and tendency to permanence; therefore, it includes, in addition to the information that permanently connotes a person throughout his existence (such as, for example, fingerprints or the structure of the ocular iris or retina), also those that can be associated with the person for more or less long periods of his life (for example, handwritten signature, body odor, gait).

paragraphs 4 and 5). It follows that the rules dictated on the subject of biometric data apply to all treatments that have them as their object, independently of their finality.

As a consequence of what has been observed, it must therefore be affirmed that also the treatments for commercial purposes are subject to the general discipline on the protection of biometric data. Also for them, therefore, are valid all the cautions examined previously, imposed with the purpose of reducing within tolerable limits the risks that derive from them.

Of these precautions, the instrument of case-by-case evaluation by the supervisory authority (Art. 36 of the European Regulation) appears today to be the most appropriate.[25] This is because neuromarketing is still at an early stage and, as it manifests itself in very heterogeneous ways, makes it difficult for the legislator to devise specific protective measures. The fact remains that the current discipline presents margins for improvement; margins that are destined to increase as a consequence of the progress of AI technologies and cognitive neuroscience.

5. The New Frontiers Created by Developments in Cognitive Neuroscience and Studies on AI

From this perspective, the laws currently in force can serve as a test bench on which to verify whether and to what extent the instruments of protection currently known are suitable to deal with the new needs of protection aroused by neuromarketing. Therefore, the lack of a specific discipline on neuromarketing at least has the advantage of allowing the selection of the instruments of protection on which to focus *de iure condendo*.[26] Moreover, developments in research on the mechanisms that allow our brain to process and make decisions, could make it necessary to revise the traditional way of understanding traditional categories such as the capacity to act and the will to negotiate. This is all the more so since the progress of studies on robotics and AI makes it necessary to redefine the borderline between the latter and human intelligence.[27]

---

[25] These decisions can be found at www.garanteprivacy.it. See, for example, the Authority's decision of February 16, 2017, no. 60, concerning the preliminary verification of a biometric-facial access control system, which allowed the processing by prescribing special precautions; or the decision of July 13, 2016, no. 306, concerning the preliminary verification of targeted advertising spots, which also allowed the processing but imposed the adoption of specific precautions.

[26] For a vision of consumer law as a point of emergence and a means of guaranteeing fundamental liberties and social rights see A. Barba, *Consumo e sviluppo della persona*, Giappichelli, Turin, 2017, p. 10 ff.

[27] As is well known, the European Parliament on February 16, 2017 passed a Resolution with recommendations to the Commission on civil law rules on robotics (2015/2013 INL). In doctrine, on the topic of civil law of robotics see, among others C. Perlingieri, "L'incidenza dell'utilizzazione della tecnologie robotica nei rapporti civilistici", in *Rass. dir. civ.*, 2015, p. 1235 ff.; E. Palmerini, "Robotica e diritto: suggestioni, interserzioni, sviluppi a margine di una ricerca europea", in *Resp. civ. prev.*, 2016, p. 1816 ff.; F. Parente, *Dalla persona biogiuridica alla persona neuronale e cybernetica*, ESI, Naples, 2018, p. 68 ff.

Such arduous and complex tasks cannot be carried out by means of the jurist's tools alone. The scientific and technological progress imposes a radical change of perspective because it makes clear that man, in order to govern increasingly complex systems and tools, must get used to an interdisciplinary approach, implemented through the comparison and sharing of the results of different researches and reflections, such as those of the jurist, the bioethicist, the philosopher, the doctor and the scientist. In the absence of this, human intelligence is likely to be overtaken by AI because the latter, being able to process in a short time a huge amount of information, can easily combine the results of different knowledge, ending up being more efficient and competitive.[28]

From this perspective, the modern tendency, also legislative, to give an increasingly important role to the Codes of Ethics of the category or to the Ethics Committees in an advisory capacity, is certainly worthy of support.[29] Both of these instruments, in fact, since they are realized with the contribution and/or participation of experts from different disciplines, constitute a privileged place of experimentation of new methods of study and work for the elaboration of rules and solutions suitable to govern complex and rapidly evolving phenomena. In this direction, in fact, is also oriented the Privacy Code which includes seven annexes containing as many deontological codes of conduct of the category and which, by means of the general provision of art. 2 quater, 154, lett c, and 154 bis, lett. b, imposes on the Supervisory the task of promoting and approving further deontological rules.

More perplexing, however, is the thesis according to which the gap between human and AI can be bridged thanks to the progress of science and, precisely, to the results of those medical and pharmacological researches aimed at enhancing the physical and / or cognitive abilities of people (so-called human enhancement).[30] The questions arise from the consideration that the road of enhancement can be very risky, since it implies the same problems of discrimination and generalized control of the masses aroused by the processing of biometric data, as well as further significant dangers to the physical and mental health of people.[31]

---

[28] R. Kurzweil, *La singolarità è vicina*, Apogeo Education, Milan, 2008, p. 197 ff., an American computer scientist and inventor, argues that our future will be profoundly marked by advances in genetics, robotics and nanotechnology, which will allow us to redesign and reconstruct, molecule by molecule, our bodies, our brains and the way we interact, as well as to create robots capable of exceeding the performance of human intelligence.

[29] See by P. Fabbio, "*I codici di condotta nella disciplina delle pratiche commerciali sleali*", *Giur. comm.*, 2008, I, p. 706 ff., e di F. Ghezzi, "*Codici di condotta, autodisciplina, pratiche commerciali scorrette. Un rapporto difficile*", *Riv. soc.*, 2011, I, p. 680 ff. In jurisprudence cf. TAR Lazio, sez. I, 24 dicembre 2011, n. 10185, <*www.gadit.it* >.

[30] Among the most convinced supporters of human enhancement is R. Bailey, "*The Right to Human Enhancement and also uplifting animals and the rapture of the nerds", 2 june 2006,* <www.reason.com> *see more J. Sirius, "The NeuroAge: Zack Lynch in conversation with R.U. Sirius", Life Enhancement, 2005,* <www.life-enhancement.com/neofiles. >.

[31] On the risks of enhancement see, among others, C. Donisi, "Tecnoscienze, human enhancement e scopi della medicina", in C. Buccelli and C. Casella (eds.), *Ricerche di biodiritto*, edited by C. Buccelli and C. Casella, ESI, Naples, 2020, 109 ff.; S. Amato, "Neuroscienze e utilizzazione militare delle tecniche di potenziamento umano", in *Etica & politica*, 2014, 2, p. 182 ff. and also the National Bioe-

In conclusion, many of the issues examined remain open. This is not necessarily a bad thing, since their extreme complexity and delicacy, together with the speed with which scientific and technological research is evolving, suggest a critical and prudent approach. There is no doubt, however, that these are questions to which increasing attention must be paid since, as emerges from the observations made so far, it is also on these issues that the difficult match between technological progress and the guarantee of the fundamental rights of the human person will be played out in the future.[32]

thics Committee has issued two opinions on the subject: *Neuroscienze e potenziamento cognitivo farmacologico: profili bioetici*, del 22 febbraio 2013, and *Diritti umani, etica medica e tecnologie di potenziamento (enhancement) in ambito militare*, del 13 marzo 2013, <*www.governo.it/bioetica* >.

[32] Several predictive studies, published by Italian and foreign experts, strive to demonstrate that the concentration of the processing of personal data, especially if biometric or genetic, in the head of a few large corporations (such as, for example, Google, Amazon, Apple) creates the conditions for an involution of society and for the establishment of a true digital dictatorship. This is because these data lend themselves well to be used - even by means of persuasive techniques of neuromarketing - to control and manipulate the masses. Particularly effective and worrying is the analysis carried out by historian Y.N. Harari *in the world best seller Sapiens. A brief history of humankind*, London, 2014, published in Italy by Bompiani with the title *Sapiens. Da animali a dei. Breve storia dell'umanità*, Milan, 2014. On the subject, with particular regard to the pandemic emergency, please refer to R. Catalano, *Pandemic and Panopticon: evolutionary profiles of the right to the protection of personal data*, being published in a volume edited by L. Chieffi per il CIRB (Centro Interuniversitario per la Ricerca Bioetica), Mimesis, Milan, 2021.

THE HUMANITARIAN ORGANISATIONS AND THE USE OF THE CYBER TOOLS DURING ARMED CONFLICTS

Caroline Cornella

1. Introduction

"As humanitarian organizations become more active in and reliant upon new technologies and the digital domain, they evolve from simple bystanders to full-fledged stakeholders in cyberspace – able to build on the advantages of new technologies but also vulnerable to adverse cyber operations that could impact their capacity to protect and assist people affected by violence or armed conflict".[1] These words illustrate both the current need and the threat around the matter of cyber tools used during armed conflicts. The recent pandemic highlighted[2] the uncompressible need of cyber-safety for humanitarians. Whether at a time of peace or during an armed conflict, it is of a peculiar importance for health workers and the general population. At the heart of this lies the significance of this issue that resulted in several new reflections.[3]

Assuming that cyber tools will become the go-to means and methods for warfare,[4] legal work is required to address the various challenges that civilians and the humanitarian workers will face during an armed conflict. Instead of going for the

---

[1] M. Marelli, "Hacking Humanitarians: Moving towards a Humanitarian Cybersecurity Strategy", *ICRC Blog Humanitarian Law and Policy*, 16 January 2020, <https://blogs.icrc.org/law-and-policy/2020/01/16/hacking-humanitarians-cybersecurity-strategy/> (03/21).

[2] See: The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector, 21 May 2020; The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research, 7 August 2020, *Oxford Institute For Ethics Law and Armed Conflict*, <https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea#/> (03/21). See also the Declaration by the High Representative Josep Borrell, on behalf of the European Union, on Malicious Cyber Activities Exploiting the Coronavirus Pandemic, 30 April 2020, *Council of the European Union Press Releases*, <https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/> (03/21).

[3] For a recent illustration, the new International Review of the Red Cross, dedicated to cyber risks illustrates this current and important subject. At the time this article was proposed, the review was not yet published. But some of the main questions and proposals of this article can be find and detailed in this review: *International Review of the Red Cross*, *Digital Technologies and War*, n° 913, vol. 102, March 2021, p. 509.

[4] In a broad sense, cyber means and methods of warfare are "the [cyber] tools of war and the ways in which they are used", K. Lawand, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare Measures to Implement Article 36 of Additional Protocol I of 1977,* International Committee of the Red Cross, Geneva, January 2006 (revised in November 2006), p. 3, note 1.

restrictive and well-known mindset that new technology only equals to danger, we must consider cyber tools in a different light. Indeed, "negative presumptions"[5] should not be accepted as the only possible way to discuss and address these challenges. Cyber tools are innovative solutions. They can be view as "tech for good"[6], not only for the military field, but also for humanitarian actors. The classic opposition between an old International Humanitarian Law (IHL) and a new technology rekindles a dangerous cocktail. It is also a natural opportunity for humanitarians and jurists to study and adjust humanitarian protections and standards to this innovation.

If humanitarian organisations generally include "the International Committee of the Red Cross [ICRC] or any other impartial humanitarian organization"[7], that does not illustrate their numerous activities and the variety of principles[8] that dictate their operations. However, humanitarian's actions are often taking place in perilous contexts of "international armed conflicts, opposing two or more States, and non-international armed conflicts, between governmental forces and nongovernmental armed groups, or between such groups only".[9] The perpetual strategic and military thinking, joined to technological research and the evolution of the armed conflict, need (even, dictate) a systematic renewal of humanitarian solutions. At the same time, IHL must be seen for what it is: "a set of rules which seek, for humanitarian reasons, to limit the effects of armed conflict. It protects people who are not or are no longer participating in the hostilities and restricts the means and methods of warfare".[10] Even if IHL might be seen as an antique, it still has an efficient set of rules

[5] Col. G. P. Corn, "The Potential Human Costs of Eschewing Cyber Operations", *ICRC Blog Humanitarian Law and Policy*, 31 May 2019, <https://blogs.icrc.org/law-and-policy/2019/05/31/potential-human-costs-eschewing-cyber-operations/> (03/21).

[6] Literally, the technology for the purpose of the good. Cyber Tech for good can be broadly defined as "the positive impact [and use] of the tech and digital revolution in the service of human progress [and good of mankind]", *The Tech for Good Call*, 2018, <https://www.techforgood.international/en/tech-for-good-call> (03/21).

[7] Art. 9 of the First Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (GC I), Art. 9 of the Second Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (GC II), Art. 9 of the Third Geneva Convention relative to the Treatment of Prisoners of War (GC III) and Art. 10 of the Fourth Geneva Convention relative to the Protection of Civilian Persons in Time of War (GC IV), Geneva, 12 August 1949, entered into force 21 October 1950. As underlined by the Commentaries to the above-mentioned Conventions and to the First Additional Protocol, the non-State bodies – international or non-international – must therefore by their very nature but also in their activities fulfil with the conditions of *humanity* and *impartiality*. For further information, see: E. David, "Les fondements normatifs de l'assistance humanitaire dans le cadre des conflits armés", in S. Szurek, M. Eudes and P. Ryfman (Dir.), *Droit et pratique de l'action humanitaire*, LGDJ-Lextenso, Issy-Les-Moulineaux, 2019, pp. 175-187.

[8] See, *infra* note 66.

[9] International Committee of the Red Cross, "How is the Term "Armed Conflict" Defined in International Humanitarian Law?", Opinion Paper, March 2008, <https://www.icrc.org/en/doc/assets/files/other/opinion-paper-armed-conflict.pdf> (03/21).

[10] International Committee of the Red Cross, Advisory Service on Humanitarian Law, "What is international humanitarian law?", 2014, p. 1, <https://www.icrc.org/en/document/what-international-humanitarian-law> (03/21).

for humanitarian workers and protected persons. In this scenario, the humanitarian sector may integrate cyber tools.

For the purpose of this article, and due to the lack of a universally accepted definition of cyber operations[11] or cyberspace,[12] we will use the neutral word of "cyber tools". In a broad sense, cyber tools are offensive, defensive or humanitarian digital capacities, used for military or non-military purposes and actions, created for, integrated, used or intended to use during an armed conflict (international or not).

This combination of opportunities and unexpected risks for all the entities involved in an armed conflict have been the driving force behind a global discussion on "cyber". Since there is no doubt concerning the application of international law, specifically IHL, it is the scrutiny and interpretation of the latter that still raise questions regarding expected long-term use. In this perspective, the introduction of cyber tools must also be borne by humanitarians: cyber technology brings with it new parameters and uncertainties which need deciphering by all actors – including humanitarians.

In times of war, cyber tools can be a destabilising factor or a catalyst for persistent humanitarian problems. Legal and ethical progresses must be made and analysed both by reading the protections offered by the law, but also by analysing concrete actions provided by humanitarian organisations. It is, therefore, crucial to understand the extent of the implications of using cyber tools, their risks as well as their benefits for humanitarian action. Ultimately, this will help to answer the important question of whether humanitarian action and IHL should be renewed by a modernising approach based on cyber tools.

Exploring the interactions between cyber tools and humanitarian agencies involves analysing a dual-security position. In a classical approach, humanitarian actions and principles must and will have to face cyber challenges in order to respond to a growing humanitarian demand.[13] But humanitarian organisations also have an interest in taking advantage of technological opportunities, in this "tech for good" approach.[14]

2. The Humanitarian Actions and Principles Facing Cyber Tools: an Increased but Well-Known Complexity of the Humanitarian Mission

The question of disastrous humanitarian consequences is a central concern for humanitarian organisations. For several years, experts have been analysing whether

[11] For the Tallinn Manual 2.0 International Group of Experts, cyberoperations may be defined as "[t]he employment of cyber capabilities to achieve objectives in or through cyberspace", M. N. Schmitt (Ed.), CCD-COE*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017, p. 564.

[12] According to the Experts' definition, cyberspace is "[t]he environment formed by physical and non-physical components to store, modify, and exchange data using computer networks", *Ibid*.

[13] See para. 2.

[14] See para. 3.

cyber tools generate more risks for humanitarians, assets and people on which humanitarian aid relies. The question is not so much whether the risks exist, but whether the concentration of old risks and dilemmas experienced by organisations will have to be accommodated by new ones.[15] Accommodating, adjusting or rethinking challenges on a digital battlefield will therefore involve a solution-oriented effort and the integration of new legal and humanitarian perspectives.[16]

2.1. Cyber Risks: a New Spin on Old Legal and Practical Dilemmas for Humanitarian Organisations

From a humanitarian perspective, belligerents-used cyber tools have to be analysed for their unique characteristics and all the ways they can be used. They could significantly increase the actual dangers or even create new ones. The use of cyber tools must also take into account the risks for the humanitarian agencies, their staff and assets, the beneficiaries of the aid, and finally, the humanitarian mission itself. A growing concern about the negative effects on impartial humanitarian agencies assisting people during armed conflict seems to be emerging. This concern rests on the singularities and freedom offered by and in cyberspace. In doing so, it points out that cyber military operations raised a concentrate of legal and practical dilemmas i.e. a combination of identical or exacerbated risks and challenges.

Firstly, cyber tools used during armed conflicts do not necessarily change the fact that IHL casualties and violations occur. But this is an opportunity to reaffirm that "cyber operations during armed conflict are regulated, and therefore restricted, by existing rules of international humanitarian law".[17] Thus, it encompasses the prohibition of attacks against both civilians and objects, as well as medical devices and people.[18] Unfortunately, even if forbidden, civilians and humanitarian workers – who have a special protection under IHL – are targeted as well as civilian objects. Cyber does not change that. We must consider that the world digitalisation (with cyber-dependency and an architecture of interconnected networks) and the dual-use

[15] See para. 2.1.

[16] See para. 2.2.

[17] International Committee of the Red Cross, *Norms for Responsible State Behaviour on Cyber Operations Should Build on International Law*, Statement to the United Nations open-ended working group on developments in the field of information and telecommunications in the context of international security, Second substantive session, 11 February 2020, <https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law> (03/21).

[18] For a concise *exposé* of this rules: *Ibid.* IHL prohibits direct attack (whether cyber or kinetic) against civilian objects: Arts. 48, 51 and 52, Additional Protocol I to the Geneva Conventions of 12 August 1949 relating to the Protection of Victims of International Armed Conflicts, 8 June 1977, entered into force 7 December 1978 (AP I). It also prohibits direct attack against the humanitarian sector, like medical structures: respectively, Arts. 19, 12 and 18 GC IV, Art. 12 AP I and Art. 11 of the Additional Protocol II to the Geneva Conventions of 12 August 1949 relating to relating to the Protection of Victims of Non-International Armed Conflicts, 8 June 1977, entered into force 7 December 1978 (AP II).

of cyber tools, for military, civil and essential services purposes, create greater risks for the civilians and their objects.[19] Often highlighted, some category of specific objects, like objects indispensable to the survival of the civilian population[20] such electric installations;[21] works and installations containing dangerous forces[22] such as nuclear electrical generating stations[23] have already experienced cyber events. From a practical point of view, such acts on these infrastructures have and will have harmful consequences on civilians, but also on the capacity of the humanitarian mission to respond effectively. In this space, the freedom of action as well as the increasing use of cyber tools make the risks of violations and casualties all the more worrying. At the same time and as previously mentioned, the increasing number of cyber intentional incidents during the recent pandemic crisis, against hospitals and other healthcare facilities also contribute to alert the international community. The sector must be protected at all times. If this is not the case, the consequences would be devastating.[24] Initial debates about the potential for a war without death or physical damage should be strongly reconsidered.[25] The dual use of cyber, coupled with

[19] See S. Caltagirone, "Industrial Cyber Attacks: A Humanitarian Crisis in the Making", *ICRC Blog Humanitarian law and Policy*, 3 December 2019, <https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/> (03/21). The author discusses about the crowing digitalisation of industrial control systems and, consequently, the increase risk of cyber disruption or damages. For him, "[w]ith increasing connectivity and the proliferation of malware and knowledge, all of this is at risk of cyber attacks. Without these industrial systems, millions or more may suffer from the lack of medical care, food, drinking water, or heating during winter and cooling during summer. It is a humanitarian imperative to protect these systems from disruption and to protect human life".

