The Big Data of International Migration: Opportunities and Challenges for States under International Human Rights Law

DR ANA BEDUSCHI*

Technology, as the epitome of our contemporary society, permeates the realm of international migration. Migrants and refugees are increasingly using mobile phones and digital features available online to prepare for migration and while on the move. Concurrently, advances in computer science allow for progressively more accurate analysis of the data generated by mobile devices and online searches. In particular, big data can be used to determine specific behavioral patterns, geolocation and human interactions. This article investigates the implications of these technological advances for States under international human rights law. It argues that big data can and should be used as a tool for the protection of migrants’ human rights by enhancing both decision-making and measures to prevent unnecessary deaths at sea, ill-treatment and human trafficking of migrants. Consequently, the article examines whether the development of new technologies can affect States’ capabilities for the identification of individuals in need of protection. It posits that to the extent that protection is mandated by human rights instruments, States may have a positive obligation to use available technologies to identify and assist vulnerable migrants. It evaluates this possibility against the protection of migrants’ right to life, the prohibition of torture, inhuman and degrading treatment, and the prohibition of slavery and forced labour. In doing so, the article also emphasizes the limits and risks posed by the unrestrained use of new technologies, notably with respect to the protection of migrants’ right to privacy and data protection.

* Senior Lecturer in Law, University of Exeter, UK. Earlier versions of this article were presented at the ESIL 2017 Conference, Interest Group on Migration and Refugee Law, Workshop on “The Future of International Migration Law” in Naples, Italy on 6 September 2017, and at the ASIL Midyear Meeting, Research Forum, in St Louis, United States on the 28 October 2017. I am grateful to the participants for their helpful comments. I would like to express a special word of thanks to Dr Kubo Mačák, Professor Michael N. Schmitt, Professor Helena Wray, and Mr Milan Tahraoui for their valuable insights and instructive comments.
# TABLE OF CONTENTS

I. INTRODUCTION ..................................................................................................................................................... 2

II. BIG DATA AS A COMPLEMENTARY TOOL FOR INTERNATIONAL MIGRATION MANAGEMENT ................................................................. 5

III. BIG DATA AS A VALUABLE TOOL FOR THE PROTECTION OF VULNERABLE MIGRANTS ................................................................. 10
   A. Jurisdiction and State Obligations ..................................................................................................................... 10
   B. The Positive Obligation to Prevent Migrant Deaths at Sea ............................................................................. 13
   C. Protection of Migrants at Risk of Ill-Treatment and Human Trafficking ....................................................... 22

IV. LIMITS AND RISKS OF USING BIG DATA IN INTERNATIONAL MIGRATION ............................................................... 26
   A. Migrant Safety and Protection ........................................................................................................................ 26
   B. Migrant Privacy and Data Protection ............................................................................................................. 29

V. CONCLUSION ............................................................................................................................................................... 33

---

## I. INTRODUCTION

Technology is ever present in the ongoing global migration crisis.¹ Migrants and refugees are increasingly using mobile phones and digital features available on Facebook or Google to communicate with family members, to find better routes, and to stay informed about the situation in transit and destination countries.² At the same time, advances in computer science allow for progressively more accurate aggregation and analysis of the data generated by mobile devices and online searches, determining specific behavioural patterns and human interactions.³ Yet, research

---

¹ The term migrants is used here to encompass regular and irregular immigrants as well as asylum-seekers.
is scarce in relation to the use of big data analysis in international migration management and its implications for the protection of migrants’ human rights.4

Big data can be defined as the ‘large volumes of high velocity, complex and variable data that require advanced techniques and technologies to enable the capture, storage, distribution, management, and analysis of the information.’ Part of this data originates in interactions mediated by social media channels or online platforms that allow users to create and exchange content.6 This type of ‘big social data’ constitutes a major part of human-generated data, such as text, images, audio, and video.7 ‘Big social data’ therefore can be defined as ‘large data volumes that relate to people or describe their behaviour and technology-mediated social interactions in the digital realm’.8 Additionally, individuals leave digital footprints by simply searching for information via online search engines such as Google.9 Migrants’ digital footprints, whether originating in social media interactions or relating to online searches, can be used to determine individual behaviour and also to inform trends in migratory flows.10

---

6 Social media is a term that encompasses social networks (e.g. Facebook), blogs (e.g. WordPress), microblogs (e.g. Twitter), social news (e.g. Reddit), media sharing (e.g. YouTube), wikis (e.g. Wikipedia), and review sites (e.g. TripAdvisor). See Amir Gandomi & Murtaza Haider, Beyond the hype: big data concepts, methods, and analytics, 35 INT. J. INFORM MANAGE 137 (2014) 142 (for a definition of social media and a discussion of social media analytics); Andreas M. Kaplan & Michael Haenlein, Users of the world, unite! The challenges and opportunities of Social Media, 53 BUSINESS HORIZONS 59 (2010) (describing the concept of social media, and discussing how it differs from related concepts such as Web 2.0 and User Generated Content).
7 Gandomi & Haider, supra note 6, at 138 & 143 (explaining that text, images, audio, and video are examples of unstructured data which amounts to 95% of all big data, whereas structured data such as the tabular data found in spreadsheets or relational database constitutes only 5% of all existing data).
8 See Olguzhan Gencoglu et al., Conceptualizing Big Social Data, 4 J. BIG DATA 1 (2017).
9 See Ekaterina Olshannikova et al., Conceptualizing Big Social Data, 4 J. BIG DATA 1 (2017).
Against the backdrop of the ongoing migration crisis, the protection of migrants’ human rights in the digital era and the potential obligations of States to identify and assist vulnerable migrants are of great relevance. The article investigates the implications of these technological advances for State obligations under international human rights law (IHRL). It argues that the development of modern technologies can enhance the capabilities of States for the identification of individuals in need of protection. It examines big data from an angle that is not yet fully explored in the academic literature. Rather than analysing big data solely as an instrument of surveillance and control, the article argues that big data can and should be used as a tool for the protection of migrants’ legal rights. It suggests that protection can improve decision-making and facilitate measures to prevent unnecessary deaths at sea, ill-treatment and human trafficking of migrants. It posits that, to the extent that protection is mandated by human rights instruments, States may have a positive obligation to use the available technologies to identify and assist vulnerable migrants.

This possibility is evaluated against the protection of three core human rights set forth by universal and regional human rights treaties: the right to life, the prohibition of torture, inhuman and degrading treatment, and the prohibition of slavery and forced labour. The choice of rights is based on their nature and significance. The prohibition of torture, inhuman and degrading treatment, and the prohibition of slavery and forced labour are absolute, while the right to life is


12 As respectively provided by Article 4 of the UDHR; Article 7 of the ICCPR; Article 3 of the ECHR; Article 5 of the ACHR.

13 As respectively provided by Article 5 of the UDHR; Article 8 of the ICCPR; Article 4 of the ECHR; Article 6 of the ACHR.

14 Article 15 (2) of the ECHR provides no possibility of derogation from Articles 3 and 4 ECHR in times of emergency or war; Article 27 (2) of the ACHR also establishes no derogations from the right to life, right to humane treatment and prohibition of slavery in times of war or emergency; Article 4 (2) of the ICCPR also provides that there should be no derogation in relation to Articles 6, 7 and 8 of the ICCPR in times of public emergency. See also Questions Relating to the Obligation to Prosecute or Extradite (Belgium v. Senegal), Judgment, 2012 I.C.J. Rep. 422, ¶ 99 (July 2012) (affirming that “the prohibition of torture is part of customary international law and it has become a peremptory norm (jus cogens)”), Soering v. United Kingdom, App. No. 14038/88, ¶ 88 (Eur. Ct. H.R., Jul. 7, 1989) (affirming the absolute prohibition of torture and of inhuman or degrading treatment or punishment under the terms of the Convention); Separate Opinion of Judge ad hoc J. Dugard in Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Rwanda), Judgment, 2006 I.C.J. Rep. 86, ¶ 10 (February 2006) (counting the prohibitions on aggression, genocide, torture and slavery and the advancement of self-determination as norms of jus cogens); Fazenda Brasil Verde Workers v. Brasil, Preliminary Objections, Merits, Reparations and Costs, Judgment,
considered a fundamental right and a prerequisite for the enjoyment of all other human rights. Additionally, questions relating to respect for the right to privacy and data protection are examined insofar as they set limits on the use of big data vis-à-vis international migration. The article draws upon the jurisprudence of international human rights courts and quasi-judicial bodies, in particular the European Court of Human Rights (ECtHR), the Inter-American Court of Human Rights (IACtHR) and the Human Rights Committee (HRC).

The analysis proceeds in three consecutive steps. Firstly, the article examines the changes in State capabilities and the uses of big data for better decision-making in international migration management. Secondly, it assesses the possibility of using big data as a tool of protection of vulnerable migrants. In particular, it investigates whether States have a positive obligation to use available technologies to identify and assist vulnerable migrants. Thirdly, it examines the limits and risks of the uses of big data in the field of international migration. The article concludes by calling on States to adopt a rights-based approach in this area as new technologies evolve.