[20] Art. 54 AP I; Art. 14 AP II; Rule 54 of the ICRC's Study on Customary International Humanitarian Law, 2015, *IHL Database*, <https://ihl-databases.icrc.org/customary-ihl/fre/print/v1_rul_rule54> (03/21).

[21] For example, the 2016 attack of an electric power grid in Ukraine, named "Industroyer" or "Crash Override", A. Greenberg, " 'Crash Override': The Malware That Took Down a Power Grid", *Wired Journal*, 6 December 2017, <https://www.wired.com/story/crash-override-malware/power grid Ukraine> (03/21).

[22] Art. 56 AP I; Art. 15 AP II; Rule 42 of the ICRC's Study on Customary International Humanitarian Law, 2015. Such works and installations include "dams, dykes and nuclear electrical generating stations, and other installations located at or in their vicinity".

[23] The 2012 Stuxnet cyberattack (even, a nuclear enrichment facility and not an electrical station) has been see as a case study because of this sophistication and the physical damages.

[24] For this reason and while citing the recent ICRC proposal for a new norm of responsible State behaviour, Mačák, Gisel and Rodenhäuser "hope that this crisis will create the necessary impetus for the international community to reaffirm, in an unequivocal manner, that international law comprehensively prohibits cyber operations against medical services not only in times of war, but at all times", K. Mačák, L. Gisel and T. Rodenhäuser, "Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong Are International Law Protections?", *Just Security,* 27 March 2020, <https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-thecovid-19-pandemic-how-strong-are-international-law-protections/> (03/21).

[25] For example, a German hospital reported an indirect death (i.e. resulting from treatment delays) after a ransomware attack: M. Eddy and N. Perlroth, "Cyber Attack Suspected in German Woman's Death", *New York Times*, 18 September 2020, <https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html> (03/21).

the increasing interconnectedness of networks, seems to bring the potential for large-scale effects - which could entail additional risks to people. These could therefore make it even more difficult to provide humanitarian aid and assistance.

Secondly, it is thus important to consider the introduction of cyber tools with the difficult compliance with IHL's fundamental principles. Many studies have already demonstrated the difficulty of complying with the principles of distinction, proportionality or precaution.[26] Under the banner of "new technology" generally emerges a legal opportunity to remind these essential principles and usually alarms the future user about the dangers. With cyber tools, these practical and guiding principles can be extremely difficult to apprehend, especially in a new non-tangible and dual environment. Without it, we can easily expect that humanitarian organisations – which benefit from these principles for themselves and, for the general perspective of assisting and helping the civilian population – will broadly suffer from frequent violations.

Finally and in direct connection with the IHL provisions, these risks and challenges may be multiplied by the anonymity, rapidity and potential reuse of cyber tools. As regards the latter characteristic, the fact that cyber tools can be disseminated and reused, by multiple individuals or entities (e.g. armed group, State-army) for different goals with or without significant modifications, adds additional concerns to the respect of IHL. Furthermore, the velocity of action in the cyber domain and the ability for users to hide themselves can cause substantial difficulties and can be as well seen like new dangers to the application and respect of IHL due to the attribution problem and the difficult responsibility which may result therefrom.[27] From a humanitarian perspective, these growing dangers are challenging if freedom in cyberspace became synonymous with repeated violations or impunity.

Humanitarian organisations need to anticipate these aggravating factors to fully understand the needs and be able to effectively react. For this reason, some speeches mention proposals for technical safeguards (e. g. the segregation from Internet of certain civil infrastructures[28] or the creation of a "humanitarian cloud"[29] and even

[26] See for ex.: M. N. Schmitt (Ed.), CCD-COE, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013, 215 p.; ID., CCD-COE, *Tallinn Manual 2.0*, *supra* note 11; C. Droege, "Get Off my Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians", *International Review of the Red Cross*, n° 886, vol. 94, 2012, pp. 533-578.

[27] "How can we expect a global coalition to implement sanctions when attributing groups and attackers could be based anywhere in the world, and there is no recognized standard or institutionalized process for attribution?": M. Mueller, K. Grindal and al., "Cyber Attribution: Can a New Institution Achieve Transnational Credibility?", *The Cyber Defense Review*, n° 1, vol. 4, 2019, p. 108. For this dual-issue, see: F. Delerue, *Cyber Operations and International Law*, Cambridge University Press, 2019, pp. 55 ff.; P. Margulies, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", *Melbourne Journal of International Law*, vol. 14, 2013, p. 496 ff.; V. Kaluk, "Know Your Enemy and Know Yourself: Attribution in the Cyber Domain", *ICRC Blog Humanitarian Law and Policy*, 3 June 2019, <https://blogs.icrc.org/law-and-policy/2019/06/03/know-your-enemy-know-yourself-cyber-domain-attribution/> (03/21).

[28] International Committee of the Red Cross, *Norms for Responsible State Behaviour on Cyber Operations*, *supra* note 17.

virtual emblems). At the same time, humanitarian organisations, such as the ICRC, participate in international meetings to provide guidance to States and ensure that these humanitarian consequences of using cyber tools are fully recognised.[30]

Obviously, these few examples do not exhaustively illustrate the various problems caused by the integration of cyber tools in armed conflicts. However, they help demonstrating that there is no upheaval, but a disconcerting ease (as with all new technology?) to disregard the respect of the IHL provisions or to interfere with humanitarian actions. This fact creates, at least, a great opportunity for the international community to reaffirm the importance of these humanitarian protections. Meanwhile, it appears that these legal protections, traditionally under stress during hostilities, are also questioned or even challenged by jurists and legal advisors.

2.2. The 'Digitalisation' of the Battlefield: Questioning the Future of IHL Protections and the Introduction of New Opportunities for Clarification

The increased dangers imply a renewal of the question: is IHL still relevant? This general question conceals numerous legal questions about the applicability and interpretation of IHL's rules and main notions. The legal considerations are crucial, because the responses offered and/or verified in practice will contribute to shape the future of both IHL and humanitarian work. So far, in our opinion, these main questions have already been discussed but there is still no consensus, except for the general acceptance of IHL's application.[31] This refocuses the debate on the requirement to come up with new rules. For humanitarian agencies, the discussion is different. It will center around encouraging initiatives to maintain essential protections. Legal interpretation is key. Restrictive or not, it could lead to an increase of dangers but also who and what can be exposed or damaged during an armed conflict. Within the limits of the present contribution, the next developments will focus on two of these main questions due to their particular links and their prevailing reception in the legal sphere.

---

[29] For M. Marelli, "Hacking Humanitarian", *supra* note 1: "international humanitarian organizations need to consider unique and specific technical solutions to their specificities, such as the creation of a 'digital humanitarian space' following the model of a 'sovereign cloud' or a 'digital embassy".

[30] For instance, "[t]he ICRC welcomes the clear and unequivocal manner in which the current draft Report recognizes the 'potentially devastating humanitarian consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public", International Committee of the Red Cross*, Comments on the Substantive Report*, First Draft of the "Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security", 3 March 2021, p. 1.

[31] See K. Mačák and T. Rodenhäuser, "Even 'Cyber Wars' Have Limits. But What if they Didn't? ", *Blog of the European Journal of International Law*, 9 March 2021, <https://www.ejiltalk.org/even-cyber-wars-have-limits-but-what-if-they-didnt/ > (03/21). This article reminds the ICRC posture (the affirmation that IHL applies to cyber tools), and proposes an original approach to 'spotlight' the importance of this set of rules: "However, technical legal questions may cloud the very real benefits in terms of humanitarian protection offered by the application of this body of law to cyber operations. So instead of risking a pedantic debate, let's imagine for a moment that IHL didn't apply to cyber operations during armed conflicts. What could modern conflicts look like? ".

Despite its fundamental importance, a question remains unanswered: the qualification of "attack"[32] which is a prerequisite for the application of IHL principles. For instance, there is the principle of distinction between civilians and combatants and between civilian objects and military objectives.[33] The prohibitions that result from this "basic rule",[34] such as the prohibition of attacks against civilians[35] and against civilian objects, require this qualification.[36] The interpretation is, therefore, particularly relevant. And yet, the notion is not completely resolved in the cyber realm, creating a dangerous blur – for the significance of IHL as a protected set of rules, but most of all from a humanitarian perspective. Several views exist and highlight that the difficult apprehension is related to the spectrum covered by an "act of violence" (physical damages, deaths, injuries, loss of functionality). For Schmitt, there are three main approaches on the question: "one permissive (in the sense of allowing a wider range of cyber operations against the civilian population) and the other restrictive (restricting cyber operations as a matter of law [i.e., injury, death or damages])".[37] The third approach, which is the one adopted by the Tallinn's Experts, is "focusing on the functionality of an object that has been targeted by a cyber operation".[38]

Undoubtedly linked to the precedent, another important issue arises from the cyber tools: the question of the "civilian object" protected under IHL in this dual technology. For this issue, the debate is mostly focused on "data"[39] created, stored, circulating and essential to the digital domain. The international community has not been able to agree on a consensus yet.[40] Different views[41] exist which are contributing to extend the protection to data.

---

[32] According to Art. 49(1) AP I: " 'Attacks' means acts of violence against the adversary, whether in offence or in defence".

[33] IHL offers a negative definition of civilian objects based on the definition of military objectives: Art. 52(1) and (2) AP I.

[34] Art. 48 AP I.

[35] Art. 51(2) AP I.

[36] Art. 52 AP I.

[37] M. N. Schmitt, "Rewired Warfare: Rethinking the Law of Cyber Attack", *International Review of the Red Cross,* n° 893, vol. 96, 2014, p. 191.

[38] *Ibid* p. 192.

[39] For a legal *exposé* and a categorisation of data, see: R. Geiβ and H. Lahmann, *Research Brief Protection of Data in Armed Conflict*, The Geneva Academy of International Humanitarian Law and Human Rights, February 2021, 9 p. For the authors, "[t]he debate revolving around the question of the protection of data in armed conflict at times suffers from conceptual confusion and definitional ambiguities concerning the notion of 'data' itself." (p. 2). They expose the difference between data and metadata (data about data), and a useful classification.

[40] "[I]t remains unclear whether data enjoys the same protection as 'civilian objects'": T. Rodenhäuser, "Hacking Humanitarians? IHL and the Protection of Humanitarian Organizations Against Cyber Operations", *Blog of the European Journal of International Law*, 16 March 2020, <https://www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/> (03/21). The Author mentions some of these views and State-opinions.

[41] For some of the main positions: K. Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review*, vol. 48, 2015, pp. 55-80; K. Mačák, L. Gisel and T. Rodenhäuser, *supra* note 24; See also R. Geiβ and H. Lahmann, *supra* note 39, p. 6: they expose two main positions: "Proponents of the first view contend that the no-

Despite numerous views on the concepts of "data" and "attack", a big step was taken in 2019. The ICRC, in its position paper,[42] opted for a broader and protective interpretation on both issues:

> It is widely accepted that cyber operations expected to cause death, injury or physical damage constitute attacks under IHL. In the ICRC's view, this includes harm due to the foreseeable direct and indirect (or reverberating) effects of an attack …. [and] an operation designed to disable a computer or a computer network constitutes an attack under IHL whether the object is disabled through kinetic or cyber means. … While the question of whether and to what extent civilian data constitute civilian objects remains unresolved, in the ICRC's view the assertion that deleting or tampering with such essential civilian data would not be prohibited by IHL in today's data-reliant world seems difficult to reconcile with the object and purpose of IHL. The replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to them. Excluding essential civilian data from the protection afforded by IHL to civilian objects would result in an important protection gap.[43]

These two examples or "greys zones"[44] demonstrate the fact that, in a certain way, IHL must be updated[45] and States must, at least, agree on common interpretations. For the ICRC, "[i]f new rules are to be developed to protect civilians against the effects of cyber operations or for other reasons, they should build on and strengthen the existing legal framework – including IHL".[46] In this digitalised world, some authors even suggest to integrate a new protection dimension based on the cyber dependency of society: "the disruption of societal processes".[47] From a humanitarian perspective, these interpretations must be broad. However, for the legal and military spheres, great precautions must be taken in order to maintain the relevance of the rules. The non-resolution of the interpretation and of the objects

---

tion of 'object' in Article 52(2) AP I, taking its ordinary meaning, implies that the target of the military operation must be an entity of a physical quality, i.e. be something that is visible and tangible in the real world. … The opposing position holds that data can indeed be subsumed under the notion of 'object'".

[42] ICRC, Position Paper, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, Submitted to the 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' and the 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', November 2019, pp. 7-8.

[43] *Ibid* pp. 7-8.

[44] M. N. Schmitt, "Grey Zones in the International Law of Cyberspace", *The Yale Journal of International Law Online*, 2017, n° 2, vol. 42, 2017, pp. 17-19.

[45] The New Commentaries of firsts Geneva Conventions taking into account new technologies constitute a clear and relevant illustration, see *infra*.

[46] ICRC, Position Paper, *supra* note 42, p. 9. That position was repeated: ICRC*, Comments on the* Substantive *Report, supra* note 30, p. 2.

[47] R. Geiβ and H. Lahmann, "Protecting Societies – Anchoring a New Protection Dimension in International Law during Armed Conflict: An Agenda for Discussion", *Blog of the European Journal of International Law,* 23 February 2021, <https://www.ejiltalk.org/protecting-societies-anchoring-a-new-protection-dimension-in-international-law-during-armed-conflict-an-agenda-for-discussion/> (03/21).

protected by these rules, reveals a necessary insecurity for all entities present on the battlefield, including for humanitarian missions. Nonetheless, this alarming element should not obscure the fact that cyber also offers attractive solutions for humanitarian actors.

3. Cyber Tools for and by Humanitarians: the Challenging Perspective of Cyber «Tech For Good»

The "Cyber tech for good" approach is at a crossroads,[48] which explains the growing number of studies dedicated to the impacts but also to technological humanitarian solutions. The classic question would therefore be: Does appropriate humanitarian action necessarily need new technologies? This is why it is important to look at the changes brought by cyber from a humanitarian perspective.[49] But this question should not cloud the idea of the 'good' behind the 'tech'. Humanitarian organisations will therefore need to consider these integration difficulties in order to understand whether modernised technical actions are possible or incomplete.[50]

3.1. The Significant and Positive Cyber Changes Operated in the Humanitarian Field

Humanitarian organisations play a crucial role in armed conflict. They often contribute to mitigating effects during the conflict, but also for the aftermath. As the need for humanitarian aid increases,[51] organisations may choose to introduce new solutions to enable a more effective, appropriate or rapid humanitarian response. As the ICRC stated, it will "embrace innovation and digital transformation to become a more flexible and agile organization, one that responds more promptly and effectively to the changing needs of populations affected without losing the human, personal and informal character of its interaction with the populations and communities affected".[52] Cyber tools have therefore been integrated for several years and have the potential to contribute positively at different stages of humanitarian interventions. Within the limits of these developments, we will mention some of these integrations with the aim of illustrating the growing importance, as well as the practical and even legal implications of these cyber tools at different stages of the humanitarian action.

We can easily observe that organisations are using digital means to "fulfil" their existence (e.g. financial donations, public information of results, online campaigns

[48] According to M. Marelli, "Hacking Humanitarians", *supra* note 1, "they [Humanitarian organisations] evolve from simple bystanders to full-fledged stakeholders in cyberspace".

[49] See para. 3.1.

[50] See para. 3.2.

[51] See for example, United Nations Office for the Coordination of Humanitarian Affairs (OCHA), *The Global Humanitarian Overview*, 1 December 2020, <https://gho.unocha.org/> (03/21).

[52] ICRC, *Institutional Strategy 2019-2022*, September 2018, p. 7.

or pleas/advocacies etc.). Although not necessarily taking place during an armed conflict, we could argue that the humanitarian aid is facilitated by cyber initiatives. It can also contribute to a better knowledge and respect of IHL.[53] For example, in 2020, the ICRC and Fortnite partnership has led to the creation of a new game mode called "Liferun" – for the dissemination and respect of IHL.[54] Moreover, it contributes to a global discussion around good cyber behaviours and human cyber-security.

During an armed conflict, digitalised solutions are increasingly offered in order to facilitate aid delivery. For example, humanitarian organisations are currently using biometric authentication processes to prevent identity fraud or fraud aid.[55] This also goes for digital technology in order to inform the beneficiaries of the aid locations or programs and to control situations in real-time (e.g. cartography of displaced population).

These general cyber-improvements for humanitarian actions also extend to specific humanitarian missions like visiting liberty-deprived people, which is a traditional mandate of the humanitarian organisation – the ICRC.[56] Cyber tools can facilitate, for example, the record of people, and maybe[57] the detainee's right to correspond with their family.[58] In 2020, the updated ICRC Commentary of the Third Geneva Convention even admits to the use of cyber tools (e.g. emails) for the latter.[59]

Cyber tools can facilitate humanitarian assistance during but also after hostilities. In doing so, these actions can mitigate the disastrous consequences of the war as well as improving the respect of IHL. For example, in the light of the families' right to know the fate of their relatives,[60] cyber tools (communications between

---

[53] IHL indicates that "States must encourage the teaching of international humanitarian law to the civilian population*"* (Rule 143, *ICRC's Study on Customary International Humanitarian Law*, *supra* note 20); Art. 47 GC I, Art. 48 GC II, Art. 127 GC III, Art. 144 GC IV and Art. 83 AP I.

[54] Fortnite is an online game developed by Epic Games. It has multiple game modes, including the "Life run" mode. It invites players to "[e]xperience how ICRC helps civilians in war", *ICRC Website*, < https://www.icrc.org/en/fortnite-liferun> (03/21).

[55] For an interesting and practical debate about the utilisation of biometric see for ex.: Opinion, "Head to Head: Biometrics and Aid", *The New Humanitarian*, 17 July 2019, <https://www.thenewhumanitarian.org/opinion/2019/07/17/head-head-biometrics-and-aid> (03/21).

[56] Art. 126 GC III; Arts. 76(6) and 143 GC IV; Rule 124 of ICRC' Study on Customary International Humanitarian Law, *supra* note 20.

[57] According to the Tallinn's Experts: "Traditionally, the term 'correspondence' referred to letters or other handwritten communications. It is unclear whether, as a matter of law, correspondence includes electronic communications such as email. This is because the law is clear that a right of correspondence exists, but is not prescriptive as to its form" Rule 136(3), M. N. Schmitt (Ed.), CCD-COE, *Tallinn Manual 2.0, supra* note 11, p. 522.

[58] Arts. 70 and 71 GC III; Arts. 106 and 107 GC IV; Art. 5(2)(b) AP II; Rule 125 of ICRC' Study on Customary International Humanitarian Law, *supra* note 20.

[59] ICRC, Commentary of the Third Geneva Convention relative to the Treatment of Prisoners of War, vol. III, Geneva, 12 August 1949, 2020, Art. 71 GC III, paras. 3186 ff., *IHL Database,* <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=57E8B789BE64B449C12585880038C7C8> (03/21).

[60] Arts. 32, 33 and 34 AP I; Art. 26 GC IV; Rule 117 of ICRC' Study on Customary International Humanitarian Law, *supra* note 20.

humanitarian agencies, storage and share of personal information about displaced populations for example) can be particularly relevant to facilitate this binding obligation. In the same perspective, cyber means have already proved their usefulness for restoring family links:[61] via, for example, the ICRC's online platform Trace the Face.[62]

The initial question was: do cyber tools contribute to a better respect of IHL and to a facilitated humanitarian mission? If an affirmative answer seems to be forthcoming, the answer would not be complete without analysing the result and dangers ensuing from the integration of humanitarian cyber tools.

3.2. The Incomplete but Promising Cyber Proposals: the Difficult Integration of Humanitarian Cyber Tools

According to Marelli, "[n]ew technologies create opportunities for improved humanitarian response as well as risks to the operating organization and the people it seeks to protect and assist".[63] Humanitarian organisations should be able to develop an *exclusively positive* conception of cyber technology (in contrast to the predominantly negative approach mentioned in introduction), while at the same time allowing new protections for staff and beneficiaries to be considered. In order to do this, it is necessary to assess this progress verifying two fundamental factors: the respect of humanitarian principles and standards and the beneficiaries' respect and protection.

As it stands, it would seem appropriate to overcome three challenges: ensuring compliance with humanitarian principles and standards (which also includes respecting the organisation's limits of action), ensuring the protection of organisational structures and their staff (which increasingly includes taking into account the risk of discrediting the mission or the entire organisation), and finally, if these steps are taken, ensuring that the new tools are sufficiently relevant and secure so that they do not cause further negative consequences for beneficiaries. In each of these areas, both legal and humanitarian experts seem to agree on the fact that cyber tools are still a challenge. Nevertheless, the humanitarian community is willing to take a chance – sometimes without a safety net.[64]

The relatively stable humanitarian structure must not be unbalanced by cyber. It necessarily implies the respect of humanitarian principles[65] such as humanity, im-

---

[61] Arts. 25 and 26 GC IV; Art. 74 AP I; Art. 4(3)(b) AP II; Rule 105 of ICRC' Study on Customary International Humanitarian Law, *supra* note 20.

[62] *Trace the face*, <https://familylinks.icrc.org/europe/en/Pages/home.aspx> (03/21).

[63] M. Marelli, "Hacking Humanitarians"*, supra* note 1.

[64] It raises the issue of 'humanitarian experimentation': K. Bergtora Sandvik, K. Lindskov Jacobsen and S. Martin McDonald, "Do no Harm: A Taxonomy of the Challenges of Humanitarian Experimentation", *International Review of the Red Cross*, *Migration and displacement*, n° 1, vol. 99, 2017, pp. 319-344.

[65] For a presentation of legal origins: J. Labbé, "Les principes de l'action humanitaire", in Szurek, Eudes and Ryfman (Dir.), *Droit et pratique de l'action humanitaire, cit. supra* note 7, pp. 235-251.

partiality, neutrality and independence.[66] As described by Labbé, "the humanitarian principles set the ethical goals of humanitarian action and provide an operational framework and tools that distinguish it from other forms of aid".[67] Cyber humanitarian actions must also include the principle of "do no harm".[68] For example, it seems a priori difficult to fully respect the principle of independence due to technical specificities of cyber tools and their financial implications. As mentioned before, humanitarian organisations use cyber tools such as specific software solutions, which imply financial resources and long-term dependence in order to acquire, use, update and secure their utilisations.

Humanitarian actors will face parallel risks too. Those risks can be various in nature, reasons (for example, suspend or impede the humanitarian aid, or discredit the mission or even, the organisation itself) and consequences. Humanitarian organisations can become direct targets of cyberattacks. Some recent incidents[69] confirm this dark spectrum while highlighting the growing dependency.

While assisting to the "rise of 'connected beneficiary'",[70] we can also observe colossal risks for protected persons. Therefore, the responsibility of ensuring full protection to protected persons is borne by the organisations. Their responsibility extend to the digital domain due to the ever-growing consequences of an armed conflict. For Solinge, two major risks exist: "The (mis)use of data or digital technology by State and non-state actors which lead to humanitarian consequences for affected population …. Behaviour or practices of humanitarian actors or affected people that enable increased exposure to digitally-related risks (e.g., through mal-

[66] "Humanitarian action should be motivated by the sole aim of helping other human beings affected by conflicts or disasters (humanity); exclusively based on people's needs and without discrimination (impartiality); without favouring any side in a conflict or engaging in controversies where aid is deployed (neutrality); and free from any economic, political or military interest at stake (independence)" (J. Labbé, "Chapter 2: How do humanitarian principles support humanitarian effectiveness?" in Humanitarian Accountability report called On the Road to Istanbul, How Can the World Humanitarian Summit Make Humanitarian Response More Effective?*,* 2015, p. 20).

[67] *Ibid.*

[68] "Protection actors must avoid harmful effects that could arise from their work …. [and] must contribute to the capacity of other actors to ensure that no harmful effects derive from their actions" ICRC, *Professional Standards for Protection Work Carried Out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence*, 3rd edition, Geneva, 2018, p. 27.

[69] Non exhaustive but recent disclosed incidents: the 2019 phishing-campaign targeting several organisations; the 2020 cyberattack against the servers of the United Nations; the spring ransomware attack against a fundraising online platform (2020) that affect numerous non-governmental organisations. See respectively: T. Seals, "U.N., UNICEF, Red Cross Under Ongoing Mobile Attack", *Threapost*, 25 October 2019, <https://threatpost.com/un-unicef-red-cross-mobile-attack/149556/> (03/21); B. Parker, "The Cyber Attack the UN Tried to Keep Under Wraps", *The New Humanitarian*, 29 January 2020, <https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack> (03/21); B. Parker, "Dozens of NGOs Hit by Hack on US Fundraising Database", *The New Humanitarian*, 4 august 2020, <https://www.thenewhumanitarian.org/news/2020/08/04/NGO-fundraising-database-hack> (03/21).

[70] A. Kaspersen and C. Lindsey-Curtet, "The Digital Transformation of the Humanitarian Sector", *ICRC Blog Humanitarian Law and Policy*, 5 December 2016, <https://blogs.icrc.org/law-and-policy/2016/12/05/digital-transformation-humanitarian-sector/> (03/21).

practice, mishandling of information and personal data, digital illiteracy)".[71] For the first one, the new term of "weaponisation of the information"[72] is often used.

From that perspective, an increasing number of studies (carried out by the humanitarian sector or academics) point out the important question of personal data[73] and metadata[74] regarding both the risks for populations and the humanitarian principles. For example, data and metadata created by the use of humanitarian cyber tools can easily be analysed, in order to recreate the life "pattern" of protected people in the purpose of targeting them (broad sense).[75] In times of peace, the issue of storage and use of personal data is already a central concern given the threats to the freedom or privacy of individuals.[76] In times of war, browsing the Internet, for example to obtain information on or to benefit from humanitarian aid, puts individuals at risk of being harmed in their physical integrity.

4. Concluding Remarks

As stated in the introduction to this book, there is a clear need for dialogue and collaboration between all sectors to ensure the security of all in cyberspace. An emphasis should be put on the times of armed conflict, where the navigation in cyberspace appears to be necessary but perilous. Cyber tools are therefore both a springboard for increased security risks for humanitarian organisations and their beneficiaries and a platform of many solutions to address the humanitarian consequences of armed conflicts. The characteristics of cyberspace then require unique solutions, both legal and technical. States, international organisations, tech companies and humanitarian organisations will have to act together in order to establish a framework to guarantee human security.

Obviously, these rules, principles and standards need to be reinforced. It is particularly true at a time of competition between humanitarian organisations and the

---

[71] D. Van Solinge, "Digital Risks for Populations in Armed Conflict: Five Key Gaps the Humanitarian Sector Should Adress", *ICRC Blog Humanitarian Law and Policy*, 12 June 2019, <https://blogs.icrc.org/law-and-policy/2019/06/12/digital-risks-populations-armed-conflict-five-key-gaps-humanitarian-sector/> (03/21).

[72] "An umbrella term that covers a range of new phenomena, including: online disinformation campaigns; online hate speech; viral rumours and dangerous speech; information operations; and computational propaganda" ICRC, *Symposium Report On Digital Risks In Situations Of Armed Conflicts*, Codenode London, United Kingdom, 11-12 December 2018, p. 8.

[73] For example: C. Kuner and M. Marelli (Ed.), *Handbook On Data Protection In Humanitarian Action*, 2nd edition, 2020, p. 302.

[74] For example, International Committee of the Red Cross and Privacy International, *The humanitarian metadata problem: "Doing no harm" in the digital era*, 2018, p.127.

[75] *Ibid*.

[76] For specific issues regarding personal data see, for example, the contributions of O. Koshevaliska, "Human Security Of Migrants In The On-Line World", R. Catalano,"Neuroscience, Artificial intelligence and Protection for Personal Rights" and F. De Simone *La prevenzione del crimine alle frontiere 2.0, una questione di dati biometrici*, in this Volume.

emergence of "benefactors 2.0"[77] that where enabled by the diversity and attractiveness of the cyber domain. Humanitarian organisations are essential. Their missions and goals must be respected, regardless of the means employed and the risks involved. We hope that these few pages will be enough to draw the reader towards a more positive approach, to welcome the long-standing rules and the humanitarian aid built on solid foundations. As Maurer said, "[i]nternational humanitarian law is a living body of law. Sometimes we forget it".[78] Cyber tools seem to encourage an enlightened and conscious modernisation of the future of humanitarian actions in this continuous "paradox of progress".[79]

[77] C. Luangsay-Catelin, « La diplomatie humanitaire ou l'impact du numérique sur la mobilisation (cyber)citoyenne », *Hermès la Revue*, n° 81, vol. 2, 2018, p. 117. The author refers to the multiplication of humanitarian entities and the influence of Internet. She illustrates the evolution of the humanitarian diplomacy with J. Jarre who raised funds via twitter during the Rohingyas crisis.

[78] P. Maurer, President of the International Committee of the Red Cross, Rules in War – A Thing of the Past?, *Centre for Strategic and International Studies, Washington*, *ICRC Statement*, 10 May 2019, <https://www.icrc.org/en/document/speech-icrc-president-rules-war-thing-past> (03/21).

[79] ICRC, *Institutional Strategy 2019-2022*, *supra* note 52, p. 4.

VECCHI ODI, NUOVE FORME DI VENDETTA: LO SPAZIO INFINITO DEL *REVENGE PORN*

Giuliana Doria

1. Premessa

La libertà intrinseca del web come spazio di condivisione di informazioni e come accesso alla conoscenza ha spinto alcuni a ritenere come necessario garantire a tutti la possibilità di accedere al mondo informatico. Internet, come spazio senza confini, dovrebbe infatti rientrare tra i beni comuni,[1] "definibili in senso lato come quelli idonei a esprimere utilità funzionali all'esercizio di diritti fondamentali nonché al libero sviluppo della persona e informati al principio della salvaguardia intergenerazionale delle utilità",[2] e ciò proprio in quanto influenza molti aspetti della vita quotidiana e incide anche sull'effettivo godimento dei diritti umani e delle libertà fondamentali.[3] Internet non si può ritenere solo un semplice mezzo di comunicazione, ma si traduce sempre più in uno strumento di ridefinizione dello spazio pubblico, privato ed economico: "una risorsa globale e che risponde al criterio della universalità".[4]

È evidente come sia cambiato il mondo della condivisione a livello globale. Si è passati da un modello di diffusione delle informazioni cd. *One-to-Many*, quello dei classici mezzi di informazione, i libri o la televisione, in cui vi sono team editoriali che costituiscono un filtro, a quello cd. *Many-to-Many*[5] in cui i dati e le notizie sono

---

[1] S. Rodotà, **"**'Il sapere come bene comune' - Il popolo di Internet"**,** *Intervento proposto al Festival filosofia di Modena, Carpi, Sassuolo,* 2007 < *https://www.privacy.it/archivio/rodota20070915.html* >(04/21); M. Taddeo - F. Bosco, "We must treat cybersecurity as a public good. Here's why", 22 agosto 2019 < https://www.weforum.org/agenda/2019/08/we-must-treat-cybersecurity-like-public-good/ > (05/21); F. Soulard, "The Internet as a Common Good. Framework and Perspectives for a Citizen Internet", *Wall Street Journal*, 31 ottobre 2018, < https://wsimag.com/science-and-technology/44147-the-internet-as-a-common-good > (05/21). Si veda anche G. De Minico, *Libertà in rete, libertà dalla rete*, Giappichelli, Torino, 2020, pp. 36-40, la quale si occupa del diritto di accesso ad Internet anche come diritto sociale. Cfr. Assemblea Parlamentare del Consiglio d'Europa, risoluzione n. 2256*, Provisional version, Internet governance and human rights"* del 2019.

[2] Così il disegno di legge n. 2031, Senato della Repubblica, comunicato alla presidenza il 24 febbraio 2010, <https://www.senato.it/service/PDF/PDFServer/DF/217244.pdf>, a seguito della proposta di modifica della Commissione Rodotà, creata per elaborare uno schema di legge delega per la modifica delle norme del codice civile in materia di beni pubblici del 21 giugno 2007, che non è stata fatta. Nella stessa prospettiva della Commissione Rodotà si colloca anche la decisione della Corte di Cassazione Civile a Sezioni Unite con la sentenza 3665 del 2011.

[3] Cit. *supra* Assemblea Parlamentare risoluzione n. 2256.

[4] Dichiarazione italiana dei diritti di Internet, Camera dei deputati, XVII Legislatura Commissione per i diritti e i doveri in Internet, Preambolo.

[5] J. Knauer - M. Rickard, "Internet Global Environmental Information Sharing", in D. J. Richards,

completamente liberi di circolare. Attraverso il web tuttavia questo filtro è venuto a mancare. Ciò ha comportato il fluire di un numero incredibile di informazioni, rendendo Internet un luogo in cui il diritto di espressione trova la più grande libertà. Le Nazioni Unite con una risoluzione non vincolante del *Human Rights Council* del 2016 condannano chiaramente: le misure per ostacolare intenzionalmente l'accesso o la diffusione di informazioni online in violazione del diritto internazionale dei diritti umani e invita tutti gli Stati ad astenersi e a cessare tali misure.[6] Inutile discutere sulla "giustizia" di questa affermazione. Bisognerebbe però riflettere relativamente al senso e al valore di "*information*". Sulla base della dichiarazione, infatti, si aprono spazi al fenomeno delle *fake news*, ma anche a usi distorti delle libertà, che possono incidere su libertà altrui, sbilanciando il diritto fondamentale a esprimersi in una *licentia* potenzialmente dannosa.

Il carattere ubiquitario del cyberspazio e l'evoluzione tecnologica continua rendono Internet un bacino di utenza immenso. Le informazioni vengono diffuse istantaneamente in tutto il mondo, attraverso anche gli *smartphone* e le nuove applicazioni di condivisione. Tali libertà consentono un fluire di notizie e scambi sociali semplificati e velocissimi, potremmo dire immediati, che se da una parte vengono visti come un grande beneficio, un *quid pluris*, da salvaguardare (fondamentale il diritto di espressione) comportano dall'altra la nascita di nuove forme di attività dannose e, quindi, di reato. È quanto mai opportuno un bilanciamento dei diritti affinché non venga, in primo luogo, lesa la dignità umana.

Si può registrare, nel crescente uso di Internet, oramai indispensabile nella vita di tutti i giorni, che crimini comuni possano essere commessi impiegando le nuove tecnologie e il web. Si tratta di cd. crimini impropri, che, al contrario dei crimini propri come la frode informatica con il classico esempio del *phishing*, sono tipizzati proprio a partire dall'uso necessario del web per la configurazione del reato e la qualificazione del fatto, servendosi di Internet solo come mezzo per perpetrare il crimine. Al giorno d'oggi si sente sempre più parlare nelle notizie di cronaca di *cyber violence* in particolare risaltano crimini d'odio come l'*hate speech*, il cyberbullismo e il *revenge porn*. In questi crimini sentimenti, come odio, vendetta e (pseudo) onore si intrecciano andando a incidere su diritti personalissimi, mettendo a rischio pertanto la sicurezza umana. In ambito internazionale, la Convenzione sulla criminalità informatica[7] del 2001 del Consiglio d'Europa è per ora l'unico strumento vincolante in tema di *cybercrime*, in cui vengono indicate però solo alcuni tipi di offese e tra queste non troviamo il *revenge porn*.

B. R. Allenby, W. Dale Compton (eds.), *Information Systems and the Environment*, National Academy of Engineering, National Academy Press, Washington, D.C. 2001 p. 185 <https://www.nap.edu/read/6322/chapter/18 > (04/21).

[6] UN Human Rights Council 32ma sessione, Agenda item 3, A/HRC/32/L.20, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, del 27 giugno 2016. Si criticano i Paesi che con il controllo di Internet o addirittura il blocco dello stesso adottano vere e proprie campagne di censura per mantenere il proprio potere.

[7] Convenzione sul *cybercrime* del Consiglio d'Europa, detta anche Budapest Convention, adottata il 23 novembre 2001, Budapest.

Questi reati sono intrinsecamente connessi con il rapido sviluppo dello spazio cyber, che ha modificato profondamente l'approccio alla socialità. Quel nuovo sistema di condivisione globale delle informazioni che ha rivoluzionato la quotidianità, è divenuto, come si è accennato, un circuito discorsivo nel quale si può danneggiare l'altro attraverso parole, immagini, minacce, spesso combinando questi tre elementi. La globalizzazione digitale crea infatti una realtà interdipendente: si è formato un vero e proprio mondo parallelo in cui le relazioni si sono modificate. Partendo da tali premesse, il mio lavoro si concentrerà sul fenomeno del *revenge porn* al fine anche di individuare le criticità e le problematiche legate ad Internet e ai conseguenti limiti e preoccupazioni relativi alla protezione internazionale dei diritti umani.

2. Cosa si intende per *revenge porn*?

Comunemente si utilizza la locuzione *revenge porn* per identificare il fenomeno della diffusione non consensuale di immagini intime.[8] La fattispecie ha una portata ampia, viene considerato un illecito plurioffensivo, la cui condotta è idonea a ledere contemporaneamente una pluralità di beni giuridici. Sono ancora pochi i Paesi[9] che hanno adottato normative specifiche per combattere il fenomeno comportando una tutela dei soggetti non sempre facile da attuarsi. In Italia il *revenge porn* è stato introdotto come reato nel 2019 con il cd. Codice Rosso.[10] I differenti approcci delle legislazioni nazionali al fenomeno di *revenge porn* rendono ancora più evidente la necessità di identificazione della fattispecie. Potrebbe essere quindi a tal fine molto utile un intervento a livello internazionale per cercare di uniformare un fenomeno così complesso.

L'European Institute for Gender Equality (EIGE), agenzia dell'Unione Europea sull'uguaglianza di genere, fornisce la seguente definizione di *revenge porn*:

---

[8] Per tutti, da diversi punti di vista: A. Sorgato, *Revenge porn, aspetti giuridici, informatici e psicologici*, Giuffrè Francais Lefebre, Milano, 2020; A. Paladino, *Revenge porn e cyberbulismo*, Alpes, Roma, 2020; G. Ziccardi, *L'odio online, violenza verbale e ossessioni in* rete, Raffaello Cortina Editore, Milano, 2016; G.M. Caletti, "*'Revenge porn*' e tutela penale", *Diritto Penale Contemporaneo*, 2018.