II. BIG DATA AS A COMPLEMENTARY TOOL FOR INTERNATIONAL MIGRATION MANAGEMENT

A good understanding of migratory patterns is a key asset for informed decision-making. However, traditional statistical tools based on administrative sources, national population censuses and sample surveys present important disadvantages. For instance, sample surveys and national

---

15 See McCann and others v. the United Kingdom, App. No. 18984/91, ¶ 147 (Eur. Ct. H.R., Sept. 27, 1995) (affirming that Article 2 ECHR providing for the right to life “enshrines one of the basic values of the democratic societies making up the Council of Europe”); Baldeón García v. Peru, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 147, ¶ 82 (Apr. 6, 2006) (affirming that “the right to life is a fundamental right, the full exercise of which is a prerequisite for the enjoyment of all other human rights”).

16 See infra Section IV, B.

17 Marzia Rango, How big data can help migrants, WORLD ECONOMIC FORUM, 2 (October 5, 2015) available at https://www.weforum.org/agenda/2015/10/how-big-data-can-help-migrants/ (explaining that these traditional statistical sources have important limitations); Peter Struijs et al., Official statistics and Big Data, BIG DATA & SOCY 1, 2
population censuses can be resource-intensive and time-consuming. The accuracy and relevance of such traditional tools are also limited to the time at which the data is collected in the sense that they only measure past behaviour. These factors limit the utility of traditional tools for predicting migratory trends.

Reception of migrants and refugees in the context of large scale displacement could be more efficiently planned and managed if State authorities in transit and destination countries were willing to use a combination of big data and traditional statistical data effectively. For instance, traditional statistical data and mobility forecasts were certainly available to European countries in the summer of 2015, when the upshots of the Syrian conflict were severely shown in terms of migration. The European Border and Coast Guard Agency (Frontex) had pointed out that “the unprecedented number of migrants crossing illegally the external borders has roots in the fighting in Syria that has resulted in the worst refugee crisis since the Second World War.” Yet, the European response to the large influxes of asylum-seekers from Syria was highly unsatisfactory. As summarized by Professor Guy Goodwin-Gill, “the current crisis in the movement of people was, if not predictable, then at least foreseeable as a consequence of demographic pressure, turmoil, civil strife

(2014) (explaining that big data sources “may be used to substitute or supplement more traditional data sources, such as questionnaire and administrative data” in the context of location data).

18 See notably, Rango, supra note 17, at 2; Andrew McAfee & Erik Brynjolfsson, Big Data: The Management Revolution, HARV. BUS. REV. 1, 6 (2012) (explaining that real-time big data analysis in the context of real property retail was more efficient in predicting near-term forecasts on the housing market than the official sources).


21 Frontex, Annual Risk Analysis 2015, 9 (Apr., 2015) available at http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2015.pdf (explaining that the ‘the unprecedented number of migrants crossing illegally the external borders has roots in the fighting in Syria that has resulted in the worst refugee crisis since the Second World War. Indeed, most of the detections at the borders concerned migrants from Syria, who later applied for asylum within the EU’).

and long-standing conflicts.” Indeed, large movements of refugees and migrants could have been better addressed if decision-makers had paid more attention to the existing indicators, intelligence and available statistical data in 2015.

Big data could provide an additional advantage for decision-makers as the information is not exclusively obtained through traditional State bodies and authorities. Data collection relates, for instance, to mobile phone usage, social media and other types of online service usage, and online searches. All of these are person-generated data. Individuals have in principle consented to the collection, storage and sometimes use of their data by the social media channels and online services. Furthermore, research demonstrates that it is possible to use Wireless Fidelity (WiFi) network connected to mobile devices such as smartphones to identify the device and estimate its location. Besides, migrants leave a considerable digital footprint as a result of their activities

24 EUROSTAT, Asylum applicants and first instance decisions on asylum applications: 2014, 8 & 23 (March 20, 2015) available at http://ec.europa.eu/eurostat/documents/4168041/6742650/KS-QA-15-003-EN-N.pdf/b7786ce9-1ad6-4720-8a1d-430f0c55018 (explaining that there was a substantial increase of number of asylum applicants during 2014 in the 28 Member States of the EU with a breakdown by applicants’ nationalities. This dataset was entirely based on administrative sources provided to Eurostat by the Member States relevant authorities and agencies, indicating that traditional statistical tools were available for consultation). See also Frontex, FRAN Quarterly Quarter, 4 & 8 (2015) available at http://frontex.europa.eu/assets/Publications/Risk_Analysis/FRAN_Q4_2014.pdf (mainly using statistical data provided by participating States); Frontex, Annual Risk Analysis, 9 (2015) available at http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2015.pdf (indicating that the main sources originate in statistical data from member States and other EU agencies). See also Satoko Horii, The effect of Frontex's risk analysis on the European border controls, 17 EUR. POL. & Soc’y 242, 247 (2016) (explaining how the common risk analysis model operates within the context of Frontex and how EU member States provide key data for the risk assessment).
28 Alfredo Alessandri et al., WiFi positioning and Big Data to monitor flows of people on a wide scale, PROC. EUR. NAV. Conf. 2017, 322, 322 (2017) available at https://ec.europa.eu/irc/en/publication/wifi-positioning-and-big-data-monitor-flows-people-wide-scale (“[s]martphones, tablets and many other devices use wireless connectivity. Whenever, one of these tools is active, the device broadcasts probe requests to identify known networks. For each device, the probe request contains a unique identifier: the Media Access Control (MAC) address. A MAC address is a 12- characters hexadecimal identifier: the first 6 digits identify the manufacturer, while the remaining digits identify the device. This
online. Such footprints can be used to determine migratory patterns. For example, researchers have successfully traced migratory patterns in the Mediterranean region by comparing online data aggregated by Google Trends with official data provided by governments and the United Nations High Commissioner for Refugees (UNHCR).

Big data, and in particular social media data, has been effectively used for risk assessment and disaster management, healthcare and economic predictions. Analogously, big data analytics could prove useful in the field of international migration. Insofar as the rules on data protection and privacy are respected, big data and in particular big data analytics, could be a useful complement to traditional statistical tools. Big data analytics are the ‘techniques used to analyze and acquire intelligence from big data’, including extracting meaningful information from text, audio, video, and data from social media channels. In addition, predictive analytics techniques, which ‘seek to uncover patterns and capture relationships in data’ can be useful in capturing trends in migration identifier is visible to a network whenever the user is in its range; so, the MAC address can potentially be used to collect information on the activities of users, tracking the movements of the device’.

Google Trends is a publicly available online tool provided by Google in which search terms are showed in relation to their total search-volume across different regions of the world and different languages used (see https://trends.google.co.uk/trends/).


Huiji Gao et al., Harnessing the Crowdsourcing Power of Social Media for Disaster Relief, 26 IEEE INTELLIGENT SYSTEMS 10-14 (2011) (about the advantages and disadvantages of using social media for disaster relief); Xiangyang Guan & Cynthia Chen, Using social media data to understand and assess Disasters, 74 NAT. HAZARDS 837 (2014) (about the uses of social media and notably Twitter activities for rapid damage assessment); Jonathan Cinnamon et al., Evidence and future potential of mobile phone data for disease disaster management, 75 GEOFORUM 253 (2016) (for a critical analysis of uses of mobile phone data derived from call detail records and two-way short message service platforms for managing and responding to humanitarian disasters); Michael Ettredge et al., Using Web-based Search Data to Predict Macroeconomic Statistics, 48 Communications of the ACM, 87 (2005) available at http://dl.acm.org/citation.cfm?id=1096010 (suggesting that online web searches data can be useful for forecasting economic statistics); Philip Polgreen et al., Using Internet Searches for Influenza Surveillance, 47 CLIN. INFECL. DIS., 1443 (2008) and Jeremy Ginsberg et al., Detecting Influenza Epidemics Using Search Engine Query Data 457 NATURE, 1012 (2009) (on how online web search data could be useful for predicting the incidence of diseases such as influenza); Hyunyoung Choi & Hal Varian, Predicting the Present with Google Trends, 88 ECON. RES. 2 (2012) (explaining that Google Trends data can help in predicting the present).

See the European Commission Knowledge Centre on Migration and Demography’s Dynamic Data Hub, an interactive mapping tool that gives access to single datasets and provides visualisation of migration and demography data and trends: https://bluehub.jrc.ec.europa.eu/migration/app/index.html. See also Huub Dijstelbloem, Migration tracking is a mess, 543 NATURE 32 (2017) (arguing that technologies to monitor mobility are in reality political tools).

See infra Section IV, B.

See notably Rango, supra note 17; Piet J.H. Daas et al., Big Data as a Source for Official Statistics, 31 J. OFF. STAT. 249, 259 (2015) (affirming that “the official statistics community can greatly benefit from the possibilities offered by Big Data”).

Gandomi & Haider, supra note 6, at 140.
flows. For instance, data scientists could use data generated by individuals during natural disaster or conflict (e.g. Facebook check-in function, videos on online channels such as YouTube, photographs posted publicly via online platforms such Instagram or Pinterest, online searches for specific terms on Google) to predict migratory flows as the conflict or a natural disaster unfolds.

If correctly used, big data technology could contribute to achieving fairer and better-planned reception and integration strategies in the context of large movements of migrants and asylum-seekers. For example, decision-makers could anticipate the nature and density of upcoming migratory inflows by using tools based on a combination of big data and traditional statistical data analysis. Similarly, big data and traditional statistics can be used to map the diversity of migrant communities in cities. This would allow decision-makers to foresee which areas or neighbourhoods could attract specific migrant flows and would necessitate additional infrastructure such as housing, schools, or health care provision. However, all of these uses of big data relate to the management of migratory flows. Accordingly, the next section explores the extent to which big data could be used as a tool for the actual protection of vulnerable migrants.