[9] In Europa tra i Paesi che hanno criminalizzato il *revenge porn* vi sono: l'Inghilterra che ha aggiunto la *section 33* al Criminal Justice and Courts Act nel 2015; la Spagna che, nel 2015, ha implementato l'art. 197 del *Codigo Penal*; la Francia che, nel 2016, ha adottato il *Projet de loi pour une République numérique* (*Digital Republic Bill*); e in ultimo l'Italia che ha introdotto l'art. 612 *ter* nel codice penale con la legge 19 luglio 2019 n. 69, entrata in vigore il 9 agosto, il cd. Codice Rosso. Nel resto del mondo invece: gli USA non hanno una legislazione comune in materia, ma sono 41 gli Stati che hanno criminalizzato il fenomeno, il primo è stato il New Jersey nel 2004; le Filippine hanno adottato, nel 2009, l'*Anti-Photo and Video Voyeurism Act* (*Republic Act* No. 9995); il Canada, nel 2014, il *Bill C-13, Protecting Canadians from Online Crime Act*, sul crimine online volto a contrastare il cyberbullismo, integrandolo quindi anche della fattispecie della diffusione di immagini intime senza il consenso; la Nuova Zelanda, invece, l'*Harmful Digital Comunication Act* nel 2015.

[10] Articolo 612 *ter* c.p.

> Non-consensual pornography (the most common form of which is known as 'revenge porn') involves the online distribution of sexually graphic photographs or videos without the consent of the individual in the images. The perpetrator is often an ex-partner who obtains images or videos in the course of a prior relationship, and aims to publicly shame and humiliate the victim, in retaliation for ending a relationship. However, perpetrators are not necessarily partners or ex-partners and the motive is not always revenge.[11]

L'EIGE specifica come il *revenge porn* sia la forma più nota della cd. *Non Consensual Pornography* (NCP). In senso stretto nel *revenge porn* si considera come autore l'ex partner che con finalità vendicative pubblica immagini intime, destinate a rimanere private, ritraenti l'ex compagno/a che ha posto fine alla relazione sentimentale. È possibile trovare la voce *revenge porn* nelle enciclopedie[12] o nei dizionari[13] ma non rientra in essi anche la *Non Consensual Pornography*. Il *revenge porn* è divenuto il termine di riferimento per trattare di diffusione non consensuale di immagini intime o NCP. La scelta di continuare ad utilizzare l'espressione *revenge porn* in modo ampio è data sicuramente dalla semplice riconoscibilità dell'illecito, e oltre a ciò è anche in qualche modo d'effetto.[14] Secondo Glynn "the term is at once too narrow and applied too widely".[15]

Attuando un'analisi più approfondita i termini *revenge* ("vendetta") e *porn* ("porno") non sono pregnanti. Invero, il primo farebbe presumere che la vittima abbia commesso un torto o un qualche atto non consono e che pertanto, sia necessaria una vendetta, rendendo l'atto quasi "giustificabile".[16] L'uso di "vendetta", potrebbe far intendere che il movente dell'autore sia limitato a quel fine, mentre l'uso di "porno" si concentra sulle azioni della vittima che si è prestata a farsi ritrarre in momenti intimi, colpevolizzando di fatto la vittima e alimentando il cd. *victim blaming*. Per ovviare a tale problematica semantica si cerca quindi di utilizzare delle

---

[11] The European Institute for Gender Equality (EIGE), Glossary & Thesaurus, "*Revenge porn*" <https://eige.europa.eu/thesaurus/overview> (04/21).

[12] La definizione di *revenge porn* è entrata nell'Enciclopedia Italiana Treccani nel 2016, dal 2019, è stata inserita la definizione anche di "pornovendetta" termine italianizzato. Si veda sull'argomento M. A. Cortelazzo, "Le parole della neopolitica - *Revenge Porn*" *Enciclopedia Italiana Treccani*, 17 aprile 2019 <https://www.treccani.it/magazine/lingua_italiana/articoli/parole/Neopolitica12.html > (05/21).

[13] Cambridge dictionary "*Revenge Porn*": "private sexual images or films showing a particular person that are put on the Internet by a former partner of that person, as an attempt to punish or harm them" <https://dictionary.cambridge.org > (04/21) and Oxford Dictionary "*Revenge Porn*": "Sexually explicit images or videos of an individual, published online without their consent and with the intent to cause them distress" <https://www.oxfordreference.com/view/10.1093/acref/9780191803093.001.0001/acref-9780191803093-e-1231 > (04/21).

[14] Il termine è molto efficace a livello giornalistico e pertanto è utilizzato comunemente anche per le altre fattispecie legate alla NCP, viene utilizzato come "*catch all phrase*", così, *supra* nota 8 Caletti, "'Revenge porn' e tutela penale" cit. p. 71.

[15] C. McGlynn et al., "Beyond '*Revenge Porn*': The Continuum of ImageBased Sexual Abuse", *Feminist Legal Studies*, 2017, p. 30.

[16] Senato Australiano, Legal and Constitutional Affairs References Committee, "Phenomenon colloquially referred to as '*revenge porn*'", febbraio 2016, p. 49.

espressioni in maggior misura corrispondenti, come ad esempio si è già accennato alla NCP, o ancora secondo alcuni si potrebbe utilizzare la locuzione "*image-based sexual abuse*",[17] potendo in tal modo ricomprendere ugualmente altre sfaccettature dell'illecito, cosicché la motivazione alla base non sia ristretta alla sola vendetta. Nel resto del lavoro mi riferirò alla fattispecie come NCP con l'esclusione dei casi in cui sia necessario l'uso della locuzione *revenge porn*, nella concezione ristretta.

L'autore di NCP può corrispondere a un vendicativo ex partner, ma non solo. Anche familiari o amici della vittima, o un soggetto completamente sconosciuto possono perpetrare il crimine. Si individuano due distinte ipotesi a) chi diffonde le immagini, ha contribuito alla realizzazione delle stesse o le ha sottratte; b) chi diffonde le immagini, le ha ricevute o acquisite in altro modo. In Italia per il secondo caso vi è la richiesta di un dolo specifico,[18] la diffusione deve avvenire "con l'intenzione di creare un nocumento", pertanto si discute se siano da considerare "secondi distributori" anche coloro che ricevono per uso privato immagini dal proprio partner e che, violando la fiducia dell'altra persona, diffondano tali immagini.[19] Nell'Illinois non viene fatta una distinzione con i cd. "secondi distributori", e questo rientra tra i motivi per cui la Cyber Civil Rights Initiative ritiene questo Stato USA come quello con la migliore legislazione in tema di NCP.[20]

---

[17] McGlynn et al., "Beyond '*Revenge Porn*'", cit. nota 15, p. 26-27; in tal senso si veda anche N. Henry - A. Powell, "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research", *Trauma, Violence and Abuse*, 2016, pp. 195-208.

[18] Art. 612 *ter* c.p. : "(1) Salvo che il fatto costituisca più grave reato, chiunque, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate, è punito con la reclusione da uno a sei anni e con la multa da euro 5.000 a euro 15.000. (2) La stessa pena si applica a chi, avendo ricevuto o comunque acquisito le immagini o i video di cui al primo comma, li invia, consegna, cede, pubblica o diffonde senza il consenso delle persone rappresentate al fine di recare loro nocumento. (3) La pena è aumentata se i fatti sono commessi dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se i fatti sono commessi attraverso strumenti informatici o telematici […]".

[19] Secondo G. Di Giuseppe, "Il contrasto al c.d. '*revenge porn*': tra violenza di genere e uso illecito della rete", 2017, < https://www.diritto.it/il-contrasto-al-c-d-revenge-porn-tra-violenza-di-genere-e-uso-illecito-della-rete/ > (04/21), potrebbe creare problemi il secondo comma dell'art. 612 *ter*, nel caso in cui il dolo specifico dovesse mancare, ciò comporterebbe una restrizione dell'ambito di applicazione. Paradossalmente sarebbero i casi più frequenti quelli dei "secondi distributori", in cui chi riceve e diffonde le immagini non conosce la persona ritratta oppure, anche conoscendola, le invia a sua volta. Le conseguenze poi della viralità di un contenuto sono anche quelle che creano maggiori problemi.

[20] Si veda C. Goldberg "Seven Reasons Illinois is Leading the Fight Against Revenge Porn", Cyber Civil Rights Initiative, 31 dicembre 2014, <https://www.cybercivilrights.org/seven-reasons-illinois-leading-fight-revenge-porn/> (05/21). Illinois Statutes Chapter 720. Criminal Offenses para. 23.5(2)(3): "Non-consensual dissemination of private sexual images": "A person commits non-consensual dissemination of private sexual images when he or she: (1) intentionally disseminates an image of another person: (A) who is at least 18 years of age; and (B) who is identifiable from the image itself or information displayed in connection with the image; and (C) who is engaged in a sexual act or whose intimate parts are exposed, in whole or in part; and (2) obtains the image under circumstances in which a reasonable person would know or understand that the image was to remain private; and (3) knows or should have known that the person in the image has not consented to the dissemination".

Venendo ai diversi elementi di valutazione che si possono ricondurre alla fattispecie, possono essere individuate quattro variabili:[21] 1) l'origine delle immagini o dei video intimi; 2) il consenso; 3) la motivazione per diffondere il materiale e 4) elementi di riconoscibilità dell'immagine.

In relazione al primo punto, il materiale intimo può essere stato prodotto dalla stessa persona ritratta, oppure da un'altra persona o può essere stato rinvenuto online.[22] Si tratta quindi di un momento antecedente rispetto alla commissione del reato, presupposto dello stesso.

Per quanto riguarda il tema del consenso, il discorso dovrebbe essere più ampio in quanto in quest'ambito rilevano due momenti. Che vi sia il consenso alla produzione delle immagini intime, non comporta necessariamente che vi sia il consenso anche alla divulgazione delle stesse. Ad esempio con il fenomeno del *sexting*[23] avviene uno scambio consensuale di immagini a connotazione intima e/o erotica, eppure ciò non implica che la persona che volontariamente scatta e invia le immagini intime, voglia che le stesse vengano pubblicate e diffuse oltre la sfera privata. In questo caso manca l'approvazione a far divenire pubbliche delle immagini che erano state prodotte con la sola finalità di rimanere private. Il consenso all'interno di un rapporto di fiducia non equivale al consenso al di fuori di tale contesto, secondo Citron e Franks "we should no more blame individuals for trusting loved ones with intimate images than we blame someone for trusting a financial advisor not to share sensitive information with strangers on the street".[24] Così il *sexting*, di per sé lecito, si potrebbe trasformare in NCP. Ci si può trovare di fronte ad una moltitudine di situazioni differenti e variegate con l'esigenza di dover valutare se ci sia stato il consenso. In ogni caso non appare una questione di semplice soluzione.

Molti possono poi essere i motivi che spingono una persona a diffondere del materiale privato di un'altra persona. Come già abbiamo visto la fattispecie di *revenge porn* in senso stretto ha come motivazione la vendetta, umiliare e creare al proprio ex un danno, che è sicuramente di natura psicologica ma in alcuni casi può essere anche patrimoniale. Tuttavia vi possono essere anche altre motivazioni, si

[21] S. R. Stroud - J. Henson, "Social Media, Online Sharing, and the Ethical Complexity of Consent in *Revenge Porn*" in Angeline Close Scheinbaum (ed.), *Online Consumer Behavior: The Dark Side of Social Media*, Routledge, 2016, p.10.

[22] In dottrina le prime due fattispecie sono largamente individuate, Stroud e Henson aggiungono anche la terza possibilità, ovvero reperire il materiale intimo online. Si veda D. K. Citron - M.A. Franks, "Criminalizing *Revenge Porn*", *Wake Forest Law Review*, 2014, pp. 1-38; *Ibid.* p.12.

[23] Per *sexting* si intende: "invio di messaggi, immagini o video a sfondo sessuale o sessualmente espliciti tramite dispositivi informatici portatili o fissi" Enciclopedia Italiana Treccani < https://www.treccani.it/vocabolario/sexting_%28Neologismi%29/ > (04/21). Collegato alla NCP è il fenomeno del *sexting*, molto diffuso tra i minori i quali scambiano con i propri coetanei immagini o video intimi. Bianchi affronta il tema del *sexting* minorile alla luce della sentenza di Corte di Cassazione sezione penale n. 11675 del 21/03/2016 che ha escluso la configurabilità del delitto diffusione di immagini pedopornografiche, disciplinato all'art. 600 ter c.p. se le fotografie prodotte sono state prodotte, volontariamente e autonomamente dal minore. M. Bianchi, "Il *sexting* minorile non è più reato?", *Diritto Penale Contemporaneo,* 2016.

[24] Cit. nota 22, Citron e Franks, "Criminalizing *Revenge porn*" pp. 348-349.

pensi al caso di hacker che rubano materiale privato al fine di trarne profitto diffondendo quanto sottratto,[25] o per motivi futili di divertimento.

Dall'ultimo elemento, la riconoscibilità dell'immagine, derivano le conseguenze più gravi.[26] Si pensi al caso della "Maestra di Torino"[27] che è stata sottoposta ad una gogna mediatica e costretta a dimettersi a seguito della circolazione di sue foto intime. Le pressioni, le violenze verbali, l'imbarazzo familiare possono spingere i soggetti finanche al suicidio,[28] ma ovviamente è molto difficile in questi casi la ricostruzione di un rigoroso nesso causale. Le immagini poi, molte volte, sono diffuse su social network o gruppi specializzati correlati di dati sensibili della vittima come nome, indirizzo email o numero di cellulare,[29] mettendo a rischio la persona altresì a molestie sessuali e violenze che possono divenite persino fisiche. Paladino, stante le conseguenze devastanti della NCP commessa tramite sistemi informatici, sostiene si possa parlare addirittura di "cyber-stupro".[30]

Queste pratiche hanno antenati antichissimi nelle iscrizioni diffamatorie, che vanno dal mondo classico alla letteratura parietale che si trova ancora, ad esempio, nelle toilette delle scuole o degli autogrill,[31] con offese depotenziate dal circuito nel quale si iscriveva rispetto alla ridondanza nel web.

---

[25] Famoso è il caso del 2014 in cui gli hacker riuscirono ad accedere all'ICloud di moltissime celebrities come Jennifer Lawrence o Selena Gomes, sottraendo foto e materiale privato diffuso poi sulla rete. D. Kedmey, "Hackers Leak Explicit Photos of More Than 100 Celebrities", *Time*, 1 settembre 2014, < https://time.com/3246562/hackers-jennifer-lawrence-cloud-data/> (05/21). McGlynn et al., "Beyond '*Revenge Porn*'" cit. nota 15, p. 30.

[26] Cit. *supra* nota 17.

[27] Nel 2018 divennero virali delle immagini private di una maestra a Torino, inviate nella chat del calcetto dall'ex fidanzato e che successivamente furono diffuse. La maestra fu costretta a dare le dimissioni. La direttrice dell'asilo è stata condannata a 13 mesi di reclusione per violenza privata e diffamazione. Si veda S. Martinenghi, "*Revenge porn*, direttrice d'asilo licenziò maestra vittima della gogna online: condannata", *La Repubblica*, 19 febbraio 2021 <https://torino.repubblica.it/cronaca/2021/02/19/news/torino_condannata_la_direttrice_d_asilo_che_licenzio_la_maestra_vittima_di_revenge_porn-288283334/ > (05/21).

[28] Secondo il report statistico pubblicato nel 2014 dalla Cyber Civil Rights Initiative, End Revenge Porn, il 51% ha avuto pensieri suicida a causa dell'essere stata vittima di NCP <https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf > (04/21).

[29] Cyber Civil Right Initiative, End Revenge Porn ha rilevato che sono stati pubblicati insieme al materiale intimo il nome nel 59% dei casi, il profilo del social nel 49%; l'indirizzo email 26%; il numero di telefono nel 20%; l'indirizzo di casa nel 16% e l'indirizzo di lavoro nel 14% Ibid 28.

[30] A. Paladino, *Revenge porn e cyberbullismo*, Alpes, 2020, p. 10.

[31] La NCP ha molti punti in comune con altri tipi di reati, che in Italia prima dell'entrata in vigore del "Codice Rosso" erano contestate nei casi di NCP, come ad esempio gli atti persecutori ex art. 612 *bis* c.p. Il bene giuridico tutelato da entrambi i reati è la libertà morale della vittima, negli atti persecutori però è necessaria "l'abitualità", le molestie devono ripetersi nel tempo. In tal senso, la pronuncia del Tribunale di Milano, Giudice per le indagini preliminari, n. 1673, 21 giugno 2018, in cui la divulgazione del numero di telefono, scritto nel bagno di un autogrill con la dicitura "disinibita e porca", con la conseguenza che la vittima riceveva diverse chiamate e messaggi per prestazioni sessuali e inserito quindi in un contesto persecutorio più ampio di minacce e molestie, si può considerare un precursore delle condotte esaminate, depotenziate dalla mancanza dell'utilizzo di Internet.

3. *Revenge porn* e la violenza contro le donne

Le statistiche rivelano che oltre l'80% delle vittime è di sesso femminile[32] ed è proprio tale ragione a fare del NCP, insieme al *cyberstalking* e al *sexist hate speech*, un fenomeno di violenza di genere[33] sul punto è interessante come l'Enciclopedia Italiana Treccani nella definizione di *revenge porn* fornisca una connotazione gender definendo la fattispecie come: "diffusione nella rete di immagini sessualmente esplicite senza il consenso del soggetto ritratto, che di solito è una donna, da parte di individui che intendono denigrare l'ex partner".[34] Si ritiene infatti che le donne vengano discriminate proprio nella manifestazione della propria sessualità. Secondo alcuni studiosi, in realtà, la NCP "is on a continuum with other forms of sexual violence".[35] La NCP quindi si può includere nel discorso del *Gender-based violence*. La tematica della violenza di genere contro le donne e gli obblighi degli Stati, in base al diritto internazionale, di prendere provvedimenti per prevenire tale violenza, punire gli autori e fornire sostegno alle vittime, sono stati argomenti costanti di discussione e di azioni a livello internazionale negli ultimi 30 anni.[36] Nonostante le numerose normative, politiche e altre misure adottate a livello internazionale e nazionale e i progressi che sono stati fatti, la violenza di genere contro le donne continua ad essere diffusa e centrale nel dibattito.

L'art. 3 della Convenzione sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica cd. "*Istanbul Convention*", definisce la "*gender-based violence*" come una violenza che:

> is directed against a woman because she is a woman or that affects women disproportionately, and "violence against women" as violation of human rights and a form of dis-

[32] Il Report "Violenza Contro le Donne un Anno di Codice Rosso" del Servizio Analisi Criminale del Ministero dell'Interno pubblicato ad ottobre 2020 ha rivelato che nel periodo dal 9 agosto 2019 all'8 agosto 2020 sono stati commessi in Italia 718 reati di NCP, ex art. 612 *ter* c.p. di cui l'81,62% le vittime erano di sesso femminile < https://www.istat.it/it/files//2018/04/Polizia_Un_anno_di_codice_rosso_2020.pdf > (04/21). La Cyber Civil Right Initiative ha calcolato nel 2014 una percentuale delle vittime di sesso femminile del 90%, cit. *supra* nota 28.

[33] Si veda European Parliament, "Cyber Violence and Hate Speech Online Against Women", Study for the FEMM Committee, settembre 2018, p. 11.

[34] Enciclopedia Italiana Treccani voce "*revenge porn*" (2016) e "pornovendetta" (2019) <https://www.treccani.it> (04/21).

[35] Cfr. McGlynn et al., "Beyond '*Revenge Porn*'", cit. nota 15.

[36] Diverse convenzioni e documenti internazionali e regionali sono state adottate per tutelare le donne da forme di discriminazione e violenza tra cui: la Convenzione internazionale sull'eliminazione di tutte le forme di discriminazione nei confronti della donna (CEDAW), adottata dall'Assemblea generale delle Nazioni Unite il 18 dicembre 1979 ed entrata in vigore il 3 settembre 1981, ratificata e resa esecutiva dall'Italia con legge n. 132 del 14 marzo 1985; la Dichiarazione sull'eliminazione della violenza contro le donne, è stata adottata con la risoluzione 48/104, Assemblea Generale delle Nazioni Unite, 20 dicembre 1993; Convenzione sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica cd. "Istanbul Convention", Consiglio d'Europa, 11 maggio 2011, ratificata ad oggi da 33 Paesi, ratificata in Italia il 10 agosto 2013.

crimination against women and shall mean all acts of gender-based violation that result in, or are likely to result in physical, sexual, psychological, or economic harm or suffering to women including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or private life.[37]

4. Criticità legate ad internet

La pornografia non consensuale, pur non essendo un crimine commesso esclusivamente online, è lì che trova la manifestazione più difficile e con le conseguenze più gravi. Come abbiamo visto in precedenza, Internet assume un rilievo importante nella commissione del crimine di NCP. Caletti rileva una escalation e inasprimento di aggressività delle condotte confrontando le vicende di David Feltmeyer[38] e di Tiziana Cantone,[39] nell'avanzare dell'informatica.[40] La pericolosità di Internet e delle nuove tecnologie è nella capacità moltiplicativa, una modalità potenzialmente idonea a raggiungere un numero indeterminato di persone. In Italia, pertanto, è stata prevista come aggravante quando i fatti siano commessi attraverso strumenti informatici o telematici.[41] Le notizie, o in questo caso le immagini, possono diventare virali, possono arrivare in ogni angolo della terra e la parvenza di anonimato e di non punibilità rende sicuri i "leoni da tastiera", che nascosti dietro a un computer non ritengono che il loro comportamento possa essere punito, o comunque corrono il rischio. Prima dell'avvento di Internet tale potenza di diffusione non era immaginabile.

Ci si chiede quindi cosa si può fare nella pratica per arginare il fenomeno. Da un lato è importante certamente che gli Stati, in misura sempre crescente, adottino una legislazione che preveda il reato di NCP, dall'altro è necessario che vi sia una maggiore collaborazione con gli *Internet Service Provider* (ISP), prestatori di servizi via web, che quali intermediari, creano un collegamento tra chi comunica una informazione e chi la riceve. Il mondo *cyber* è uno spazio molto particolare, la giurisdizione degli Stati ha dei contorni non ben delimitati e ci si affida ad attori privati per determinate tutele. L'Unione Europea ha portato l'attenzione sulla necessità di

[37] Art. 3 (a) "Istanbul Convention".

[38] David Feltmeyer, nell'aprile 2007, lasciò, sui tergicristalli delle auto parcheggiate di un viale principale di Chesterfield, dei dvd contenenti un video intimo che lo ritraeva mentre compiva atti sessuali con la sua ex fidanzata. Sulla copertina del dvd aveva appuntato nome, numero di telefono e indirizzo della stessa. Feltmeyer fu condannato per diffusione di immagini oscene e non per aver causato sofferenze all'ex fidanzata. Si veda a "Former Boyfriend Pleads no Contest over Sex DVDs", *Chesterfield Observer*, 25 aprile 2007, < http://www.chesterfieldobserver.it/news> .

[39] Tiziana Cantone è tristemente nota per essere il soggetto di un video, divenuto virale, che la ritraeva mentre aveva rapporti sessuali con altri ragazzi mentre il suo fidanzato registrava. Nel 2016 a distanza di un anno dalla diffusione del video Tiziana si è suicidata, non potendo sopportare il richiamo mediatico causato dalla diffusione del video. F. Facci, "Storia di Tiziana Cantone", *Il Post*, <https://www.ilpost.it/2016/09/15/storia-tiziana-cantone/ > (04/21).

[40] Si veda Caletti, "*Revenge porn* e tutela legale", cit. nota 8, pp.65-67.

[41] Art. 612(3) *ter* c.p.

cooperazione da parte di tutti i soggetti coinvolti nei processi comunicativi online.[42] Alcuni ISP stanno quindi adottando dei regolamenti per cercare di limitare i fenomeni di *cyberviolence*, tra questi ad esempio "Facebook"[43] ha adottato degli "*Standard* della *comunity*" al fine di rendere lo stesso un luogo sicuro in cui esprimersi.[44] Facebook ha quindi creato nel 2017 un programma pilota proprio per la prevenzione di casi di NCP o *sextortion*, prima quindi che vengano pubblicate le immagini, e, inoltre, ha introdotto una tutela successiva, nel caso in cui il materiale sia stato già diffuso sulle piattaforme. Per fare ciò, utilizzando delle nuove tecnologie che consentono la creazione di una firma digitale unica o *hash* (composta da valori numerici) di un'immagine o video che permette di essere confrontata con quelle di altri video e immagini, si riescono a individuare corrispondenze, e di conseguenza la possibilità di bloccare la pubblicazione o di eliminare i materiali già diffusi.[45]

La regolamentazione del cyberspazio crea molti interrogativi anche in relazione al diritto internazionale. Un questione molto importante è se sussista un obbligo dei *Service provider* di sorveglianza rispetto ai dati immessi da terzi su di un suo sito.[46] La Direttiva sul commercio elettronico n. 2000/31/CE[47] dà una risposta a tale interrogativo, in quanto ha sancito l'assenza di un obbligo generale di sorveglianza per

[42] Si veda la Risoluzione del Parlamento Europeo, P8_TA(2016)0441, "EU strategic communication to counteract anti-EU propaganda by third parties" sulla strategia della comunicazione dell'Unione per contrastare la propaganda di terzi che possa essere lesiva della democrazia, dello Stato di diritto e del rispetto dei diritti umani e delle liberta fondamentali, del 23 novembre 2016 e la Comunicazione della Commissione Europea n. 555 del 2017.

[43] Ma non solo, anche Google e Microsoft si sono attivate per combattere i fenomeni di NCP, predisponendo dei moduli per la rimozione delle immagini e l'impegno a rimuoverle in breve tempo (solitamente 24h).

[44] Al punto 8 di questi standard specificano che la piattaforma rimuove i contenuti che esprimono, alludono a o promuovono la violenza sessuale, le aggressioni a sfondo sessuale o lo sfruttamento sessuale e anche i contenuti che mostrano, sostengono o coordinano atti sessuali con persone non consenzienti per non agevolare rapporti non consensuali. Facebook, *Standards della community* <https://www.facebook.com/communitystandards/sexual_exploitation_adults > (05/21).

[45] Facebook, *Not without my consent – Programma pilota sulle immagini intime non consensuali* (NCII) < https://www.facebook.com/safety/notwithoutmyconsent/pilot >. In Italia il Garante della Privacy dall'8 marzo 2021 è stata attivato un programma di collaborazione con Facebook per la segnalazione di casi di NCP. G. Cerrina Feroni, "Sfida al Revenge porn dal Garante Privacy: il sito per denunciare sarà on line dall'8 marzo", Garante Privacy, 6 marzo 2021, <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9556114 > (04/21).

[46] A. Monti, "Rete, leggi e processi. Vita dura per le imprese Parte Seconda - Hosting e responsabilità per contenuti illeciti", *WebMarketing Tools,* 2002; V. Zeno Zencovich, Profili attivi e passivi della responsabilità dell'utente in Internet, in A. Palazzo, U. Ruffolo (eds), *La tutela del navigatore in Internet*, Milano, 2002, p. 137 s.; F. Di Ciommo, "Programmi-filtro e criteri di imputazione/esonero della responsabilità on-line. A proposito della sentenza Google/Vivi Down", *Diritto informatico*, 2010; M. De Cata M., *La responsabilità civile dell'Internet service provider*, Milano, 2010; F. Di Ciommo, "Internet, diritti della personalità e responsabilità aquiliana del provider", *Danno e responsabilità*, 1999, p. 756.

[47] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio europeo, 8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»), recepita in Italia dal D. Lgs. n. 70 del 2003.

gli ISP,[48] non sussistendo tanto meno l'obbligo di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. Gli stessi sono tenuti ad informare le autorità competenti prontamente degli illeciti rilevati e a condividere ogni informazione che possa aiutare a identificare l'autore della violazione. Sussiste pertanto un obbligo di collaborazione, la cui mancanza fa sì che gli stessi ISP vengano ritenuti civilmente responsabili dei danni provocati. La Commissione europea ha presentato, il 15 dicembre 2020, il cd. Digital Services Act (DSA),[49] con cui sono previste alcune modifiche e integrazioni alla Direttiva n. 2000/31/CE, in particolare con gli articoli 8 e 9 vengono individuati più in dettaglio le caratteristiche e gli aspetti peculiari degli ordini provenienti dalle autorità giudiziarie o amministrative nazionali "di contrastare i contenuti illegali" e "di fornire informazioni". Il DSA mira ad armonizzare una serie di vincoli sulla gestione dei servizi digitali - al momento regolamentati in maniera differente dai singoli Stati membri, a stabilire norme uniformi per un ambiente online sicuro, prevedibile e affidabile, in cui i diritti fondamentali sanciti dalla Carta siano tutelati in modo effettivo, a migliorare la trasparenza e a chiarire le responsabilità delle piattaforme online.

Da ciò sorge anche un altro interrogativo, in relazione a come vengono bilanciati fondamentali diritti umani, come la libertà di espressione e la tutela alla privacy e il diritto alla vita privata e familiare. La Corte Europea dei Diritti dell'Uomo (Corte EDU) che è volta a tutelare i diritti sanciti dalla Convenzione Europea dei Diritti dell'Uomo (CEDU) si è espressa più volte in relazione alla libertà di espressione, sancita dall'articolo 10 CEDU, ritenendo la stessa un elemento essenziale dello Stato democratico.[50] La libertà di espressione è intesa non solamente per le idee e informazioni ricevute favorevolmente, ma anche quelle che scioccano o offendono lo Stato o qualsiasi parte della popolazione.[51] L'Corte EDU ha però anche stabilito che la responsabilità in caso di diffamazione o di altri tipi di discorsi offensivi deve, in linea di principio, essere ammessa e costituire un rimedio efficace per le violazioni dei diritti della personalità.[52] Per quanto riguarda in particolare la diffusione su Internet di affermazioni considerate diffamatorie, le cui conseguenze possono essere ricondotte similmente anche ai casi di diffusione non consensuale di immagini, la

[48] Art. 15, 2000/31/CE.

[49] Proposta della Commissione Europea di Regolamento del Parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE del 15 dicembre 2020, COM(2020) 825 (final)**.**

[50] Corte EDU, caso *Handyside v. United Kingdom*, application No. 5493/72, 7 dicembre 1976.

[51] Si discute in dottrina sulla possibilità di ritenere la diffusione di immagini intime come "*truth speech*". Negli Usa il primo emendamento che garantisce la libertà di espressione, è di estrema importanza e non può essere limitato a meno che ciò non leda interessi generali. Di conseguenza, anche se non è mai stato applicato, le leggi che tutelano le vittime dal *revenge porn* potrebbero rischiare un vaglio di costituzionalità, in quanto il contenuto divulgato è vero. Si veda P.J. Larkin, "*Revenge porn*, State law and Free Speech", *Loyola of Los Angeles Law review*, pp. 57-60; J.A. Humbach, "The Constitution and *Revenge Porn*", *Pace Law Review*, 2014-2015, p. 220; si veda anche Citron e Franks "Criminalizing *revenge porn*" cit. *supra* nota 22.

[52] Corte EDU, caso *Delfi As v. Estonia*, application No. 64569/09, Grande Camera, 16 giugno 2015, para. 110

Corte ha osservato come il rischio di danno posto dai contenuti e dalle comunicazioni su Internet all'esercizio e al godimento dei diritti e delle libertà umane, in particolare il diritto al rispetto della vita privata, sia certamente più elevato di quello posto dalla stampa, e pertanto deve essere tutelato.[53]

L'analisi non può concludersi senza aver fatto riferimento al diritto all'oblio.[54] Il gestore di un motore di ricerca in Internet è responsabile del trattamento da esso effettuato dei dati personali che appaiono su pagine web pubblicate da terzi. Così, nel caso in cui, a seguito di una ricerca effettuata a partire dal nome di una persona, l'elenco di risultati mostrasse un link verso una pagina web che contiene informazioni sulla persona in questione, questa può rivolgersi direttamente al gestore oppure, qualora questi non dia seguito alla sua domanda, può adire le autorità competenti per ottenere, la deindicizzazione. Si può chiedere la deindicizzazione anche qualora tali dati risultino inadeguati, non pertinenti o non più pertinenti ovvero eccessivi in rapporto alle finalità per le quali sono stati trattati e al tempo trascorso. [55] Sicuramente nei casi di NCP mi sembra essenziale il diritto all'oblio, uno strumento utile per cercare di ridurre (almeno in parte) i danni. Non si possono sottacere, tuttavia, le difficoltà di eliminare completamente dal web qualsiasi traccia del materiale diffuso.

5. Proiezioni

L'esplosione quantitativa della rivoluzione telematica svela il rovescio della medaglia. Appare evidente come la sicurezza umana nello spazio cyber sia più che mai messa a dura prova da tipologie di reato che trovano la più grande espressione in Internet. A fronte degli enormi vantaggi, della libertà d'informazione, si hanno abusi nella rete e scambio di immagini, dati personali e notizie anche intime che troppo spesso travalicano il circuito fiduciario all'interno del quale queste informazioni sono state prodotte e/o hanno iniziato a circolare. Questo tipo di scambio può divenire virale, mai come in questa fase storica, nella contemporaneità, si può cogliere la devastante potenza di questa qualificazione. Restringendo l'osservatorio

[53] Ibid.

[54] Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), 27 aprile 2016 (UE GPDR) all'articolo 17(1) stabilisce il diritto alla cancellazione («diritto all'oblio»): "L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali […]".

[55] CGUE, Sentenza Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos. Causa C-131/12 13 maggio 2014. Per un approfondimento si veda J. Globocnik, "The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)", *GRUR International*, aprile 2020, pp. 380–388; G. Bevilacqua, "La dimensione territoriale dell'oblio in uno spazio globale e universale", *Federalismi.*it, 2019; S. Kulk e F. Zuiderveen Borgesius, "Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe" in J. Polonetsky, O. Tene , E. Selinger (eds), *Cambridge Handbook of Consumer Privacy*, Cambridge University Press, 2017.

alla pornografia "di vendetta", si può osservare come l'intreccio tra sentimenti negativi e ingiustificabili, esito ultimo di una mentalità patriarcale e violenta, e dispositivi telematici modernissimi possa amplificare il male e produrre danni. Il profilo psicologico si compenetra con quello della responsabilità, patrimoniale e penale. Disposizioni normative, a livello diverso sia nelle gerarchie delle fonti, sia sotto un profilo spaziale intervengono ad arginare e a reprimere il fatto illecito. Ma la velocità con cui si può propagare la diffusione e l'ampiezza planetaria della stessa sono pericoli da non sottovalutare, né la prevenzione può essere una soluzione definitiva, perché non corrisponde – evidentemente – a costumi ormai amplissimamente diffusi. La risposta tecnologica sta facendo primi ma importanti passi: l'individuazione automatica dei messaggi dannosi e il conseguente rapido provvedimento interdittivo da parte dei social e dei provider sembra oggi se non una panacea, almeno un argine a comportamenti che afferiscono alla sfera morale prima ancora che giuridica. La morale si può combattere in primo luogo con l'educazione e su questa, anche nello specifico, bisogna investire, nella convergenza di forze convergenti, dal diritto internazionale, che deve anche in questo ambito dare delle direttive agli Stati, ai diritti positivi nazionali, ai regolamenti delle grandi aziende che operano nel web, sia nella sensibilizzazione sempre più diffusa del pericolo prodotto da tali attività.

VIOLAZIONE DEL DIRITTO D'AUTORE ONLINE E RESPONSABILITÀ DEGLI INTERMEDIARI DELLA RETE

Ilaria Infante

"*L'écrivain propriétaire c'est l'écrivain libre.*
Lui ôter la propriété, c'est lui ôter l'indépendance."[1]

1. Introduzione

La tecnologia digitale e l'avvento di Internet hanno inevitabilmente messo in discussione i fondamenti del diritto d'autore, dal momento che la pubblicazione online permette ad un'opera creativa (libro, musica, film, foto, etc.) di essere pubblicata simultaneamente in tutto il mondo.

Da un lato ciò è sicuramente vantaggioso per gli autori, perché permette loro di diffondere le proprie opere e raggiungere un bacino di acquirenti potenzialmente illimitato, dall'altro però crea potenziali complicazioni in quanto espone le proprietà intellettuali a maggiori rischi di violazione. La pubblicazione e la diffusione non autorizzate di opere protette dal diritto d'autore sono infatti molto frequenti e gli utenti di Internet, affascinati dalla facilità e rapidità con le quali possono accedere a milioni di contenuti, spesso non percepiscono il disvalore della propria condotta.

Tuttavia, numerosi studi dimostrano che anche qualora gli utenti dovessero essere consapevoli dell'illegalità della pirateria digitale, essi raramente considerano il ricorso ad essa come poco etico dal momento che non ne traggono profitti economici.[2]

Del resto, definizioni più tradizionali di pirateria nell'ambito del diritto d'autore, in passato, facevano riferimento alla fabbricazione di copie non autorizzate di materiale protetto e allo sfruttamento delle stesse attraverso la distribuzione e la vendita.[3] Al contrario, con la diffusione su larga scala, attraverso Internet, di materiale protetto si è visto come un atto di pirateria possa verificarsi indipendentemente dalla motivazione commerciale degli utenti, in quanto ciò che rileva è il significativo danno agli interessi dei titolari sia del diritto d'autore che dei cosiddetti diritti connessi, ossia i diritti di quei soggetti che con la loro attività contribuiscono alla diffusione delle opere creative come gli interpreti, i produttori discografici e le emittenti radiotelevisive.

La *pirateria digitale* può essere infatti definita come la copia di prodotti digitali, quali software, documenti digitali, audio e video, senza l'autorizzazione e la re-

[1] "Lo scrittore che è proprietario della sua opera è uno scrittore libero. Togliergli la proprietà equivale a togliergli l'indipendenza." (traduzione dell'autrice) - V. Hugo, Discorso al Congresso Letterario Internazionale, Parigi, 17 giugno 1878.

[2] P. Stryszowski, D. Scorpecci, *Piracy of Digital Content*, Organizzazione per la cooperazione e lo sviluppo economico (OCSE), 2009, p. 12.

[3] J.A.L. Sterling, *World Copyright Law*, Sweet & Maxwell, Londra, 1999.

tribuzione degli aventi diritto;[4] sebbene essa possa ricomprendere anche la riproduzione e la distribuzione di copie fisiche di prodotti digitali, si verifica soprattutto online grazie alle opportunità senza precedenti offerte dalla rete. Internet, infatti, è il sistema perfetto per la distribuzione di opere e informazioni in maniera rapida ed efficace, nonché pressoché priva di costi.