37 Id. at 143 (also explaining that predictive analytics techniques are subdivided into two groups. Some techniques, such as moving averages, attempt to discover the historical patterns in the outcome variable(s) and extrapolate them to the future. Others, such as linear regression, aim to capture the interdependencies between outcome variable(s) and explanatory variables, and exploit them to make predictions.).
38 Junaid Qadir et al., Crisis analytics: big data-driven crisis response, 12 INT. J. HUMANITARIAN ACTION 1, 2 (2016).
39 See Yann Algan et al., Introduction: Perspectives on Cultural Integration of Immigrants, in YANN ALGAN ET AL. (eds.), CULTURAL INTEGRATION OF IMMIGRANTS IN EUROPE, 1, 4-7 (2012) (for an overview of the different integration theories in social sciences); LUIGI SOLIVETTI, IMMIGRATION, SOCIAL INTEGRATION AND CRIME. A CROSS-NATIONAL APPROACH, 132 (2010) (identifying three forms of integration: social integration, cultural assimilation, and political participation).
40 See for example Pew Research Centre, The Digital Footprint of Europe’s Refugees, supra note 31 (“Turkey-based searches for the word “Greece” in Arabic closely mirror 2015 and 2016 fluctuations in the number of refugees crossing the Aegean Sea to Greece”).
42 European Commission, Joint Research Centre, supra note 41.
III. BIG DATA AS A VALUABLE TOOL FOR THE PROTECTION OF VULNERABLE MIGRANTS

New technologies based on big data could also play an important role as a tool for the protection of vulnerable migrants, and potentially affect the way in which States effectively protect their rights within their jurisdiction. This section examines the uses of these new technologies against the existing legal framework on State obligations under IHRL. Firstly, it assesses the matters of jurisdiction and nature of State obligations. Secondly, it focuses on the prevention of migrants’ deaths at sea. Thirdly, it considers the protection against ill-treatment and human trafficking.

A. Jurisdiction and State Obligations

Under IHRL, State parties owe treaty obligations only to individuals who fall within their jurisdiction. State jurisdiction can be triggered when individuals find themselves in a State’s territory and when a State exercises ‘effective control’ over an area outside its national territory.


46 See Loizidou v. Turkey, App. No. 15318/89, ¶ 62 (Eur. Ct. H.R., Mar. 23, 1995). See also Delia Saldias de Lopez v. Uruguay, Comm No. 52/1979, ¶ 123, U.N. Doc. CCPR/C/OP/1 88 (1984) (“[a]rticle 2 (1) of the Covenant places an obligation upon a State party to respect and to ensure rights "to all individuals within its territory and subject to its jurisdiction", but it does not imply that the State party concerned cannot be held accountable for violations of rights under the Covenant which its agents commit upon the territory of another State, whether with the acquiescence of the Government of that State or in opposition to it’’); Human Rights Committee, General Comment No 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, ¶ 10, CCPR/C/21/Rev.1/Add. 1326 (May 2004) (“a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party”); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136 (Jul. 9) ¶111 (“the
Additionally, States have jurisdiction over individuals who are within their State agents’ authority and control.47 The hypothesis under examination relates to the use of big data for the identification and assistance of individuals at risk of death at sea, ill-treatment or human trafficking. Consequently, the present analysis concerns scenarios in which migrants have either entered a State’s territory (including its territorial waters) or are in an area that is effectively controlled by that State. However, it is worth noting that States may incur responsibility if there is evidence of aid and assistance in the commission of a wrongful act by a third State.48 In addition to IHRL, the law of the sea sets forth certain rules that bear on the protection of individuals on the high seas.49

For instance, there is a general duty to render assistance to any person found at sea in danger of


48 For example, this could be the case in the context of maritime operations undertaken by Libyan forces which received financial aid and training from the EU and its member States if an internationally wrongful act was committed (e.g. ill-treatment of migrants), and if there was enough evidence that EU member States had the knowledge of the circumstances of the internationally wrongful act and if the act would be internationally wrongful if committed by one of the EU member States as per Article 16 of the ILC, Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN A/56/10 (2001). See United Nations Human Rights Office of the High Commissioner (OHCHR), UN human rights chief: Suffering of migrants in Libya outrage to conscience of humanity (Nov. 2017) available at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22393&LangID=E (affirming that “[w]e cannot be a silent witness to modern day slavery, rape and other sexual violence, and unlawful killings in the name of managing migration and preventing desperate and traumatized people from reaching Europe’s shores”); Thomas Gammeltoft-Hansen & James C. Hathaway, Non-Refoulement in a World of Cooperative Deterrence, 53 COLUM. J. TRANSNAT'L L. 235 (for a comprehensive analysis of States shared responsibility and liability for aiding or assisting and its relationship to international refugee law).

being lost and to rescue people in distress. These rules fall outside of the realm of international human rights regimes and are therefore excluded from the present analysis.

With respect to obligations within IHRL, States agree to respect, protect, and fulfil the legal rights set forth by the treaties that they ratify. The obligation to respect implies that the State must not deprive individuals from their rights. The obligation to protect entails that States should protect individuals against human rights abuses, even if those originate in actions or omissions by private persons, insofar as the State can be seen as responsible. The obligation to fulfil requires States to take positive steps to facilitate the enjoyment of an individual’s human rights. States must respect, protect and fulfil human rights with respect to all individuals within their jurisdiction, including foreigners. Additionally, the European Court of Human Rights (ECtHR) and the Inter-American Court of Human Rights (IACtHR) distinguished between negative and positive obligations which in many aspects correspond to the obligations to respect, protect and fulfil.

---

50 Article 98 (1) (a) and (b) of the UNCLOS.


53 See Künnemann, supra note 52, at 328 (“The obligation to respect obliges the State to avoid depriving a human being of this existential status in situations where that status has been attained’’); Committee on Economic, Social and Cultural Rights, General Comment No 12: The Right to Adequate Food, supra note 52, ¶ 15 (“[t]he obligation to respect existing access to adequate food requires States parties not to take any measures that result in preventing such access’’).


55 See Künnemann, supra note 52, at 328 (arguing that the obligation to fulfil should not be understood as an obligation to provide as the latter has a subsidiary nature and prevents the State from incorporating the whole life of society).

56 See notably Human Rights Committee, General Comment No 15: The Position of Aliens under the Covenant, ¶ 7, U.N. Doc. HRI/GEN/1/Rev.6 140 (Sept. 1986) (explicitly recognising that “aliens thus have an inherent right to life, protected by law, and may not be arbitrarily deprived of life. They must not be subjected to torture or to cruel, inhuman or degrading treatment or punishment; nor may they be held in slavery or servitude’’).

57 Insofar as negative obligations relate to the obligation to respect human rights and positive obligations relate to the obligations to protect and fulfil human rights, see Alastair Mowbray, The Development of Positive
Negative obligations entail that States should refrain from interfering in the exercise of rights, while positive obligations mean that States should adopt all measures necessary to safeguard the effective respect of rights. The Human Rights Committee (HRC) has also emphasised that the legal obligation to respect and to ensure the rights recognized in the International Covenant on Civil and Political Rights (ICCPR) “is both negative and positive in nature”. Accordingly, with this taxonomy in mind, the following analysis focuses primarily on the positive obligations of States.

B. The Positive Obligation to Prevent Migrant Deaths at Sea

It is generally accepted that States are not only obliged to refrain from the intentional and unlawful taking of life, but must also to take appropriate steps to safeguard the lives of those within their jurisdiction. Therefore, States have a positive obligation to adopt measures to protect the lives of individuals, including against the criminal acts of a third party, and to investigate these situations effectively. This obligation should be considered as an obligation of conduct or means


See notably, Airey v. Ireland, App. No. 6289/73, ¶ 32 (Oct. 9, 1979); Marckx v. Belgium, App. No. 6833/74, ¶ 31 (June 13, 1979)


See for instance, Kayak v. Turkey, App. No. 60444/08, ¶ 59 (Eur. Ct. H.R., Jul. 10, 2012) (concerning the murder of a 15 year-old child who was stabbed in front of his school); Pueblo Bello Massacre v. Colombia, supra note 60, ¶ 120 (Jan. 31, 2006) (relating to extrajudicial executions by paramilitary groups); Human Rights Committee, General Comment No 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, supra note 46, ¶ 8 (about State obligations under the Covenant in general and not only relating to the right to life). For the conceptual framework
and not as an obligation of result, as States cannot be subjected to an impossible or disproportionate burden while attempting to prevent deaths. Those falling within the State’s jurisdiction are entitled to the protection in the same manner as nationals. In the context of the protection of migrants’ right to life and the prevention of deaths at sea, Professor Goodwin-Gill argues that States have a “positive due diligence obligation to save lives.” The instant question is whether this duty should be carried out, when possible, by the use of new technologies relying on big data analysis.

Typically, States have a certain margin of appreciation with regard to implementing positive obligations. However, the margin of appreciation and deference to domestic decisions is limited

of positive obligations and horizontal effect of international treaties on human rights, see Andrew Clapham, Human Rights in the Private Sphere (1996).