Del resto il cyberspazio è il non-luogo per eccellenza: i dati in esso immessi "raggiungono ogni parte del mondo e il loro autore non è in grado né di controllarne l'accesso, né di prevedere quali percorsi essi seguiranno per ricongiungersi infine sullo schermo degli altri utenti".[5]

Una della maggiori difficoltà nel risalire agli autori di eventuali illeciti commessi online deriva proprio da questa caratteristica di non-luogo che fa sì che gli utenti della rete possano agire nel tendenziale anonimato; inoltre, gli atti di pirateria digitale, proprio in virtù della portata globale della rete, molto spesso coinvolgono individui di nazionalità differenti e quindi soggetti a giurisdizioni diverse, con l'ulteriore complessità di determinare quale sia la giurisdizione da applicare.

Alla luce di tali problematiche, una delle teorie avanzate, sia in dottrina che in giurisprudenza, è stata quella di prevedere una responsabilità indiretta per gli *intermediari della rete* (detti anche intermediari online), ossia quei soggetti che forniscono agli utenti servizi telematici, come ad esempio gli operatori di rete, i motori di ricerca o le piattaforme di condivisione di contenuti generati dagli utenti. Tuttavia, data anche la varietà dei servizi offerti, nonché la necessità di non ostacolare gli scambi e il traffico di dati, la normativa attualmente vigente nella maggior parte degli Stati, pur se con alcune differenze, prevede che gli intermediari della rete siano esonerati da responsabilità, a determinate condizioni e sulla base dell'attività concretamente svolta dal fornitore del servizio.

Il presente contributo, pertanto, dopo aver analizzato le diverse tipologie in cui si esplica al giorno d'oggi la pirateria digitale, si prefigura di analizzare il ruolo che gli attori non-statali, in questo caso gli intermediari della rete, possono svolgere in questo scenario, evidenziando la necessità di un accordo internazionale in merito alla responsabilità degli stessi per violazione del diritto d'autore, così da stabilire regole uniformi e garantire, da un lato, maggiori certezze per i *provider* e, dall'altro, la sicurezza e il rispetto dei diritti sia degli autori che degli utenti della rete.

2. Violazione del diritto d'autore online

Prima di soffermarsi sulle diverse modalità[6] con le quali è possibile commettere

[4] D.M. Vandiver, S. Bowman, A. Vega, "Music Piracy among College Students: An Examination of Low Self-Control, Techniques of Neutralization, and Rational Choice", *Southwest Journal of Criminal Justice*, 2021, pp. 92-111.

[5] S. Seminara, "La pirateria su Internet e il diritto penale", *Rivista trimestrale di diritto penale dell'economia*, 1997, pp. 71-114.

[6] J.P. Quintais, *Global Online Piracy Study. Legal Background Report*, Institute for Information Law, University of Amsterdam, Luglio 2018, p. 36 ss.

violazioni del diritto d'autore online, è opportuno fornire una definizione di tale diritto.

Innanzitutto occorre specificare che il termine diritto d'autore fa riferimento al regime giuridico tipico dei sistemi di *civil law*, mentre nei sistemi di *common law* si utilizza il termine *copyright*: il primo trova le sue radici nel giusnaturalismo e si focalizza sul soggetto meritevole di protezione, il secondo si basa sul principio utilitarista in base al quale concedere agli autori diritti sulle proprie opere favorisce la produzione di opere creative a beneficio dell'intera società.[7] Tuttavia sul piano pratico le differenze tra i due regimi sono poco significative, grazie anche all'armonizzazione operata dalle Convenzioni internazionali in materia, in primis la *Convenzione di Berna per la protezione delle opere letterarie e artistiche*;[8] per questo motivo, il presente contributo utilizza il termine diritto d'autore con accezione generale, inteso come il diritto che regola la proprietà delle opere dell'ingegno concedendo agli autori diritti esclusivi su di esse.[9]

La prima modalità attraverso la quale può realizzarsi una violazione del diritto d'autore è sicuramente il *download*, ossia l'atto attraverso il quale un utente trasferisce la copia di un qualsiasi file su un proprio dispositivo; va però sottolineato che non è il download in sé ad essere illegale, quanto piuttosto quello effettuato da una fonte non autorizzata: l'esempio classico è dato da chi scarica un file musicale da una piattaforma cosiddetta *peer-to-peer*[10] (P2P), quale l'antesignana *Napster* o le successive *eMule* e *The Pirate Bay*.

Del resto, per molti l'inizio della pirateria digitale su larga scala è fatto coincidere proprio con la nascita di *Naps*ter nel giugno 1999. Essa era la prima piattaforma utilizzata globalmente per la condivisione di file musicali senza l'autorizzazione degli aventi diritto e si basava su un sistema di server centrali che contenevano la lista dei sistemi connessi e dei file condivisi, mentre le transazioni vere e proprie avvenivano tra i vari utenti. Il programma fu al centro di un contenzioso giudiziario, che nel 2001 ne comportò la chiusura a seguito di un ricorso delle principali case discografiche americane per violazione indiretta del diritto d'autore, in quanto esso aveva "actual knowledge that specific infringing material is available using its system".[11]

Come affermato precedentemente, tuttavia, esistono anche sistemi leciti di

---

[7] P. Goldstein e P. B. Hugenholtz*, International Copyright. Principles, Law and Practice*, *(4th edition),* Oxford University Press, Oxford, 2019, p.13 ss.

[8] Convenzione di Berna per la protezione delle opere letterarie e artistiche, 9 settembre 1886, riveduta a Parigi il 24 luglio 1971, entrata in vigore il 10 ottobre 1974.

[9] J. Ginsburg, "Copyright", in Rochelle Dreyfuss e Justine Pila (a cura di), *The Oxford Handbook of Intellectual Property Law*, Oxford University Press, Oxford, 2018, p. 487.

[10] Con il termine *peer-to-peer* si intende un'architettura di rete decentrata, in cui i nodi sono gerarchizzati sotto forma di *client* o di *server* fissi o paritari (*peer* appunto) che possono fungere da *client* e da *server* verso gli altri nodi della rete. Esempio tipico di *peer-to-peer* è proprio la rete per la condivisione di file (*file sharing*).

[11] Court of Appeals for the Ninth Circuit (United States), *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, sentenza del 12 febbraio 2001, para. 1022: "conoscenza effettiva del fatto che, utilizzando il proprio sistema, fosse disponibile specifico materiale lesivo" (traduzione dell'autrice).

download, ossia quelli che avvengono dietro corrispettivo di pagamento su piattaforme dotate delle necessarie autorizzazioni dei titolari dei diritti. Ciò si verifica in quanto il download consiste in una riproduzione permanente di un'opera e come tale è soggetto alle restrizioni previste dal diritto di riproduzione, in base al quale soltanto gli autori hanno "il diritto esclusivo di autorizzare la riproduzione delle loro opere in qualsiasi maniera e forma".[12]

È importante sottolineare che anche tale diritto esclusivo può essere soggetto a limitazione qualora si verifichino le tre condizioni del cosiddetto "test a tre fasi", ossia: 1) quando si tratti di "taluni casi speciali"; 2) "purché una tale riproduzione non rechi danno allo sfruttamento normale dell'opera"; 3) e purché "non causi un pregiudizio ingiustificato ai legittimi interessi dell'autore".[13]

Nell'ambito del Diritto dell'Unione europea, ad esempio, la Direttiva 2001/29/CE (la cosiddetta Direttiva InfoSoc.) prevede, all'Articolo 5, un elenco esaustivo di limitazioni ed eccezioni per gli atti di riproduzione temporanea privi di rilievo economico, tra cui quelli che riguardano "le riproduzioni su qualsiasi supporto effettuate da una persona fisica per uso privato e per fini né direttamente, né indirettamente commerciali".[14]

Tuttavia, come evidenziato dalla Corte di giustizia dell'Unione europea (CGUE) nel caso *ACI Adam*,[15] l'eccezione per copia privata non ricomprende le riproduzioni originate da fonti illegali o non autorizzate, pertanto quando il download derivi da tali fonti, esso non può rientrare nella portata dell'eccezione e costituisce violazione del diritto d'autore.

Altra metodologia attraverso la quale è possibile accedere a materiale protetto dal diritto d'autore è lo *streaming*, ossia "quella particolare modalità di diffusione di un flusso audio/video da una sorgente a una o più destinazioni, mediante una rete telematica, che presuppone che i dati trasmessi vengano riprodotti man mano che arrivano a destinazione, e che non siano memorizzati […] all'interno dell'apparecchiatura che li riceve".[16]

La differenza fondamentale con il download consiste nel fatto che con lo streaming la memorizzazione del contenuto di cui si usufruisce è temporanea, in quanto avviene nella RAM (Random Access Memory, ossia un tipo di memoria volatile in cui i dati vengono automaticamente cancellati alla chiusura del programma) e comporta la creazione di copie parziali nella *cache*.

Per questo motivo è difficile ricomprendere lo streaming passivo, ovvero quello

---

[12] Convenzione di Berna, cit. *supra* nota 8, art. 9(1).

[13] Ibid. art. 9(2).

[14] Direttiva 2001/29/CE del Parlamento europeo e del Consiglio del 22 maggio 2001 sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, GU L 167, 22.06.2001, art. 5(2)(b).

[15] CGUE, Causa C-435/12, *ACI Adam BV e a. contro Stichting de Thuiskopie e Stichting Onderhandelingen Thuiskopie vergoeding*,10.04.2014, para. 45.

[16] E. Prospetti, "La circolazione delle opere digitali", in Giuseppe Cassano, Guido Scorza e Giuseppe Vaciago (a cura di), *Diritto dell'Internet. Manuale operativo. Casi, legislazione, giurisprudenza*, CEDAM, Padova, 2012.

dell'utente che usufruisce del servizio, tra le forme vietate di riproduzione. Ciononostante, i danni causati agli interessi legittimi dei titolari dei diritti sono comunque molteplici e, nel tentativo di contrastare questo fenomeno, sono nate negli anni piattaforme legali di streaming on-demand che permettono agli utenti, a seguito della sottoscrizione di un abbonamento mensile o annuale, di accedere in qualsiasi momento e su qualsiasi dispositivo ad un vasto catalogo di contenuti audiovisivi (esempi tipici sono Netflix, Prime Video, Disney Plus e Spotify).

Discorso diverso va fatto, invece, per i soggetti che effettuano l'*upload*, ossia coloro che diffondono online materiale protetto dal diritto d'autore senza l'autorizzazione dei titolari dei diritti, perché in quel caso è universalmente riconosciuto che si verifichi una violazione.

Un'altra modalità di violazione del diritto d'autore online, che si sta diffondendo sempre di più negli ultimi anni è il cosiddetto *stream-ripping*, consistente nel creare su un proprio dispositivo una copia permanente di un'opera protetta, che sarebbe invece fruibile lecitamente soltanto in streaming, cioè mediante riproduzione meramente temporanea. In pratica, attraverso un'applicazione apposita o un sito di stream-ripping, dai contenuti audiovisivi di piattaforme come YouTube vengono estrapolati (*ripped* appunto) file audio che, scaricati sul computer, permettono agli utenti di ascoltare una determinata canzone illimitatamente, senza alcun compenso per i soggetti aventi diritto alla tutela autoriale.

Sembrerebbe quindi possibile applicare anche per lo stream-ripping, lo stesso ragionamento effettuato per il download e considerarlo, a ragione, un atto di riproduzione permanente, soggetto alle stesse limitazioni evidenziate in precedenza.

Del resto, nonostante la relativa novità della tecnica, anche la giurisprudenza sta compiendo importanti passi avanti nell'evidenziazione dell'illegalità di questa pratica, come testimonia una recente sentenza[17] dell'Alta corte di giustizia inglese. Nel caso in questione, le principali case discografiche britanniche avevano richiesto di bloccare l'accesso ad alcuni siti di stream-ripping, evidenziando come questa pratica sia oggi una delle minacce più incombenti per l'industria musicale. Il giudice dell'Alta corte ha convenuto che gli operatori di tali siti abbiano violato il diritto d'autore dei ricorrenti, in quanto, in piena consapevolezza delle loro azioni, hanno reso disponibile ai propri utenti l'accesso ad opere protette che, senza il loro intervento, non sarebbero state accessibili per il download, se non a determinate condizioni (ovvero soltanto in caso di sottoscrizione al servizio premium di YouTube e in ogni caso non oltre un limitato periodo di tempo).

3. Responsabilità degli intermediari online

La crescita esponenziale di nuove e sempre più sofisticate modalità attraverso le quali violare il diritto d'autore online ha comportato una grossa sfida per i titolari

[17] [2021] EWHC 410 (Ch), England and Wales High Court (Chancery Division), *Young Turks Recordings Ltd & Ors v British Telecommunications Plc & Ors*, sentenza del 25 febbraio 2021.

dei diritti, anche e soprattutto per l'impatto economico causato dalla pirateria digitale. Nonostante, storicamente, il fenomeno delle copie non autorizzate di opere dell'ingegno sia sempre esistito, l'effetto che esso aveva sui ricavi degli aventi diritto era relativamente insignificante, se paragonato alle perdite derivanti dalla diffusione di copie digitali messe a disposizione di una moltitudine potenzialmente illimitata di utenti.[18]

Come affermato in precedenza, il problema principale consiste nella difficoltà di individuare con assoluta certezza gli autori degli illeciti online, unitamente al rischio di mancato risarcimento del danno subito.

Per ovviare a ciò e nel contempo cercare di porre un freno alla pirateria digitale, una delle soluzioni avanzate è stata quella di agire nei confronti dei soggetti che forniscono i servizi di rete agli utenti.

Gli intermediari online sono infatti più facilmente individuabili dei privati cittadini e assicurano potenzialmente una maggiore efficacia risarcitoria, dal momento che sono organizzati sotto forma di impresa e dispongono di un patrimonio economico sicuramente superiore a quello dei singoli pirati digitali, oltre ad essere frequentemente situati nella stessa giurisdizione dei titolari dei diritti lesi.[19]

Prima di capire se, e a che titolo, gli intermediari online possano dirsi responsabili delle violazioni commesse dai loro utenti occorre chiarire cosa si intende più precisamente quando si fa riferimento a questa categoria di attori non-statali.

In dottrina è stato osservato come "[t]he term 'internet intermediary' is [an] unhappy abstraction. These words must be used to describe many entities which seem to share little in common, other than activity that uses electronic computer networks. […] They are a genus whose many members' common feature have never been systematically identified".[20]

Tuttavia una definizione condivisibile potrebbe essere quella contenuta in un rapporto dell'OCSE del 2010 secondo cui "'Internet intermediaries' bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties".[21]

Spesso il termine 'intermediari della rete' viene utilizzato come alternativo di *Internet Service Provider* (ISP), ma in realtà gli ISP rappresentano soltanto una del-

[18] D. Rowland, U. Kohl e A. Charlesworth, *Information Technology Law*, *(5th edition)*, Routledge, Londra e New York, 2017, p. 144.

[19] Ibid., p. 152.

[20] "Il termine 'intermediari di Internet' è un'astrazione infelice. Tali parole devono essere usate per descrivere molti soggetti che sembrano avere poco in comune, a parte il fatto di realizzare attività che utilizzano reti informatiche. […] Essi costituiscono un genere in cui la caratteristica comune dei suoi molti membri non è mai stata identificata in maniera sistematica." (traduzione dell'autrice) – J. Riordan, *The Liability of Internet Intermediaries*, Oxford University Press, Oxford, 2016, p. 29.

[21] "Gli 'intermediari di Internet' riuniscono e facilitano le transazioni tra terzi su Internet. Essi forniscono l'accesso, memorizzano, trasmettono e indicizzano contenuti, prodotti e servizi originati da terzi su Internet o forniscono servizi basati su Internet a terzi" (traduzione dell'autrice) – *The Economic and Social Role of Internet Intermediaries*, OCSE, Aprile 2010.

le diverse categorie[22] in cui è possibile suddividere gli intermediari online. In particolare, gli ISP sono quegli intermediari che forniscono servizi Internet agli utenti dietro stipulazione di un contratto, come ad esempio le compagnie telefoniche (TIM, Vodafone, Fastweb, etc.) che consentono l'accesso alla rete.

Un'altra categoria di intermediari è rappresentata da quelli che facilitano la navigazione degli utenti nel web, come i motori di ricerca (ad esempio Google e Yahoo) o gli aggregatori di notizie (Google News o Reddit), ma più in generale qualsiasi sito che raggruppi *link* collegati ad un argomento specifico o che fornisca *hyperlink* (collegamenti ipertestuali) ad altri siti. È importante sottolineare come rientrino in questa categoria anche le piattaforme P2P, come *The Pirate Bay*, che permettono agli utenti di cercare e scaricare illegalmente musica, film e videogame in formato *torrent*.[23]

Da ultimo, un'altra tipologia di intermediari della rete da segnalare è quella delle piattaforme di condivisione di contenuti generati dagli utenti, il cui esempio tipico è rappresentato da YouTube, ma che ricomprende anche siti a fini commerciali come le aste online (Ebay) e i social network come Facebook e Instagram.

Da quanto affermato poc'anzi, si evince come gli intermediari online, in sostanza, gestiscano la diffusione e la distribuzione di qualsiasi contenuto digitale e, per questo motivo, sin dagli albori del cyberspazio ci si è chiesti se essi potessero o meno essere ritenuti responsabili per eventuali illeciti connessi a tali contenuti.

Sul finire degli anni '90, quando Internet era un settore in piena espansione e si temeva che la nascente industria dei fornitori di servizi di rete non potesse sopportare il peso di una completa responsabilità per atti commessi dai propri utenti, con possibili conseguenze per l'interesse pubblico in generale, si giunse, negli Stati Uniti prima e in Europa poi, ad un compromesso tra le varie parti in causa.[24]

I legislatori stabilirono, infatti, che i *provider* dovessero essere esenti da responsabilità per le attività illecite commesse dagli utenti nell'utilizzo dei loro servizi, fintantoché essi fossero pronti a cooperare nel rimuovere o disabilitare l'accesso ai contenuti riconosciuti come illeciti.

Questo regime di *safe harbour* (letteralmente "porto sicuro) fu introdotto dapprima negli Stati Uniti con il *Communications Decency Act*[25] (CDA) del 1996 e il *Digital Millennium Copyright Act*[26] (DMCA) del 1998 e, successivamente, in Europa attraverso la *Direttiva europea sul commercio elettronico*[27] del 2000 che impose agli Stati membri l'obbligo di implementare disposizioni normative che stabilissero limitazioni alla responsabilità degli intermediari online.

---

[22] Rowland, Kohl e Charlesworth, cit. *supra* nota 18, p. 75.

[23] Torrent è l'estensione per file, utilizzata dai programmi P2P, che contiene tutte le informazioni necessarie per scaricare il file stesso.

[24] L. Edwards, *Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights*, rapporto commissionato dall'Organizzazione mondiale della proprietà intellettuale (OMPI), 2010, p. 6.

[25] 47 U.S. Code § 230.

[26] 17 U.S. Code § 512.

[27] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno, GU L 178, 17.07.2000.

Il quadro normativo di riferimento negli Stati Uniti è di tipo *verticale*, in quanto la sezione 230 del CDA prevede l'immunità dei *provider* in generale, in applicazione della cosiddetta clausola del "buon Samaritano"[28], mentre il DMCA fa riferimento esclusivamente alle limitazioni di responsabilità in caso di violazione del diritto d'autore.