Constantin P. Economides, Content of the Obligation: Obligations of Means and Obligations of Result, in James Crawford et al. (eds.), The Law of International Responsibility, 371, 372 (2010) (“obligations of means impose on a State the obligation to do the best they can in furtherance of a specific goal, but without the guarantee that this goal will be reached. By contrast, obligations of result require a State to guarantee the achievement of the prescribed result”); Jean Combacau, Obligations de Résultat et Obligations de Comportement: Quelques Questions et Pas de Réponse, in Daniel Bardonnnet et al. (eds.), Le Droit International: Unité et Diversité. Mélanges Offerts à Paul Reuter, 181, 184-7 (1981) (for an overview of the origins of this typology of obligations in French civil law and its transposition into international law). See Osman v. United Kingdom, supra note 60, ¶ 116 (Eur. Ct. H.R., Oct. 28, 1998) (“not every claimed risk to life can entail for the authorities a Convention requirement to take operational measures to prevent that risk from materialising”).


See Article 1 of the ECHR providing that “[t]he High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention”; Article 1(1) ACHR providing that “[t]he States Parties to this Convention undertake to respect the rights and freedoms recognized herein and to ensure to all persons subject to their jurisdiction the free and full exercise of those rights and freedoms (…)”; Article 2(1) of the ICCPR providing that “[e]ach State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant”. See also Human Rights Committee, General Comment No 15: The position of aliens under the Covenant, supra note 56, ¶ 2 (affirming that “the general rule is that each one of the Covenant must be guaranteed without discrimination between citizens and aliens”).

Goodwin-Gill, supra note 23, at 25.

The margin of appreciation is understood as “tool to define relations between the domestic authorities and the Court” as per A and others v. UK, App No. 3455/05, ¶ 184 (Eur. Ct. H.R., Feb. 19, 2009). This doctrine was developed by the ECtHR and directly relates to the principle of subsidiarity. See Protocol No. 15 amending the Convention on the Protection of Human Rights and Fundamental Freedoms, CETS No 213 (June 24, 2013). See notably, Yuval Shany, Toward a General Margin of Appreciation Doctrine in International Law, 16 Eur. J. Int’l L. 907, 910 (2005) (explaining that the two principal elements at the basis of the doctrine are judicial deference and normative flexibility); George Letsas, Two Concepts of the Margin of Appreciation, 26 Oxf. J. LEG. STUD. 705, 706 (2006) (proposing a substantivist and a structural analysis of the margin of appreciation); Michael R. Hutchinson, The Margin of Appreciation Doctrine in the European Court Of Human Rights, 48 Int’l & Comp. L. Q. 638, 640 (1999) (explaining the width of the margin of appreciation in relation to existence of consensus, nature of rights and aims protected such as national security); Dominic McGoldrick, A Defence of the Margin of Appreciation and an Argument for its Application by the Human Rights Committee, 65 Int’l & Comp. L. Q. 21, 41 (2016) (discussing the non-use of the margin of appreciation doctrine by the
vis-à-vis absolute rights and the right to life. As observed by Professor Yuval Shany, international courts review the reasonableness of State measures vis-à-vis the object and purpose of the governing norm. Nevertheless, as indicated by the International Court of Justice (ICJ) “what is reasonable and equitable in any given case must depend on its particular circumstances.” In this regard, the circumstances of maritime migration can hardly be described other than alarming. Reportedly, the number of lives lost at sea in recent years is unprecedented. This is notably due to the shocking precariousness of vessels used for migrant smuggling.
Analysis of data generated by migrants and asylum-seekers (e.g. mobile applications recording geolocation, online searches, phone calls) can contribute to identifying their movement patterns.\textsuperscript{74} Moreover, data from other sources such as the Automatic Identification System (AIS)\textsuperscript{75} and the Broadcast Warning System\textsuperscript{76} can also be used for search and rescue of migrants in distress at sea, as demonstrated by an International Organisation for Migration (IOM) study in 2017.\textsuperscript{77} Data from all these sources could be useful for the identification of vulnerable groups of migrants at risk of dying in vessels unfit for sail at sea. Yet, should States be expected, and therefore required, to use such technologies to prevent migrant deaths at sea?

An analogy with disaster prevention may be useful in this respect. Pursuant to Article 9 of the International Law Commission (ILC)’s Draft Articles on the Protection of Persons in the Event of Disasters, States shall reduce the risk of disasters by taking appropriate measures including risk assessments for the prevention, mitigation and preparation for disasters.\textsuperscript{78} Similarly, the ECtHR identified an obligation to prevent and mitigate disasters within the scope of Article 2 of the ECHR.\textsuperscript{79} Acknowledging the ECtHR’s jurisprudence in this area, the Special Rapporteur Valencia-Ospina emphasized that “a State therefore incurs liability when it neglects its duty to take

\footnotesize

\textsuperscript{74} See \textit{supra} note 31.

\textsuperscript{75} An automated tracking system fitted in ships which can provide real time information to other ships and to coastal authorities. Regulation 19 (2.4) of the SOLAS (requesting that ships of more than 500 tonnes or operating internationally should be fitted with the automatic identification system [hereinafter AIS]). That would include vessels operating search and rescue missions at sea. See IOM, \textit{Fatal Journeys. Improving Data on Missing Migrants}, 28 (2017) available at http://publications.iom.int/system/files/pdf/fatal journeys_volume_3_part_1.pdf (explaining how AIS data can be captured and used).

\textsuperscript{76} Broadcast warnings are disseminated by the Worldwide Navigational Warning Service (WWNWS). This is a broadcast system based on radio and satellite technology and used for maritime safety. See National Geospatial Intelligence Agency, available at http://msi.nga.mil/NGAPortal/MSI.portal?_nfpb=true&_pageLabel=msi_wwnws (for general information about the WWNWS); IOM, \textit{Fatal Journeys}, supra note 75, at 29 (for an explanation of how the WWNWS data can be used in the context of international migration).

\textsuperscript{77} IOM, \textit{Fatal Journeys}, supra note 75, at 25-42 (demonstrating how these two data sources can be used for the purposes of studying rescue patterns in the Mediterranean).

\textsuperscript{78} Article 9 (1) and (2) of the ILC, Draft Articles on the Protection of Persons in the Event of Disasters, UN A/71/10 (2016).

\textsuperscript{79} See Budayeva and others v. Russia, App Nos. 15339/02, 21166/02, 20058/02, 11673/02 and 15343/02, ¶ 132 (Eur. Ct. H.R., Mar. 20, 2008) (about recurrent and deadly mudslides) (“[a]s regards the substantive aspect, in the particular context of dangerous activities the Court has found that special emphasis must be placed on regulations geared to the special features of the activity in question, particularly with regard to the level of the potential risk to human lives. (...) The relevant regulations must also provide for appropriate procedures, taking into account the technical aspects of the activity in question, for identifying shortcomings in the processes concerned and any errors committed by those responsible at different levels”); Önerüyildiz v. Turkey, App No. 48939/99, ¶ 89 (Eur. Ct. H.R., Nov. 30, 2004) (about a methane explosion in a slum near Istanbul and the consequent death of nine individuals) (“this positive obligation entails above all a primary duty on the State to put in place a legislative and administrative framework designed to provide effective deterrence against threats to the right to life”).
preventive measures when a natural hazard is clearly identifiable and effective means to mitigate the risk are available to it.”

Identification of natural disasters is nowadays for a large part dependent on satellite imagery and computerised technologies. Furthermore, Article 3 of the Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations expressly encourages States to deploy satellite telecommunication equipment to predict, monitor and provide information concerning natural hazards, health hazards and disasters. Arguably, when State authorities have the capabilities to use satellite imagery and computerised new technologies to foresee a natural disaster such as an earthquake or a tsunami, it is reasonable to believe that they must do so in order to prepare for it as efficiently as possible and to prevent losses of lives and damage to individuals and property within their jurisdiction.

The use of these technologies can be a useful means for the prevention of damage and for the delivery of technical assistance during such disasters. Accordingly, it is possible to argue that a State would have a duty to use such technologies if this was within its technical capabilities and if this was the most effective way to prepare for, prevent, and mitigate natural disasters.

A similar argument could be made in relation to the use of new technologies based on big data as means of preventing migrant deaths at sea. Arguably, States have a duty to use new technological means to prevent migrants’ deaths at sea if and when:

80 Sixth report of the Special Rapporteur, Mr. Eduardo Valencia-Ospina (65th session of the ILC (2013)) ¶ 53.
81 See notably, Charter on Cooperation to Achieve the Coordinated Use of Space Facilities in the Event of Natural or Technological Disasters, Article 2, Rev.3 (25/4/2000) 2 (affirming that one of its objectives is to “supply during periods of crisis, to States or communities whose population, activities or property are exposed to an imminent risk, or are already victims, of natural or technological disasters, data providing a basis for critical information for the anticipation and management of potential crises”); United Nations Platform for Space-based Information for Disaster Management and Emergency Response (UN-SPIDER) available at http://www.un-spi.jpger.org/space-application/satellite-technology (explaining the types of services that satellites can provide for disaster risk management and emergency response); Thomas W. Gillespie et al., Assessment and Prediction of Natural Hazards from Satellite Imagery, 31 PROG. PHYS. GEOGR. 459, 459 (2007) (explaining that “since 2000, there have been a number of spaceborne satellites that have changed the way we assess and predict natural hazards”)
83 Sixth report of the Special Rapporteur, Mr. Eduardo Valencia-Ospina, supra note 80, ¶ 53 (“a State’s duty is triggered when a disaster becomes foreseeable, which mirrors the foreseeability requirement within the principle of due diligence”).
84 See Eighth report of the Special Rapporteur, Mr. Eduardo Valencia-Ospina (68th session of the ILC (2016)) ¶ 168 (recalling that the European Union recommended that a specific mention should be made in the commentary of the ILC’s Draft Articles on the Protection of Persons in the Event of Disasters according to which satellite imagery can be used as an important means of delivering technical assistance during emergency response).
the use of such technologies does not amount to an impossible or disproportionate burden on them; and (3) it is reasonable to believe that the use of these means is the most effective way to fulfil the obligation.

Firstly, it is submitted that States which already use such technologies may have the technical capability to transform them into tools for the much-needed protection of migrants’ lives at sea. This is illustrated, for instance, by the fact that big data has been increasingly used by States for surveillance purposes, as in the case of bulk surveillance techniques used by many States, from Europe to the Americas. In this regard, developing States may not be capable of employing such technologies until the digital divide between developing and developed world has been bridged, or until a stronger international cooperation for technical matters has been established.

Secondly, it is accepted that States are not expected to bear an impossible or disproportionate burden while complying with their positive obligations. In this regard, the ECHR emphasizes that State authorities will be deemed to have violated a positive obligation only if they “knew or

---


86 See PIPPA NORRIS, *DIGITAL DIVIDE: CIVIC ENGAGEMENT, INFORMATION POVERTY AND THE INTERNET WORLDWIDE*, 4-9 (2001) (on the global divide amongst countries). See also Article 26 of the ACHR (“[t]he States Parties undertake to adopt measures, both internally and through international cooperation, especially those of an economic and technical nature, with a view to achieving progressively, by legislation or other appropriate means, the full realization of the rights implicit in the economic, social, educational, scientific, and cultural standards set forth in the Charter of the Organization of American States as amended by the Protocol of Buenos Aires”). See mutatis mutandis Rio Declaration on Environment and Development, UN Doc. A/CONF.151/26 (vol. I); 31 ILM 874 (1992), Principle 7 (“In view of the different contributions to global environmental degradation, States have common but differentiated responsibilities”); Virgine Barral, Sustainable Development in International Law: Nature and Operation of an Evolutive Legal Norm, 23 Eur. J. Int’l L. 377, 381-2 (2012) (for an analysis of the principle of common but differentiated responsibilities in the field of international environmental protection).

ought to have known at the time of the existence of a real and immediate risk to the life of an identified individual or individuals … and [if] they failed to take measures within the scope of their powers which, judged reasonably, might have been expected to avoid that risk’. 88 The IACtHR has adopted similar criteria. 89 However, UN agencies, NGOs, charities and private service providers operating in the field regularly assess the situation on the ground and inform State authorities about the existence of real risks to migrants’ lives. 90 For instance, the UNHCR provided evidence that the risk to migrants’ lives is heightened on certain maritime routes, such as the Central Mediterranean route from North Africa to Italy. 91 It is submitted that State authorities can acquire sufficient knowledge about the existence of a real risk to migrants’ lives in specific migratory routes where individuals are smuggled in vessels unfit for sail. Once they have the knowledge of the risk, State authorities are required to act, adopting measures to prevent migrant deaths at sea. New technologies based on big data analysis (e.g. analysis of mobile applications recording geolocation, online searches, phone calls, AIS data and Broadcast Warning System data) should, if available, figure amongst these measures. 92

88 Osman v. the United Kingdom, supra note 60, ¶ 116.
91 The UNHCR provides information about the situation in the Mediterranean via its data portal available at https://data2.unhcr.org/en/situations/mediterranean. See also UNHCR, Dead and missing at sea (Nov. 16, 2017) available at https://data2.unhcr.org/en/documents/download/60779; UNHCR, Desperate Journeys. Refugees and Migrants Entering and Crossing Europe via the Mediterranean and Western Balkan Routes, 6-7 (Feb., 2017) available at http://www.unhcr.org/58b449f54 (“[t]he number of deaths of refugees and migrants in the Mediterranean as they attempted to reach Europe in 2016 is the highest on record, primarily due to 4,578 deaths in the central Mediterranean, compared to 2,913 in the whole of 2015”).
92 See supra notes 74-7 and accompanying text.
Thirdly, the principle of effectiveness entails that the parties to a treaty have intended it “to have a certain effect, and not to be meaningless.”93 As Professor Hugh Thirlway has noted, “an interpretation which would make the text ineffective to achieve the object in view is, again, prima facie suspect.”94 The ECtHR and the IACtHR have interpreted the right to life as encompassing a positive obligation for a State to “take appropriate steps to safeguard the lives of those within its jurisdiction”95 in order for that right to be effective.96 If the use of new technologies based on big data analysis becomes a feasible way to identify individuals whose lives are at risk at sea, as this is the case with the use of satellite imagery for the prevention and mitigation of natural disasters, not using such technologies would deplete the obligation of its effect.97 In other words, failure to use feasible technologies would amount to unnecessary loss of lives, emptying the obligation under the right to life of effectiveness.

The following example could be used for illustrative purposes. Arguably, Italy and the European Border and Coast Guard Agency (Frontex),98 had access to sufficiently clear information provided by the UNHCR that a precise maritime route (e.g. the Central Mediterranean route) had

---

95 Osman v. United Kingdom, supra note 60, ¶ 115.
96 Id, ¶ 116; Pueblo Bello Massacre v. Colombia, supra note 60, ¶ 111. See also Human Rights Committee, General Comment No 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, supra note 46, ¶ 6 (on the “continuous and effective protection of Covenant rights”).
97 See supra notes 81-4 and accompanying text (on the use of satellite imagery). Comparatively, see on the concept of feasibility as applied in International Humanitarian Law: Article 57 (2) a) ii of the Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 (“those who plan or decide upon an attack shall: … take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects”); Int’l Comm. of the Red Cross (ICRC), Customary International Humanitarian Law 56, Rule 17 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005) (“[e]ach party to the conflict must take all feasible precautions in the choice of means and methods of warfare with a view to avoiding, and in any event to minimising, incidental loss of civilian life, injury to civilians and damage to civilian objects”); Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 479 commentary under Rule 115 (2017) (“[f]easible has been widely interpreted as that which is ‘practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations’”); Michael N. Schmitt & John J. Merriam, The Tyranny of Context: Israeli Targeting Practices in Legal Perspective, 37 U. Pa. J. Int’l L. 53, 133 (“[i]n some cases, feasibility may be an issue of asset availability” – which could relate for example to advanced technologies).
been consistently deadly in the past months. However, extensive search and rescue operations had been ruled out, as they were controversially deemed to increase the number of migrant smuggling attempts. Consequently, this may have led in practice, to a larger number of migrant deaths in this maritime route. Yet, big data analysis could have been useful to predict and map migratory paths in near real-time. Frontex already performs risk analysis and has a dedicated data science team to carry out big data analytics. Italy, may have already the capability to conduct big data analysis, notably as its authorities seem to use such technology for mass surveillance operations. Moreover, Frontex can provide technical assistance to EU Member States and could in theory assist Italian authorities with data science support. Therefore, Italy could potentially use big data analysis to inform targeted search and rescue operations in this specific maritime route if they had sufficient knowledge about the existence of real risks to migrants’ lives entering their jurisdiction. Such operations could contribute to prevent unnecessary migrant deaths. If such targeted operations were considered as more effective than non-targeted operations, recourse to new technologies based on big data would be required.

---

99 See supra note 91.
100 The Italian operation Mare Nostrum was discontinued in October 2014 and was followed by the Frontex-led operation Triton. In parallel, the so called ‘EU NavFor/Sophia’ operations were launched in June 2015 with a specific anti-smuggling mission. See European Political Strategy Centre, supra note 72, at 3 (for a detailed overview of the different operations in the Central Mediterranean route); MORENO-LAX, ACCESSING ASYLUM IN EUROPE, supra note 20, at 195 (“in October 2014 Mare Nostrum was terminated on account of excessive costs—and perhaps due to a perceived ‘call effect’ attracting continuous arrivals. Frontex operation Triton took over, but with a much less ambitious remit”).
101 See UNHCR, Dead and missing at sea, supra note 91 (for the number of deaths in the central Mediterranean route since 2015).
102 See Pew Research Centre, The Digital Footprint of Europe’s Refugees, supra note 31, fig. 1; IOM, Fatal Journeys, supra note 75, at 29; Facebook Data Science, Coordinated Migration available at https://www.facebook.com/notes/facebook-data-science/coordinated-migration/10151930946453859?notif_t=notify_me (mapping migration by contrasting Facebook users' data about their declared “hometown” and their declared “current city”).
103 See supra note 24. See also http://frontex.europa.eu/intelligence/analytics/ (explaining that “[t]he Analytics Sectors was established to expand the Risk Analysis Unit’s data and geo analysis capabilities and to sustain the high quality level of knowledge delivered and managed by it. The sector consists of two teams supporting the Strategic and Operational Sectors in their ad-hoc and bespoke exploitation of data and intelligence (Data Team) and through the provision and development of geospatial services (GIS Team”)”).
104 See Disegno di legge S. 2886, Disposizioni per l’adempimento degli obblighi derivanti dall’appartenenza dell’Italia all’Unione europea - Legge europea 2017, A.C. 4505-B, art. 24 (allowing the use of mass surveillance in the fight of terrorism).
105 Article 8 (1) (f) of the Regulation (EU) 2016/1624, supra note 20 (“provide technical and operational assistance to Member States and third countries in accordance with Regulation (EU) No 656/2014 and international law, in support of search and rescue operations for persons in distress at sea which may arise during border surveillance operations at sea”).
Accordingly, if new technologies based on big data were the most effective tools for the prevention of migrants’ deaths, and their use did not impose any impossible or disproportionate burden on States that have the technical capabilities to operate them, it is submitted that, due to the particular circumstances of maritime migration, it is reasonable to expect those States to use such technologies in order to fulfil their positive obligation. The next section examines whether the same approach could also be applied in relation to the protection of migrants at risk of ill-treatment and human trafficking.