Al contrario, il regime di responsabilità degli intermediari previsto dalla Direttiva sul commercio elettronico è di tipo *orizzontale* poiché trascende dal tipo di illecito commesso dai fruitori dei servizi, anche se ha mutuato dal DMCA la distinzione in diverse modalità di esenzione da responsabilità, sulla base delle varie funzioni concretamente svolte dai prestatori.

3.1. La disciplina statunitense

Il DMCA, infatti, prevede l'immunità dalle azioni risarcitorie per: 1) i *provider* che trasmettono comunicazioni transitorie su una rete digitale come, ad esempio, le compagnie di telecomunicazione);[29] 2) i *provider* che svolgono funzioni di *system caching*, ossia di memorizzazione solo temporanea di dati prodotti da un terzo e destinati ad essere ritrasmessi, come il servizio di Amazon Elasticache;[30] 3) i *provider* che svolgono attività di memorizzazione permanente di informazioni fornite dagli utenti (il cosiddetto *hosting*), come le piattaforme di condivisione di video;[31] 4) e infine, i *provider* che forniscono *link* ad indirizzi web che contengono materiale che viola il diritto d'autore (*information location tools*, detti anche *linking tools*), come ad esempio gli aggregatori di ricerca.[32]

Per quanto riguarda la prima categoria, l'immunità del *provider* si verifica solo se la trasmissione dei dati sia effettuata da un soggetto terzo e se i servizi offerti dal prestatore siano eseguiti mediante un processo tecnico di carattere automatico; e, inoltre, se esso non sia coinvolto nella selezione dei contenuti da diffondere né nella scelta dei suoi destinatari, limitandosi a trattenere i dati senza modificarli per un lasso di tempo necessario alla mera trasmissione.

Per la seconda categoria, il *safe harbour* si realizza a patto che il materiale sia messo a disposizione da un soggetto diverso dal *provider* e sia ritrasmesso ad un terzo soggetto. Occorre poi che la memorizzazione sia effettuata attraverso un processo tecnico automatico e il materiale sia trasmesso senza modificarne il contenuto. Infine, qualora il materiale reso disponibile online sia in violazione del diritto d'autore, il *provider* dovrà agire rapidamente per rimuoverlo o disabilitarne l'accesso.

Per le ultime due categorie, infine, il principio di irresponsabilità si applica al

---

[28] In base a tale clausola, il *provider* che dimostri di aver agito in buona fede per bloccare l'accesso a materiale considerato offensivo o in ogni caso lesivo dei diritti altrui, sarà esente da qualsiasi responsabilità.

[29] Cit. *supra* nota 26, § 512 (a).

[30] Ibid., § 512 (b).

[31] Ibid., § 512 (c).

[32] Ibid., § 512 (d).

verificarsi di determinate condizioni. Innanzitutto, il prestatore dei servizi non deve avere conoscenza effettiva delle violazioni del diritto d'autore commesse dagli utenti; nel caso in cui il *provider* abbia la capacità di controllare le attività degli utenti e sia quindi a conoscenza dell'illiceità dei contenuti veicolati, esso non dovrà trarre alcun beneficio economico dalla condotta illecita; qualora, infine, il *provider* sia informato di una violazione e riceva una notifica di rimozione (cosiddetta procedura di *notice and take down*) del contenuto ritenuto lesivo del diritto d'autore da parte degli aventi diritto, esso dovrà agire tempestivamente per rimuoverlo o disabilitarne l'accesso.

3.2. La disciplina europea

Prima di soffermarsi sulla normativa europea attualmente vigente è opportuno sottolineare che il 15 dicembre 2020 la Commissione europea ha presentato formalmente una proposta di regolamento denominato *Digital Service Act* (DSA), volta proprio a modificare la disciplina della Direttiva sul commercio elettronico. Il DSA, infatti, pur mantenendo le medesime distinzioni previste dalla Direttiva in merito alle varie funzioni svolte dai prestatori intermediari, introdurrebbe l'obbligo per gli stessi di agire contro i contenuti illegali e di fornire informazioni alle autorità giudiziarie o amministrative nazionali, e prevederebbe, inoltre, una parziale applicazione del principio del buon Samaritano.[33]

Per quanto riguarda la Direttiva europea attualmente vigente va ricordato come, a differenza del modello statunitense, essa non disciplina specificatamente il regime di responsabilità degli intermediari in riferimento alle violazioni del diritto d'autore, bensì adotta un approccio di tipo orizzontale che prescinde dal tipo di illecito.

Negli Articoli 12-14 la Direttiva fa riferimento alle varie funzioni svolte dai prestatori di servizi della società dell'informazione distinguendo tra tre diverse tipologie di *provider*. In primo luogo la Direttiva menziona i *provider* che si limitano a svolgere attività di semplice trasporto di dati (*mere conduit*), come i fornitori di servizi e-mail; successivamente, i *provider* che realizzano un'attività di memorizzazione temporanea (*caching*); ed infine i *provider* che svolgono un'attività di memorizzazione permanente (*hosting*), come YouTube.

Sulla base dell'Articolo 12, il prestatore che si limiti a trasmettere informazioni fornite da un destinatario del servizio gode dell'immunità in relazione alle predette informazioni a patto che non dia inizio alla trasmissione, non selezioni il destinatario della stessa e non modifichi né selezioni le informazioni trasmesse.[34]

Secondo l'Articolo 13 il *provider* non è responsabile della memorizzazione au-

[33] Per un approfondimento sulle novità del DSA si veda ad esempio: G. Caggiano, "La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea", *I Post di AISDUE*, III, 2021, Focus "Servizi e piattaforme digitali", n. 1; G.M. Ruotolo, "Digital Services Act e Digital Markets Act tra responsabilità dei fornitori e rischi di bis in idem", SIDIBlog, <http://www.sidiblog.org/2021/03/29/digital-services-act-e-digital-markets-act-tra-responsabilita-dei-fornitori-e-rischi-di-bis-in-idem/>, (04/21).

[34] Direttiva sul commercio elettronico, art. 12(1).

tomatica, intermedia e temporanea delle informazioni fornite da un terzo a patto che non modifichi tali informazioni, che si conformi alle condizioni di accesso alle stesse e che aggiorni regolarmente le copie *cache* secondo le modalità riconosciute dalle imprese del settore. Inoltre affinché si abbia l'immunità occorre anche che il prestatore agisca immediatamente per rimuovere le informazioni memorizzate, non appena venga a conoscenza del fatto che la fonte delle informazioni sia stata rimossa o che l'accesso ne sia stato disabilitato, oppure che un organo giurisdizionale o un'autorità amministrativa ne abbia disposto la rimozione.[35]

Infine, l'Articolo 14 prevede che il prestatore che memorizza le informazioni richieste dal destinatario del servizio sia esente da responsabilità penale a condizione che non sia effettivamente al corrente del fatto che l'attività o l'informazione sia illecita, ed esente da responsabilità civile a patto che non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione.[36] In ogni caso, non appena il *provider* dovesse venire a conoscenza di tali fatti, per poter invocare l'immunità dovrà agire immediatamente per rimuovere le informazioni o disabilitarne l'accesso.

L'ultimo paragrafo dell'Articolo 14, tuttavia, "lascia impregiudicata la possibilità, per un organo giurisdizionale o un'autorità amministrativa[…]di esigere che il prestatore ponga fine ad una violazione o la impedisca nonché la possibilità, per gli Stati membri, di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime".[37]

Da ciò si evince che il regime appena descritto non esclude la possibilità che agli intermediari online venga richiesto di porre in essere misure contro la violazione del diritto d'autore e del resto l'Articolo 8(3) della Direttiva InfoSoc. obbliga gli Stati membri ad assicurarsi "che i titolari dei diritti possano chiedere un provvedimento inibitorio nei confronti degli intermediari i cui servizi siano utilizzati da terzi per violare un diritto d'autore o diritti connessi".[38]

Tuttavia, come ha sottolineato la CGUE in diverse occasioni, le azioni inibitorie devono sottostare ad una serie di limitazioni, operando un equo bilanciamento tra diritti fondamentali.

Nel caso *Promusicae*,[39] ad esempio, la Corte di Giustizia ha affermato che qualsiasi inibitoria volta ad ottenere da un *provider* i nominativi dei presunti autori di atti lesivi del diritto d'autore deve garantire il giusto equilibro tra il diritto alla proprietà intellettuale[40] e il diritto al rispetto della vita privata[41] e alla tutela dei dati personali.[42]

---

[35] Ibid., art. 13(1).
[36] Ibid., art. 14(1).
[37] Ibid., art. 14(3).
[38] Direttiva InfoSoc., art. 8(3).
[39] CGUE, Causa C-275/06, *Productores de Música de España (Promusicae) contro Telefónica de España SAU*, 29.01.2008.
[40] Carta dei diritti fondamentali dell'Unione europea, art. 17(2).
[41] Ibid., art. 7.
[42] Ibid., art. 8.

Nel caso *Scarlet* la Corte ha evidenziato che, sebbene la tutela del diritto di proprietà intellettuale rientri nei diritti tutelati dalla Carta dei diritti fondamentali del'Unione europea, "*non può desumersi né da tale Carta né dalla giurisprudenza della stessa Corte che tale diritto sia intangibile e che la sua tutela debba essere garantita in modo assoluto*".[43] Pertanto, un'ingiunzione volta ad imporre a un *provider* di predisporre un sistema di filtraggio preventivo di tutte le comunicazioni sulle reti elettroniche in modo da bloccare lo scambio illegale di file è da considerarsi sproporzionata ed incompatibile sia con l'Articolo 15[44] della Direttiva sul commercio elettronico, sia con i diritti fondamentali tutelati dalla Carta, nello specifico il diritto alla privacy degli utenti e il loro diritto a ricevere informazioni,[45] nonché il diritto alla libertà di impresa[46] dell'intermediario.

Tuttavia, lo sviluppo delle piattaforme P2P e di quelle a contenuto generato dagli utenti come YouTube e i social network ha messo in discussione il quadro normativo fin qui riferito, perché tali intermediari online, svolgendo attività di indicizzazione e filtraggio di contenuti condivisi dagli utenti, ben potrebbero essere esposti al rischio di vedersi riconosciuti quali responsabili diretti della diffusione illecita di opere protette dal diritto d'autore.

Ad esempio, la piattaforma P2P *The Pirate Bay* è stata ritenuta dalla CGUE direttamente responsabile di atti di comunicazione al pubblico (rientrante tra i diritti esclusivi degli autori e dei titolari dei diritti connessi e per questo necessitante della loro espressa autorizzazione), in quanto gli amministratori di tale piattaforma, con piena cognizione di causa, svolgevano un ruolo imprescindibile nella messa a disposizione delle opere protette dal diritto d'autore, indicizzando ed elencando i file torrent che permettevano agli utenti di localizzare e condividere tali opere.[47]

La scriminante sembra essere proprio quella della concreta conoscenza, da parte del gestore di una piattaforma di condivisione di video o di file, dell'avvenuta messa a disposizione di contenuti lesivi del diritto d'autore e il non aver fatto nulla per rimuoverli o l'averne addirittura promosso scientemente la condivisione, come ribadito dalla CGUE nella recentissima sentenza delle cause riunite *YouTube e Cyando*.[48] Tuttavia la Corte, pur specificando che spetti alle corti nazionali verificare la sussistenza dei predetti criteri per stabilire se le piattaforme di condivisione di contenuti siano responsabili dirette di violazioni del diritto d'autore, nel caso in que-

---

[43] CGUE, Causa C-70/10, *Scarlet Extended SA contro Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24.11.2011, para. 43.

[44] "Nella prestazione dei servizi di cui agli articoli 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite."

[45] Cit. *supra* nota 40, art. 11.

[46] Ibid., art. 16.

[47] CGUE, Causa C-610/15, *Stichting Brein contro Ziggo BV e XS4All Internet BV*, 14.06.2017, para. 36. Per un maggiore approfondimento sulla sentenza in questione si veda ad es.: E. Rosati, "The CJEU *Pirate Bay* judgment and its impact on the liability of online platforms", *European Intellectual Property Review*, 2017, pp. 737-748.

[48] CGUE, Cause riunite C-682/18 e C-683/18, *Frank Peterson contro Google LLC e a. e Elsevier Inc. contro Cyando AG*, 22.06.2021, para. 84.

stione ha specificato che YouTube non compie atti di comunicazione al pubblico, in quanto non interviene nella creazione e selezione dei contenuti caricati dai suoi utenti e anzi ha messo in atto delle misure tecniche volte a contrastare la condivisione di materiali protetti sulla sua piattaforma.[49]

3.3. La nuova Direttiva europea sul diritto d'autore e sui diritti connessi nel mercato unico digitale

È opportuno sottolineare però che in quest'ultimo caso le interpretazioni fornite dalla Corte riguardano la normativa applicabile all'epoca dei fatti in questione e non, invece, il regime attualmente istituito dall'articolo 17 della *Direttiva europea sul diritto d'autore e sui diritti connessi nel mercato unico digitale*,[50] approvata il 17 aprile 2019.

Tale articolo, infatti, introduce una nuova disciplina per i prestatori di servizi di condivisione di contenuti online, stabilendo che tali intermediari nel concedere l'accesso ad opere protette dal diritto d'autore effettuano un atto di comunicazione al pubblico, anche se tali materiali sono di fatto caricati dai propri utenti, e per questo motivo sono chiamati ad ottenere l'autorizzazione degli aventi diritto, ad esempio mediante uno specifico accordo di licenza.[51]

Nel caso in cui tale autorizzazione non sia concessa, la Direttiva dispone un regime specifico di responsabilità dei prestatori per atti non autorizzati di comunicazione al pubblico di opere e materiali protetti, a meno che essi non dimostrino di:

a) aver compiuto i massimi sforzi per ottenere un'autorizzazione, e

b) aver compiuto, secondo elevati standard di diligenza professionale di settore, i massimi sforzi per assicurare che non siano disponibili opere e altri materiali specifici per i quali abbiano ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti; e in ogni caso,

c) aver agito tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere dai loro siti web le opere o altri materiali oggetto di segnalazione e aver compiuto i massimi sforzi per impedirne il caricamento in futuro.[52]

Come evidenziato dalla dottrina,[53] tali obbligazioni possono essere implementa-

[49] Ibid., para. 92-94.

[50] Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE, GU L 130, 17.05.2019.

[51] Ibid., art. 17(1).

[52] Ibid., art. 17(4).

[53] Si veda *ex multis*: M.L. Montagnani, "Virtues and Perils of Algorithmic Enforcement and Content Regulation in the EU – A Toolkit for a Balanced Algorithmic Copyright Enforcement", *Case Western Reserv Journal of Law, Tech. & Internet*, 2020; e della stessa autrice anche il contributo "A New Liability Regime for Illegal Content in the Digital Single Market Strategy", in Giancarlo Frosio (a cura di), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, Oxford, 2020, p.295.

te solo attraverso un sistema di filtraggio automatico dei contenuti caricati dagli utenti, con il conseguente rischio che i gestori delle piattaforme, per non incorrere nella responsabilità, possano bloccare preventivamente qualsiasi contenuto prima ancora della sua pubblicazione, in contrasto con i diritti fondamentali degli utenti tra cui il diritto alla libertà di espressione e di informazione.[54] Del resto, l'Articolo 17(4)(b)(c) è attualmente in discussione presso la CGUE a seguito di un ricorso di annullamento presentato dal governo polacco proprio sulla base della presunta incompatibilità di tale sistema di filtraggio con il diritto alla libertà di espressione.[55]

La Commissione europea è intervenuta sulla questione nelle linee-guida[56] recentemente pubblicate e volte a sostenere la corretta implementazione dell'Articolo 17 negli Stati membri,[57] affermando che, in linea di principio, i gestori delle piattaforme dovrebbero attuare il blocco automatizzato (ovvero l'uso della tecnologia per impedire il caricamento) soltanto in relazione ai caricamenti manifestamente lesivi del diritto d'autore o dei diritti connessi, mentre quelli non manifestamente lesivi dovrebbero essere ammessi online ed essere oggetto di una verifica umana *ex post* soltanto qualora gli aventi diritto inviino una segnalazione.

Tuttavia, secondo la Commissione, una verifica umana *ex ante* da parte degli intermediari potrebbe comunque essere necessaria in caso di contenuti (segnalati preventivamente dagli autori) la cui disponibilità online non autorizzata potrebbe causare un significativo danno economico ai titolari dei diritti, come ad esempio i film in anteprima o gli *highlights* di trasmissioni recenti di eventi sportivi.[58]

4. Conclusioni

Alla luce di quanto affermato finora emerge come, a seguito dell'entrata in vigore della Direttiva 2019/790, possano acuirsi ancora di più le differenze tra i due principali regimi di responsabilità degli intermediari online, quello europeo e quello americano, con conseguenti effetti negativi tanto per i *provider* quanto per gli utenti.

Mentre negli Stati Uniti e negli altri paesi di *common law* gli intermediari online continueranno ad avere al massimo una responsabilità indiretta in merito alle

[54] Per un'analisi più approfondita si veda: J. Reda, J. Selinger e M. Servatius, "Article 17 of the Directive on Copyright in the Digital Single Market: a Fundamental Rights Assessment", studio commissionato da GFF (Società per i diritti civili), 16.11.2020.

[55] CGUE, Causa C-401/19, *Polonia/Parlamento e Consiglio.*

[56] Comunicazione della Commissione al Parlamento europeo e al Consiglio, Orientamenti relativi all'articolo 17 della direttiva 2019/790/UE sul diritto d'autore nel mercato unico digitale, 04.06.2021.

[57] È opportuno evidenziare che sebbene la Direttiva dovesse essere implementata entro il 7 giugno 2021, di fatto al tempo in cui si scrive sono pochissimi gli Stati che lo hanno fatto: tra questi Olanda e Germania, mentre in Italia è stata approvata il 21.04.2021 soltanto la legge di delegazione europea per il recepimento della Direttiva.

[58] Per una visione molto critica su queste disposizioni si veda: J. Reda e P. Keller, "European Commission back-tracks on user rights in Article 17 Guidance", Kluwer Copyright Blog, <http://copyrightblog.kluweriplaw.com/2021/06/04/european-commission-back-tracks-on-user-rights-in-article-17-guidance/>, (06/21).

violazioni del diritto d'autore commesse online, in Europa, a specifiche condizioni, essi potranno essere riconosciuti anche come direttamente responsabili di tali violazioni.

Tuttavia, mentre le grosse multinazionali potrebbero adottare con più facilità strumenti tecnici diversi a seconda del regime giuridico in cui si trovano ad operare, alcune compagnie più piccole potrebbero persino decidere di non fornire più i loro servizi in Europa. In ogni caso questa situazione potrebbe porre un freno all'idea di Internet come siamo abituati a conoscerlo, ossia uno spazio privo di confini, e renderlo più frammentato, in quanto alcune informazioni potrebbero non essere più disponibili per tutti, con conseguente lesione dei diritti fondamentali degli utenti.

Sarebbe auspicabile, quindi, un'armonizzazione a livello globale del regime di responsabilità degli intermediari online, attraverso un trattato internazionale che possa stabilire regole uniformi per tutti.

Fin dalla fine del 1800 gli accordi internazionali hanno cercato di armonizzare la disciplina del diritto d'autore e dei diritti connessi, tuttavia tali norme nulla dicono in merito alla responsabilità dei prestatori di servizi dal momento che, all'epoca dei trattati più recenti in materia, ossia quelli istituiti nell'ambito dell'OMPI,[59] il web era in pieno sviluppo e non si riuscì a trovare un accordo su una questione così complessa.