C. Protection of Migrants at Risk of Ill-Treatment and Human Trafficking

Migrants and asylum-seekers in large migratory movements are particularly vulnerable to abuse, human trafficking and exploitation.\(^{106}\) This is especially concerning in relation to migrant and asylum-seeking children.\(^{107}\) According to the UNICEF and the IOM, 77% of migrant and asylum-seeking children travelling in the Mediterranean region have reported experiencing abuse, exploitation, and practices that may amount to ill-treatment and human trafficking.\(^{108}\)

Torture, inhuman and degrading treatment or punishment are forms of ill-treatment which human rights treaties prohibit and condemn.\(^{109}\) Defined criteria allow for the identification of

---


\(^{107}\) The term ‘children’ is defined in Article 1 of the Convention on the Rights of the Child, Nov. 20, 1989 1577 U.N.T.S. 3 (“For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier”).


\(^{109}\) See notably Articles 7 of the ICCPR, 3 of the ECHR, 5 of the ACHR, and also Article 2 of Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Dec. 10, 1984, 1465 U.N.T.S. 85 [hereinafter “CAT”].
situations falling within the scope of each of these types of ill-treatment. 110 The protection afforded by these instruments applies to all individuals within the jurisdiction of the State parties to the treaties, including foreigners. 111

Human trafficking is defined by Article 3 (a) of the Palermo Protocol and Article 4 (a) of the Anti-Trafficking Convention. 112 According to both identically worded provisions, trafficking in persons shall mean the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs.

It is generally accepted that States are required to adopt measures to ensure that individuals within their jurisdiction are not subjected to ill-treatment, even if such treatments are administered by private individuals. 113 Likewise, the ECtHR recognised that States have the positive obligation

---


111 See Human Rights Committee, General Comment No 15: The position of aliens under the Covenant, supra note 56, ¶ 7 (affirming that aliens “must not be subjected to torture or to cruel, inhuman or degrading treatment or punishment”); Chahal v. The United Kingdom, App No. 22414/93, ¶¶73-4 (Eur. Ct. H.R., Nov. 15, 1996) (on the applicability of Article 3 ECHR to aliens in expulsion cases); Rights and Guarantees of Children in the Context of Migration and/or in need of International Protection, Advisory Opinion OC-21/14, supra note 46, ¶ 225 (Aug. 19, 2014) (on the relationship between the prohibition of torture, inhuman and degrading treatment and the principle on non-refoulement).


to adopt operational measures to protect victims, or potential victims, of trafficking. The IACtHR has also imposed positive obligations on States with the view to ensure respect for Article 6 of the American Convention on Human Rights (ACHR). Amongst these obligations, the IACtHR emphasised the positive obligation to adopt preventive measures vis-à-vis defined groups of people at risk of falling into slavery and human trafficking.

The same analytical framework proposed above can be used to verify whether State positive measures to protect migrants against ill-treatment and human trafficking should also encompass the use of new technologies building on big data analysis. It is certainly not possible to generally infer that States have an all-encompassing duty to use new technological means to protect individuals from ill-treatment and human trafficking. However, States may have a duty to use new technological means in specific circumstances.

As discussed in the previous section, a growing number of States have mass surveillance programmes drawing upon big data already in place, demonstrating their capability to use such technological tools. Yet, State authorities enjoy some discretion as to the types of measures adopted within the scope of their powers to fulfil their obligations, notably when they are

---

114 Curiously, Article 4 of the ECHR does not expressly refer to human trafficking. However, using evolutive interpretation, the ECtHR considered that human trafficking, as defined by the Palermo Protocol and the Anti-Trafficking Convention, fell within the scope of Article 4 of the ECHR. See Rantsev v. Cyprus and Russia, App. No. 25965/04, ¶ 286 (Eur. Ct. H.R., Jan. 7, 2010); C.N. v. United Kingdom, App No. 4239/08, ¶ 67 (Eur. Ct. H.R., Nov. 13, 2012); M. and Others v. Italy and Bulgaria, App No. 40020/03, ¶ 151 (Eur. Ct. H.R., Jul. 31, 2012).

115 Fazenda Brasil Verde Workers v. Brasil, supra note 14, ¶¶ 319-20 (Oct. 20, 2016). Noteworthy, Article 6 of the ACHR, unlike Article 4 of the ECHR, explicitly refers to slave trade and traffic in women. Art 6 (1) of the ACHR (“[n]o one shall be subject to slavery or to involuntary servitude, which are prohibited in all their forms, as are the slave trade and traffic in women”); art 4 (1) of the ECHR (“[n]o one shall be held in slavery or servitude”).

116 Fazenda Brasil Verde Workers v. Brasil, supra note 14, ¶ 320 (also recognising that this obligation is reinforced by the imperative character of the peremptory norm of international law prohibiting slavery and the severity and intensity of the violation of rights); Rights and Guarantees of Children in the Context of Migration and/or in need of International Protection, Advisory Opinion OC-21/14, supra note 46, ¶ 92 (imposing the obligation upon States to adopt specific border control measures in order to prevent, detect, and prosecute any type of trafficking of persons).

117 Id. (for the three criteria proposed above — State capability, no impossible or disproportionate burden, and effectivity of the measure adopted).

118 See supra Section III, B.

119 Id. (for the three criteria proposed above — State capability, no impossible or disproportionate burden, and effectivity of the measure adopted).

119 See supra notes 85 and 104.

obligations of conduct or means.\textsuperscript{121} Moreover, State responsibility can be engaged only when the legal framework fails to adequately protect the individuals,\textsuperscript{122} or when the authorities have failed to take reasonable steps to prevent ill-treatment whereas they knew or ought to have known about the specific risks.\textsuperscript{123} Knowledge of the risk may be more difficult to establish in this context than that of migrants at sea, where States are regularly warned about the risks of death in specific migratory routes.\textsuperscript{124} By contrast, instances of human trafficking and ill-treatment of migrants are less well reported.\textsuperscript{125}

However, as protection is strongly intertwined with fighting criminality, States may have a strong interest in using new technologies. Arguably, big data analysis and in particular predictive analytics techniques could become a fundamental asset for the effective fight against criminality in relation to ill-treatment and human trafficking.\textsuperscript{126} Such technologies could be used to identify and map areas at risk where human trafficking and ill-treatment may be taking place within the State territory.\textsuperscript{127} For instance, human traffickers use mobile phones and the Internet for recruitment,
advertisement, and communication of their activities. The data that they generate could be used for the identification of trafficking networks in the physical world. Although such operations are not yet widespread, they are certainly not hypothetical either. For instance, big data science was used to successfully map human trafficking networks in India and to help fostering prevention tools in the civil society. If effectively used by States for fighting criminality, these new technologies could also be applied for the protection of individuals. Nonetheless, that would depend significantly on political will and, as discussed below, would not be without risks.

IV. LIMITS AND RISKS OF USING BIG DATA IN INTERNATIONAL MIGRATION

New technologies based on big data are increasingly present in many areas of societal interests. As discussed above, these technologies have the potential to contribute to better international migration management and enhance the protection of migrants at risk. However, unrestrained use of such technologies could in fact pose serious risks to the safety of migrants, as well as amount to unjustified interference with their right to privacy and data protection.

A. Migrant Safety and Protection

Big data analysis has the potential to provide accurate and detailed breakdown not only of human migration patterns, but also of one’s individual behaviours and potentially one’s identity. It is presently possible to determine with precision behaviour relating to virtually all

---

128 Hao Wang et al, Data integration from open internet sources to combat sex trafficking of minors, Proc. 13th Dig. Govt. Res. Conf. 246, 247 (2012) (“[a]s with licit activities, the use of the Internet in child sexual abuse is increasing with greater use of digital media”); Mark Latonero et al., Human Trafficking Online. The Role of Social Networking Sites and Online Classifieds, Report, USC Annenberg Center on Communication Leadership & Policy, 8 (2011) available at http://ssrn.com/abstract=2045851 (“[t]he rapid expansion of the Internet and online technologies is affecting numerous aspects of daily life around the globe, including facilitating domestic and international trafficking in persons”).

129 Konrad et al., supra note 127, at 738 (enumerating the technologies that can be used to analyse data from the Internet and potentially assist victim protection).


131 See supra note 32.

132 See supra Sections II and III.


134 See KITCHIN, THE DATA REVOLUTION, supra note 3, at 100-12 (for a detailed explanation of data analytics); World Bank, Principles on Identification for Sustainable Development: Toward the Digital Age (2017) available at
areas of one’s life. Examples include behaviour ranging from personal care to eating habits and from shopping preferences to health concerns. Data mining techniques can extract information such as individual names, locations, dates, search terms, or product terminology from large datasets, and link them together in order to determine, for example, how a person’s name relates to a location or to an opinion expressed online about a precise item. These techniques are already used by businesses to promote their products and target specific consumers, and may also conceivably be used in the domain of international migration.