Come detto precedentemente, infatti, nella seconda metà degli anni '90 Internet si stava appena diffondendo e la mancanza di regole ben definite era proprio dovuta alla volontà di permettere questa espansione senza gravare troppo sulla nascente industria dei fornitori di servizi della rete, con il rischio di un rallentamento nelle operazioni che avrebbe potuto comportare conseguenze negative anche per gli utenti. Tuttavia uno spazio sempre connesso come la rete necessita più che mai di una disciplina armonizzata che possa dettare regole omogenee.

Un trattato internazionale comporterebbe, infatti, una serie di vantaggi per tutte le parti in gioco (autori, aziende fornitrici di servizi e singoli utenti), perché grazie a norme applicabili a livello internazionale gli intermediari non dovrebbero più sottostare all'incertezza quando operano in diversi Stati e, al contempo, ai titolari del diritto d'autore verrebbe garantita una maggiore protezione.

Tuttavia, considerando che gli Stati Uniti hanno aderito alla Convenzione di Berna soltanto nel 1989, dopo ben un secolo dalla sua entrata in vigore, non è da escludere che il cammino verso un accordo tra i due distinti modelli sia ancora molto lungo.

[59] Trattato OMPI sul diritto d'autore, 20 dicembre 1996, entrato in vigore il 06 marzo 2002; Trattato OMPI sulle interpretazioni, le esecuzioni e i fonogrammi, 20 dicembre 1996, entrato in vigore il 20 maggio 2002.

CONCLUDING REFLECTIONS: WHAT IS THE ROLE OF THE STATE IN ENHANCING HUMAN SECURITY IN NAVIGABLE SPACES?

Claudia Cinelli

This edited Volume mainly explored the role of non-State actors (NSAs) in maritime areas and cyberspace, especially when they act as do-gooders in advancing comprehensive responses to complex challenges for enhancing human security; or, on the contrary, when their actions constitute relevant threats to human security. Despite their relevant differences, maritime and cyberspace were here considered as both navigable spaces, addressed, respectively, by Section I and Section II.

Starting from Section I on human security at sea, the evolving notion of human security was especially explored in relation to the migrant rescue operations by non-governmental organizations (NGOs) in the Mediterranean. Special attention, amongst others, was also paid to the difficulties and challenges faced by the commercial private ships when rescuing people in distress at sea. It is also interesting to mention that a relevant analysis was offered with reference to the NGOs role during the migration crisis in the North of Macedonia and the subsequent consequences occasioned by the implementation of the EU-Turkey Agreement.

At the same time, this Section asked the nature of State obligations when facing the need of safeguarding human life at sea. Furthermore, an important look was devoted to the cooperation at the EU external borders control as an undoubtedly essential tool to render assistance and ensure human security. However, recently, NGOs denounced European authorities' involvement for the forced return of escaping migrants to Libya, according to their 'remote control' practices, including the spotting of boats and the coordination of interceptions from distance.

In addition, human security at sea was also addressed by reflecting on how the information and communication technologies (ICTs) have been revolutionizing the maritime shipping sector. Where, on one hand, the increasing use of the ICTs could benefit the international maritime shipping sectors, it could, at the same time, facilitate cyber-attacks on the maritime security industry, including digital piracy attack. Equally, it has not been forgotten that the use of such technologies could be very useful for preventing maritime piracy actions.

Passing to Section II of this Volume, this opened by taking up the topic of migration from a cross-cut approach to human security within maritime and cyber space. In this sense, the impact of the ICTs on the migrants' lives could be good thanks to online services and applications; but, also bad for services and applications which facilitate the access to migrants' personal data and privacy. Consequently, this Section highlighted the role of NGOs in emphasizing that migrants should not be victims of unlawful interference when using the Internet. This interference raises awareness, amongst other things, about human trafficking and mi-

grant smuggling characterized by online recruitment through fraudulent advertising websites or virtual brokerage agencies, international marriage agencies etc.

More generally, this Section II underlined that the 'technology is not neutral.' Indeed, systems of digital surveillance might facilitate abuses related to access to the user's personal data by third parties, while 'hackers with ethics' and NGOs are fighting for the protection of the right to privacy and other human rights and freedoms.

Given the wealth of data available today, artificial intelligence (AI) is becoming one of the ways to keep up with increasingly transnational criminals. AI-powered crime-fighting tools were here analysed also as tools for large businesses within the context of neuromarketing, which benefits from neuroscience research for defining marketing opportunities. However, in the military field, cyber tools offer alternatives to achieve military targets that other means and methods of warfare do not, but it also carries risks. In this sense, it was underlined that humanitarian organisations call upon States to take a clear position on how international humanitarian law applies in cyberspace.

Furthermore, Section II of this edited Volume addressed discussions on how international law protects human rights online, with a specific reference to the protection of victims of non-consensual pornography pushes (revenge porn) as well as victims of copyright violation, while exploring responsibilities of Internet service providers.

Finally, this Volume addressed a complex analysis of the impact of cyberspace in re-shaping political power and influence of contemporary society, with particular attention to the several and increasing uses of cyber tools during the Covid-19 pandemic. Technologies for persuasion and algorithmic induction of behavior have been facilitated by the close relationship between social distancing, isolation and new ways of managing cognitive work where NSAs played a protagonistic role.

Against this background, the research findings outlined in this Volume shows that the regulation of navigable spaces taken into consideration is vastly fragmented and that the role played by NSAs in addressing key issues of human security is very complex as they reflect a large number of very different actors with distinct roles, for good and for bad, in maritime areas and cyberspace. There is an acute need to better distinguish the various types of NSAs to identify strategies to enable States to fight the critical role of NSAs; or, alternatively, take full advantage of their contributions in the elaboration and implementation of international standards.

Consequently, as concluding reflections, the main question to be addressed is the role of the State in enhancing human security in navigable spaces. To address this question, it must be emphasized that this edited Volume studies the field of international law of navigable spaces, especially navigable national spaces as those related to maritime areas where migrant rescue operations mainly occur and those related to the virtual domain of cyberoperations. Notwithstanding, the utilization of both aforementioned spaces reflects a perspective of protection of common values and interests which tends to overcome, at least in part, the spatial criterion of State (territorial) sovereignty.

With the passage of time, the power exercised by each State as a single and independent entity in the international arena turns out to be increasingly *less exclusive* within its national boundaries, with the realization of common interests and values, including that of enhancing human security. Indeed, the analysis proposed by this Volume is conducted with an interdisciplinary view that looks at the transformation and evolution of the international law system and, more precisely, at its cardinal principle: State sovereignty and jurisdiction.

The amazing growth in the number and modes of participation of NSAs in navigable spaces is having the effect of transforming certain features of the State sovereignty-based system. On one hand, States seem reluctant to limit sovereign power within their territorial boundaries, thus making changes in the international system very hard to achieve. That seems evident for cyberspace where its virtual dimension makes the territorial criterion of sovereignty quite anachronistic. That is valid, in my opinion, also for other sectors of international law aimed at the progressive affirmation and consolidation of common values, such as those related to human security at sea. When human lives at sea are endangered and when human dignity is in jeopardy, maritime national borders become irrelevant.

On the other hand, the rise of different international actors that enjoy significant independence, as well as their increased relevance in the field of human security, is putting the effectiveness of State sovereignty-based system into question. However, the current fashion of referring to NSAs as 'new' actors in the maritime areas and cyberspace seems inappropriate. They are not 'new' as such. What is new, however, is the amazing growth in the number of NSAs and the lack of a harmonious normative pattern in the relationships between States and NSAs. And this is important because at present NSAs are deeply involved in several areas of significant international activity in navigable spaces.

Accordingly, I am not suggesting that the impact of different utilizations of navigable spaces in the international regulatory frameworks, as NSAs become relevant and powerful for good or for bad, results necessarily in the increasing irrelevance and powerlessness of States as such. On the contrary, in my view, the current transformation of the regulation of navigable spaces is heading towards the search for new ways and means to enforce States policy actions in enhancing human security standard-setting and, in so doing, to combine the voluntary energy and legitimacy of the civil society with the financial interest of private actors' business.

With no early guarantee of success, States will indeed be required to advance a *responsible behaviour*. Recent developments promoted by the United Nations General Assembly seem to pave the way towards the development of responsible State behavior in the use of cyberspace for peaceful purposes.[1] The use of navigable spaces for peaceful purposes is not a novel conception in international law.[2] It is sufficient to

[1] In this context UN General Assembly resolutions and other relevant documents are available at UN website <https://www.un.org/disarmament/ict-security/> (07/21).

[2] UN General Assembly resolution, UN Doc. 2749 (XXV), 17 December 1970, paras. 5 and 8. See, T. Treves, "La notion d'utilisation des espaces marins à des fins pacifiques dans le nouveau droit de la mer", *Annuaire Français de Droit International*, 1980, pp. 687-699.

recall the 1982 UN Convention on the Law of the Sea, whose Preamble underlines the historical significance of this Convention "… as an important contribution to the maintenance of peace, justice and progress for all peoples of the world"[3] and reads that it "… will promote the peaceful uses of the seas and oceans".[4]

Such emerging and re-emerging developments seem to find their rationale in the more general context of the progressive implementation of multilateral cooperation instruments that are aimed at sensitizing States towards the exercise of *responsible sovereignty*.[5] That requires States to cooperate across national borders to address transnational threats and to exhibit a high degree of collaboration with other entities towards the enforcement of human security.[6]

State territorial sovereignty has indeed been slowly transformed and/or eroded because of searching the best way of serving the 'interests of human beings,'[7] as individuals as well as human community, i.e. humanity.

The growing limitations and restrictions that international law places on the State reflect a complex mosaic of different instruments, legally binding and non-binding, which model – or at least try to model – responsible State behavior. In other words, a behavior that pursues the search for a balance between the realization of particular and common interests and values. The search for this balance is certainly not a new issue in international law that recalls its classic functions as already identified by the Permanent Court of International Justice (PCIJ) in relation to the well-known 1927 *Lotus* case: 'to regulate the relations between [these] co-existing independent communities or with a view to the achievement of common aims.'[8] At

[3] United Nations Convention on the Law of the Sea, 10 December 1982, entered into force 16 November 1994. See, Preamble, para. 1.

[4] Ibid 4. See also some provisions of the Convention, especially Arts 88, 141, 143, 147, 155, 240, 242, 246, and 301.

[5] The origin of the concept of responsible sovereignty dates back to the mid-Nineties in relation to the duty of the State to diligently face the needs raised by situations of armed conflict with the aim of re-establishing the rule of law and providing for the basic needs of the population. See, F.M. Deng et alii., *Sovereignty as Responsibility: Conflict Management in Africa*, Washington, 1996. As regard to the evolution of the concept, see, *Report of the High-level Panel on Threats, Challenges and Change*, UN Doc. A/59/565, 2 December 2004; *Report of the Secretary-General: In larger freedom,* UN Doc. A/59/2005/Add.3, 26 May 2005; *Responsible Sovereignty: International Cooperation for a Changed World*, 15 July 2008, available at *United Nations website* <www.un.org> (07/21). For a contemporary analysis, see, C. Cinelli, *La disciplina degli spazi internazionali e le sfide poste dal progresso tecnico-scientifico*, Giappichelli Editore, Torino, 2020, p. 49 ff.

[6] On June 2021, the Human Development Report Office at UNDP organized a virtual symposium on human security to revisit such concept in the light of unprecedented transformations of the current digital era of 21 century, such as migration crisis, COVID-19 pandemic, climate change, and new and emerging ITCs threats. *United Nations Trust Funds for Human Security. What's new* <https://www.un.org/humansecurity/whats-new-2/> (07/21).

[7] P. Allott *et alii*, 'Review Essay Symposium: Philip Allott's Eunomia and The Health of Nations Thinking Another World: This Cannot Be How the World Was Meant to Be. An event to mark the retirement of Professor Philip Allott, Professor of International Public Law, University of Cambridge, 28-29 May 2004,' *European Journal of International Law*, 2005, pp. 255-353, p. 262.

[8] Permanent Court of International Justice, *The case of SS "Lotus"*, Judgment of 7 September 1927, p. 18.

that time, the PCIJ used the disjunctive conjunction: regulate coexistence *or* pursue common aims. If now we pause to reflect on the increasing diversity of international actors and consider 'international law in her infinite variety',[9] we are prompted to ask whether the international law of spaces of today is in fact different today from that of previous eras. Perhaps today, instead of the use of the disjunctive conjunction when identifying the main functions of the international, the use of the copulative one - that is: regulate coexistence *and* pursue common aims -, would have been more appropriate since, thanks to the progress of humanity, we live in an increasingly interdependent way.

I therefore believe that the achievement of common aims is to be currently considered, at least in a certain sense, as a condition *sine qua non* for the self-preservation of States themselves. The evolution of international law towards an ever-greater protection of common values comes not only from solidarity aims, whose effective implementation is often not a priority of the States, but comes, above all, from a sort of 'instinct' of self-preservation as a particular interest of each State and, at the same time, common to all States. Self-preservation would be difficult to pursue if the use of navigable spaces were to take place in contexts of human insecurity.

Therefore, at present, while the principle of State sovereignty persists in its essence, what, in my opinion, gives innovative connotations to the international law of navigable spaces is *how* to regulate relations between NSAs and States as well as between independent States themselves within the process of transformation, for some *humanization*,[10] of the international order. That does not fit easily into the structures of territorial sovereignty-based system of international law. Too much of it operates outside the traditional binding forms of law.

The role of the State in enhancing human security in navigable spaces will probably result in hybrid standard-setting procedures and rules and instruments. Furthermore, soft law of responsible State behaviour rules enjoys a certain importance in international law, notwithstanding their softness. It indeed may be an alternative and potentially powerful means of conceptualizing the future development of international law of navigable spaces.

---

[9] R.R. Baxter, "International Law in 'Her Infinite Variety'", *The International and Comparative Law Quarterly*, 1980, pp. 549-566.

[10] J.A. Carrillo Salcedo, *Soberanía de los Estados y derechos humanos*, Tecnos, Madrid, 2001. Reference is made to a process of "humanización del orden internacional" (p. 14). In more general terms, see also A.A. Cançado Trindade, *International Law for Humankind: Towards a New Jus Gentium*, 3rd edition, Brill, Leiden/Boston, 2020.

List of Contributors

Sara Bellezza, Borderline –Europe. Contact sb@borderline-europe.de

Giorgia Bevilacqua, Researcher of International Law, Law Department, Università degli Studi della Campania Luigi Vanvitelli. Contact giorgia.bevilacqua@unicampania.it

Fenella Billing, Associate Professor, Syddansk Universitet - University of Southern Denmark. Contact febi@sdu.dk

Gianvito Brindisi, Researcher of Philosophy of Law, Università degli Studi della Campania Luigi Vanvitelli. Contact Gianvito.Brindisi@unicampania.it

Roberta Catalano, Associate Professor of Private Law, Università degli Studi della Campania Luigi Vanvitelli. Contact Roberta.catalano@unicampania.it

Claudia Cinelli, Researcher in in International Law, Università degli Studi di Pisa, Contact claudia.cinelli@unipi.it

Carlo Corcione, Managing Director, Ocean Cogemar - D'Amato Shipowners Group. Contact carlocorcione@gmail.com

Caroline Cornella, PhD Student in International Law, Université Jean Moulin Lyon 3. Contact caroline.cornella1@univ-lyon3.fr

Adele Del Guercio, Researcher of International Law, Università degli Studi di Napoli "L'Orientale". Contact adeledelguercio@gmail.com

Federica De Simone, Researcher of Criminology, Law Department, Università degli Studi della Campania Luigi Vanvitelli. Contact federica.desimone@unicampania.it

Giuliana Doria, Research Fellow of International Law, Università degli Studi della Campania Luigi Vanvitelli. Contact giuliana.doria@unicampania.it

Christian Frier, Assistant Professor, Department of Law, Syddansk Universitet - University of Southern Denmark. Contact cfr@sam.sdu.dk

Mireille Hildebrandt, Institute of Computing and Information Science, Science Faculty -Radboud University**,** Contact m.hildebrandt@cs.ru.nl

Ilaria Infante, PhD Student in International Law, Università degli Studi della Campania Luigi Vanvitelli. Contact ilaria.infante@unicampania.it

Olga Koshevaliska, Associate Professor, Dean at the Faculty of Law, Goce Delcev University – Stip, Macedonia. Contact olga.gurkova@ugd.edu.mk

Nassim Madjidian, Associate Researcher, University of Hamburg; Legal Adviser Sea-Eye. Contact nassim.madjidian@uni-hamburg.de

Elena Maksimova, Assistant Professor at the Faculty of Law, Criminal law Department, University of Goce Delcev, Stip, North Macedonia, and Vice – Dean for education. Contact elena.ivanova@ugd.edu.mk

Fabio Marcelli, Researcher of International Law, Institute for International Legal Studies - National Research Council (ISGI-CNR). Contact fabio.marcelli@cnr.it

Michele Mastroianni, Adjunct Professor of Programming Elements, Engineering Department, Università degli Studi della Campania Luigi Vanvitelli. Contact michele.mastroianni@unicampania.it

Kiara Neri, Maître de conférences (Associated Professor), Université Jean Moulin Lyon 3, Director of the International Law Center, Director of the Master Law of International Organisations. Contact, kiara.neri@univ-lyon3.fr

Ana Nikodinovska'Krstevska, Associate Professor of EU Law and EU Foreign policy, Goce Delcev University – Stip, Macedonia. Contact ana.nikodinovska@ugd.edu.mk

Haidi Sadik, Sea Watch. Contact haidisadik@gmail.com

Francesco Schettino, Associate Professor of Economics, Law Department, Università degli Studi della Campania Luigi Vanvitelli. Contact francesco.schettino@unicampania.it

Fulvio Vassallo Paleologo, Vice-president, ADIF- Associazione Diritti e Frontiere. Contact vassallofulvio111@gmail.com

Paolo Vignola, Adjunct Lecturer, Escuela de Literatura, Universidad de las Artes de Guayaquil, Ecuador Technological University of Dublin. Contact paolo.vignola@uartes.edu.ec

Maria Chiara Vitucci, Full Professor of International Law, Law Department, Università degli Studi della Campania Luigi Vanvitelli. Contact chiara.vitucci@unicampania.it

AssIDMer – Cahiers de l'Association Internationale du Droit de la Mer
Papers of the International Association of the Law of the Sea

1. G. Andreone, A. Caligiuri, G. Cataldi (a cura di), *Droit de la mer et emergences environnementales*, 2012
2. José Manuel Sobrino Heredia (a cura di), *La contribution de la Convention des Nations Unies sur le droit de la mer a la bonne gouvernance des mers et de oceans*, 2014
3. A. Del Vecchio, F. Marrella (a cura di), *International Law and Maritime Governance*, 2016
4. Andrea Caligiuri (a cura di), *Governance of the Adriatic and Ionian Marine Space*, 2016
5. N. Ros, F. Galletti (a cura di), *Le droit de la mer face aux "Méditerranées". Quelle contribution de la Méditerranée et des mers semi-fermées au droit international de la mer?*, 2016
6. Andrea Caligiuri, *L'arbitrato nella convenzione delle Nazioni Unite sul diritto del mare*, 2018
7. Gabriela A. Oanta (a cura di), *Law of the Sea and Vulnerable Persons and Groups*, 2019
8. Simone Carrea, *I rapporti tra Stati e imprese nel diritto del mare tra attribuzione della bandiera delega di funzioni e sponsorship*, 2020

Finito di stampare nel mese di settembre 2021
presso la *Grafica Elettronica* - Napoli