Besides the obvious issues of respect for privacy and compliance with data protection legislation, there is a risk that States might use these technologies to further criminalise migration and deny protection to vulnerable groups of migrants. In the context of large movements of migrants and asylum-seekers, it is important to ensure that these new technologies based on big data do not aggravate the risks of refoulement and extreme borders securitisation. For


136 See GORDON S. LINOFF & MICHAEL J. A. BERRY, DATA MINING TECHNIQUES: FOR MARKETING, SALES, AND CUSTOMER RELATIONSHIP MANAGEMENT (2011) (for a general overview of the uses of data mining in business-related matters); Tao Zang et al., Mining target users for mobile advertising based on telecom big data, 16 ISCT 296, 296 (2016) (on telecom big data mining and mobile advertising targeting customers more accurately).

137 See infra Section IV, B.

138 As per Article 33 (1) of the Convention Relating to the Status of Refugees, U.N.T.S. 189, 137 (Jul. 28, 1951) [hereinafter “Refugee Convention”] (“[n]o 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”). See JAMES C. HATHAWAY & MICHELLE FOSTER, THE LAW OF REFUGEE STATUS 21 (2nd edn, 2014) (“Refugee status secures access to protection against refoulement, the right not to be sent back to the country of origin for the duration of the risk”); JANE MCDAM, COMPLEMENTARY PROTECTION IN INTERNATIONAL REFUGEE LAW 136 (2006) (affirming that “the scope of non-refoulement is recognized under international law as extending beyond Article 33 of the Refugee Convention to encompass torture”).

139 See Christina Boswell, Migration control in Europe After 9/11: Explaining the absence of securitization, 45 JCMS 589 (2007) (for a definition of securitization); PHILIPPE BOURBEAU (ed), HANDBOOK ON MIGRATION AND SECURITY (2017) (for a general overview of the issue of securitisation of migration); Benjamin J. Muller, Risking it all at the Biometric Border: Mobility, Limits, and the Persistence of Securitisation, 16 GEOPOLITICS, 91, 97 (2011) (on the application of biometrics to the contemporary border security and the uses of risk management in the field of migration and mobility); Celia Rooney, Exploiting a Tragedy: The Securitization of EU Borders in the Wake of Lampedusa (2013) available at http://bordercriminologies.law.ox.ac.uk/exploiting-a-tragedy (for a short overview of the already securitisation of migration before the Summer 2015 and the subsequent migration crisis).
example, big data analysis could provide States with the means to identify and locate migrants heading towards their territory.\textsuperscript{141} This information could be used to streamline pushbacks of individuals without a thorough examination of their claims. Hence, big data could be used as an instrument of exclusion of undesirable migrants at increasingly closed and secured borders.\textsuperscript{142} In addition, relying primarily on big data to profile migrants and distinguish them from terrorists, criminals and human traffickers could lead to automated decision-making, which might intensify the threat of discrimination.\textsuperscript{143} For example, research demonstrates that this is already the case with facial recognition software in relation to racial and ethnic minorities.\textsuperscript{144}

Furthermore, information falling into the wrong hands, like State authorities engaged in the persecution of asylum-seekers or non-State actors such as criminal and terrorist groups, can have drastic consequences. If not appropriately used, big data could harm more than help the protection of migrants’ human rights. For example, human traffickers and other criminal groups theoretically could use big data analytics or hack into official databases to estimate where migrants tend to concentrate, identify the routes they use, and target vulnerable migrants more efficiently.\textsuperscript{145} The information also could be used, for instance, to incite violence against specific migrant groups by communicating their geolocation to extremist groups.

\textsuperscript{141} See supra notes 31 and 75-7.


\textsuperscript{143} See CATHY O’NEIL, \textit{Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy} (2016) (calling for a more responsible use of algorithms and for more regulation of big data usages); Brent Daniel Mittelstadt et al., \textit{The ethics of algorithms: Mapping the debate}, Big DATA & SOCIETY 3, 8 (“[p]rofiling algorithms identify correlations and make predictions about behaviour at a group-level … Profiling can inadvertently create an evidence base that leads to discrimination”);

\textsuperscript{144} See Clare Garvie et al., \textit{The Perpetual Line-Up. Unregulated Police Face Recognition in America}, Center on Privacy & Technology at Georgetown Law (October 18, 2016) available at https://www.perpetuallineup.org/ (about the use of face recognition technology by the police in the United States and its implications for the protection of civil liberties and the rights of racial and ethnic minorities); Joy Buolamwini, \textit{InCoding—In The Beginning}, MIT Media Lab (May 16, 2016) available at https://medium.com/mit-media-lab/incoding-in-the-beginning-4c2a5c51a45d (explaining the existence of embedded bias in coding);

\textsuperscript{145} Konrad et al., supra note 127, at 737 (demonstrating that mapping of victims and traffickers networks via analytics is possible).
Consequently, it is important to create systems that can harness data and metadata\textsuperscript{146} in large quantities but that are also consistent with human rights protection.\textsuperscript{147} Public-private initiatives have been placing a greater emphasis on user’s data ownership, notably when it comes to big social data.\textsuperscript{148} This is certainly an interesting development where more research is needed, notably insofar as privacy rights and data protection are concerned.

\subsection*{B. Migrant Privacy and Data Protection}

Telecommunications and personal data in electronic format are encompassed in the right to respect for one’s private life and correspondence.\textsuperscript{149} State action in this regard should not result in

\begin{footnotesize}
\textsuperscript{146} Data, OXFORD ENGLISH DICTIONARY (2017) (‘[t]he quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media’); Metadata, OXFORD ENGLISH DICTIONARY (2017) (‘[a] set of data that describes and gives information about other data’). See also Jenn Riley, Understanding Metadata. What is Metadata, and What is it for?, National Information Standards Organization (2017) available at http://www.niso.org/apps/group_public/download.php/17446/Understanding%20Metadata.pdf.

\textsuperscript{147} See Organization for the Advancement of Structured Information Standards (OASIS), Classification of Everyday Living (COEL) TC (2017) available at https://coelition.org/business/resources/coel-standard/ (supporting collection and processing of behavioural data in a way that personal data is pseudonymised at the source).

\textsuperscript{148} For instance, the ID2020 initiative aiming at making digital identities available for all individuals who do not have an official proof of identity by 2020, relies on public-private partnerships including start-ups, technology companies and United Nations agencies such as the UNHCR (see http://id2020.org/).

\textsuperscript{149} Articles 12 of the UDHR, 8 of the ECHR, 17 of the ICCPR, 11 of the ACHR. In the European Union context, see Article 7 (Respect for private and family life) and Article 8 (Protection of personal data) of the Charter of Fundamental Rights of the European Union (CFREU), OJ C 326 391 (Oct. 26, 2012). See also UNGA Resolution 68/167, The Right to Privacy in the Digital Age, supra note 85, ¶ 3 (affirming that “the same rights that people have offline must also be protected online, including the right to privacy”); Klass v. Germany, App No. 5029/71, ¶ 41 (Eur. Ct. H.R., Sept. 6, 1978) (affirming that telephone conversations fall within the realm of Article 8 of the ECHR under the notions of private life and correspondence); P.G. and J.H. v. United Kingdom, App No. 44787/98, ¶57(Eur. Ct. H.R., Sept. 25, 2001) (using the definition of personal data as “any information relating to an identified or identifiable individual” as per Article 2 of the Council of Europe’s Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, ETS No.108); Liberty and others v the United Kingdom, App No. 58243/00, ¶ 56 (Eur. Ct. H.R., Jul. 1, 2008) (affirming that “telephone, facsimile and e-mail communications are covered by the notions of “private life” and “correspondence” within the meaning of Article 8”); Uzun v. Germany, App No. 35623/05, ¶ 52 (Eur. Ct. H.R., Sept. 2, 2010) (relating to GPS surveillance and use of the data obtained thereby); Bărbulescu v. Romania, App No. 61496/08, ¶ 74 (Eur. Ct. H.R., Sept. 3, 2017) (affirming that internet instant messaging services “is just one of the forms of communication enabling individuals to lead a private social life”); Tristán Donoso v. Panamá, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H. R. (ser. C) No. 193, ¶ 55 (Jan. 27, 2009)(relating to surveillance of telephone communications); Escher et al. v Brazil, supra note 85, ¶ 114-5 (Jul. 6, 2009) (relating to telephone communications and use of new technological tools). See also MICHAEL N. SCHMITT, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, Rule 35 (2017) (“[i]ndividuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy”).
a disproportionate restriction upon these rights. In principle, this general rule should apply to all individuals, including foreigners who fall within the jurisdiction of a State party to a human rights treaty providing for the protection of these rights. Accordingly, migrants’ telecommunications and personal data should receive the same level of protection as the one offered to nationals. Nevertheless, domestic legal regimes such as those in the United States and Canada treat foreigners located outside of their territory differently as data protection and privacy rights are concerned. Concerns about the lack of protection of foreign individuals have intensified since the US National Security Agency (NSA) affair in 2013. The ready availability of large amounts of data has indeed contributed to expanding the options for mass surveillance of nationals and foreigners alike.

---

150 See for instance, Uzun v. Germany, supra note 149, ¶ 78 (affirming that “the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued”); Bârbaulescu v. Romania, supra note 149, ¶ 121 (affirming that despite the rapid developments in the area of electronic communications, “proportionality and procedural guarantees against arbitrariness are essential”); Escher et al. v. Brazil, supra note 85, ¶ 116 (affirming that “the right to privacy is not an absolute right and can be restricted by the States, provided interference is not abusive or arbitrary; to this end, it must be established by law, pursue a legitimate purpose and be necessary in a democratic society”); United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, Report of the Office of the United Nations High Commissioner for Human Rights, ¶ 23, A/HRC/27/37 (Jun. 30, 2014) (affirming that “any limitation to privacy rights reflected in article 17 must be provided for by law, (…) must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available (…) must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination”).

151 Articles 12 of the UDHR, 17 of the ICCPR, 8 of the ECHR and 11 of the ACHR employ the terms “no one” and “everyone” to define the subjects of protection in relation to privacy, home and correspondence. See also, Article 5(1) b of the Declaration on the Human Rights of Individuals who are not Nationals of the Country in which They Live, G.A. res. 40/144, annex, 40 U.N. GAOR Supp. (No. 53) at 252, U.N. Doc. A/40/53 (1985) (affirming that aliens shall enjoy the protection against arbitrary and unlawful interference within their privacy rights).

152 United States Foreign Intelligence Surveillance Act, §1881(a), 50 U.S.C. §36 (“[n]otwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (j)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information”); Canada National Defence Act, S. 273.64 (2) (a), S.C. 1985, c N-5 (Can.) (“[a]ctivities carried out under paragraphs (1)(a) and (b); (a) shall not be directed at Canadians or any person in Canada”).

153 Human Rights Committee, Concluding observations on the fourth periodic report of the United States of America, ¶ 22 (a) CCPR /C/USA/CO/4 (Apr. 23, 2014) (affirming that the United States should adopt “measures to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance”). See also RUSSELL A. MILLER (ed.), PRIVACY AND POWER. A TRANSATLANTIC DIALOGUE IN THE SHADOW OF THE NSA- AFFAIR (2017) (for an insightful discussion of the NSA affair); Davor Janice, The Role of the European Parliament and the US Congress in Shaping Transatlantic Relations: TTIP, NSA Surveillance, and CIA Renditions, 54 J. C. M. S. 896, 903 (2016) (for a discussion about the role of EU institutions in the aftermath of the revelations in the NSA affair).

154 See notably Bos-Ollermann, supra note 85, at 140 (discussing the ‘bulk collection’ of untargeted data in mass surveillance techniques); Lyon, supra note 85, at 5 (affirming that big data “intensify surveillance by expanding interconnected datasets and analytical tools”).
Surveillance based on new technologies and big data can place State authorities on the top of a digital Panopticon. Individuals seem to know that they might be observed, but might not know how exactly and by whom. As in Foucault’s model of Panopticon, they are those “[who are] seen, but [do] not see; [who are] the object of information, never a subject in communication.” In the digital era, our smallest deeds and gestures can become highly visible and therefore subjected to surveillance. The safeguard of public interests plays a considerable role in limiting the scope of one’s rights to privacy and data protection in this digital Panopticon model of State surveillance. For instance, the ECtHR has held that the surveillance via GPS and use of the data obtained thereby in criminal proceedings had been proportionate to the interests of national security and public safety, the prevention of crime and the protection of the rights of the victims, as the criminal investigation had concerned “very serious crimes” relating to terrorist activities. The ECtHR also noted that when acting in the interests of national security or for the prevention of serious crimes, State authorities are not expected to exhaustively disclose all the circumstances and conditions in which they can to resort to secret surveillance measures.

Clearly, the public interest is not alone sufficient to restrain one’s right to the protection of their private life and correspondence. Any interference must be “strictly necessary” and proportionate, striking a fair balance between the competing public and private interests at stake. Accordingly, any uses of big data by States for migration management or for the protection of vulnerable migrants should conform to these exigencies, even if State action is motivated by legitimate interests such as public safety or the protection of the rights and freedoms of others. For instance, the protection of vulnerable migrants’ personal data and privacy should be taken into account while States put forward efforts to prevent irregular migration and fight human trafficking and people smuggling.

---

155 The Panopticon, as proposed by Jeremy Bentham, is a circular building structured around a central watch tower from which a watchperson can monitor the individuals placed in cells below her, without being noticed. See JEREMY BENTHAM, WORKS OF JEREMY BENTHAM, vol. 4 (Panopticon, Constitution, Colonies, Codification) (John Browning ed.) (1843). See also, RHEINGOLD HOWARD, THE VIRTUAL COMMUNITY: FINDING CONNECTION IN A COMPUTERIZED WORLD, 289 (1994) (introducing the term digital Panopticon).


157 Uzun v. Germany, supra note 149, ¶¶ 52 & 80.


159 See notably, Klass v. Germany, supra note 149, ¶ 42; Szabó and Vissy v. Hungary, supra note 85, ¶ 73.

160 See Article 8 (2) of the ECHR.

161 See UNGA, New York Declaration for Refugees and Migrants, supra note 72, ¶¶ 23 and 35.
Big data can also have important consequences with respect to horizontal relationships between private parties. Individuals voluntarily consent to the collection, storage and occasional use of their data by the companies that provide the service they benefit from. Moreover, they voluntarily upload information on social networks such as Facebook, Instagram, YouTube, or Twitter and they allow mobile applications to track their activities, their movements, or even their health statuses and sleep patterns. Therefore, non-State actors potentially have access to a goldmine of information about individuals’ behaviour, including migrants’ behaviour. This has implications for their expectations as to privacy and data protection. Accordingly, it is necessary to factor non-State actors such as private companies into the equation as well. As Sarah Horowitz correctly observes, “Foucault’s model of the Panopticon is more helpful in thinking about state surveillance – which is not voluntary – than it is for thinking about our interactions with private data collection efforts.” In this regard, the contemporary digital Panopticon has not one but several watchpersons, pursuing a plurality of objectives not always based on the safeguarding of the public interest.

Consequently more rigorous control of the use of new technologies in the field of international migration is necessary. The existing legal frameworks should be strengthened to regulate collection, usage and storage of personal data and metadata by State and non-State actors alike. Otherwise, the misuse of such technologies could bring about serious negative outcomes to already vulnerable migrants.

162 For the analysis of the issue of consent, see Bart W. Schermer, The limits of privacy in automated profiling and data mining, 27 COMP. L. & SEC. REV. 45, 49 (2011) (explaining that despite giving consent for the processing of personal data, individuals underestimate the risks that certain uses of this data can have, such as in the case of automated profiling); Fred H. Cate & Viktor Mayer-Schonberger, Notice and consent in a world of Big Data, 3 INT’L DATA PRIVACY L. 67, 68 (2013) (discussing the formality of notice and consent in collecting and processing big data).


164 See 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 (May 4, 2016) (the EU is pioneering a more restrictive data protection system with the adoption of the new General Data Protection Regulation).
V. Conclusion

As new technologies evolve, they present important challenges and valuable opportunities for States under IHRL. Because the development of new technologies based on big data affects States’ capabilities, they can be used as a tool for protection of vulnerable individuals.\textsuperscript{165} Firstly, big data analysis can be a helpful asset, informing decision-making processes and possibly contributing towards better management of migratory movement and the adoption of sensible policies for reception and integration of migrants and refugees.\textsuperscript{166}

Secondly, it is suggested that big data can also play a greater role beyond international migration management, as a tool for the identification of individuals in need of protection, such as migrants at risk of dying at sea and those who are potential victims of ill-treatment and human trafficking.\textsuperscript{167} As new technologies evolve and improve State capabilities, the interpretation of what is reasonably expected from States should also evolve. Whereas it is not possible to generally infer that States have a comprehensive obligation to use new technological means to protect migrants’ lives and against ill-treatment or human trafficking, State positive obligations under IHRL may encompass such means in specific circumstances, such as in the case of the prevention of migrant deaths at sea.\textsuperscript{168}

However, the uses of new technologies based on big data analysis are not without risks. They could be used as an additional tool of control leading to further criminalisation of migration and increased risks of refoulement.\textsuperscript{169} Moreover, in the wrong hands, behavioural digital data could be used to increase the oppression of already exposed groups of people, amplifying their vulnerability and even preventing them from seeking asylum abroad. Besides, unbridled digital surveillance by public authorities could amount to unjustified interference with the right to the protection of one’s private life and correspondence.\textsuperscript{170}

Therefore, as new technologies are being developed, they should be regulated by laws and covered by policies at the international level. Data collection, storage and accessibility of

\textsuperscript{165} See supra note 43 (on the concept of vulnerability).
\textsuperscript{166} See supra Section II.
\textsuperscript{167} See supra Sections III, B and III, C.
\textsuperscript{168} See supra Section III, B.
\textsuperscript{169} See supra Section IV, A.
\textsuperscript{170} See supra Section IV, B.
information should be considered and regulated prior to any comprehensive use of behavioural digital data for migration management or protection purposes. States should agree to adopt a rights-based approach in this area. Ideally, that should become part of the current process of negotiations of the Global Compacts on Migration and on Refugees.\textsuperscript{171} New technologies and innovation have the potential to be used as a powerful instrument for the protection of migrants’ legal rights. However, they can also be used to deny refuge or exclude individuals from protection. Accordingly, they should evolve within the existing legal framework of IHRL.