Global Campus Europe

UNIVERSITY OF NOTTINGHAM

European Master's Degree in Human Rights and Democratisation
A.Y. 2017/2018

Human Rights Obligations of Information and Communication Technology Companies in the Context of Data Governance

Author: Anastasiia Zlobina
Supervisor: Jeffrey Kenner

Abstract

While users all over the world entrust Information and Communication Technology (ICT) companies with sensitive data on a daily basis, cases of data leakages and privacy breaches have been constantly appearing in the last decade. At the same time, a cumbersome apparatus of a state does not always manage to promptly respond to the rapid technological developments. Adopted in 2011, the United Nations Guiding Principles (UNGPs) armed international law with a tool for implementation of the human rights approach in the context of business activities. However, up to now there is a number of issues regarding UNGPs implementation in ICT sector. Thus, it is important to put the general requirements for corporate responsibility to respect human rights into the operational context of ICT sector and take into consideration such issues as data usage for Big Data Analytics, privacy impacts remediation and operation in countries with high level of human rights risks. Hence, this research aims to analyse obligations that ICT companies have according to different levels of regulations and discover the ways to implement them based on existing best practices and initiatives. It also discusses the models of users empowerment and the role that they might play for their own data privacy.

Table of Acronyms

BDA - Big Data Analytics
CAHDATA - Ad hoc Committee on Data Protection
CJEU - Court of Justice of the European Union
CLAHR - Committee on Legal Affairs and Human Rights
CoE - Council of Europe
DGHRRL - Directorate General Human Rights and Rule of Law
DPD - Data Protection Directive
EC - European Commission
ECHR - the Convention for the Protection of Human Rights and Fundamental Freedoms
ECPA - Electronic Communications Privacy Act
ECtHR - European Court of Human Rights
EU AFR - European Union Agency for Fundamental
FSB - Federal Security Service of the Russian Federation
GDPR - General Data Protection Regulation
GMs - Grievance Mechanisms
GRI - Global Reporting Initiative
HRC- Human Rights Council
HRIA - Human Rights Impact Assessment
ICCPR - International Covenant on Civil and Political Rights
ICT - Information and Telecommunication Technology
IMAX - Image Maximum Cinema
MNCs - Multinational Corporations
NSA - National Security Agency
OECD - Organisation for Economic Co-operation and Development
OHCHR - Office of the United Nations High Commissioner for Human Rights
OLGMs Pperational-Level Grievance Mechanisms
PbD - Privacy By Design
PESIA - Privacy, Ethical and Social Impact Assessment
PIA - Privacy Impact Assessment
R2R - Responsibility to Respect
SRRP - Special Rapporteur on the Right to Privacy
SRSG - Special Representative of the Secretary General
UDHR - Universal Declaration on Human Rights
UNGPs - The United Nations Guiding Principles on Business and Human Rights
VPN - Virtual Private Network

Table of Contents

Introduction.....5

Chapter One: Responsibility to Respect.....9

§1 Data Protection Obligations of ICT Companies.....9

United Nations Level.....9

European Level.....13

a) Council of Europe.....13

b) European Union.....16

UNGPs and Good Practice Multi-Stakeholder Initiatives.....20

§2 Big Data: Business and Human Rights Issues.....29

Chapter Two: Business Obligations in the Context of Access to Remedy.....36

§1 Corporate Remediation: Business Incentives and General Requirements to Operational-Level Grievance Mechanisms.....36

§2 ICT Sector Grievance Mechanisms Case Study.....40

Chapter Three: Balancing out Business Obligations and State's Duty to Protect.....43

§1 Criteria for Legitimate State Surveillance.....43

§2 Case Study: Sharing Data with a Government in the Name of National Security. Digitally Facilitated Repressions.....47

Conclusion.....52

Bibliography.....56

Table of Cases.....63

Table of Legislation.....65

Introduction

"To the future or to the past, to a time when thought is free, when men are different from one another and do not live alone— to a time when truth exists and what is done cannot be undone: From the age of uniformity, from the age of solitude, from the age of Big Brother, from the age of doublethink — greetings!"

(George Orwell, 1984)

In 2010 Google's then chief executive Eric Schmidt observed that 'Google is not a country. It does not make laws. It does not do state-to-state diplomacy. But we have to secure our borders' (Ash, 2017, p. 47). He then corrected himself to 'secure our networks', but this slip of the tongue seems to fit perfectly with the role that Information and Communication Technologies (ICT) companies are playing in life of their 'netizens' nowadays. Even though, clearly, even biggest businesses are not states, they might have enough power to exercise certain functions that have always been under the ambit of states' obligations. According to Sergey Kapitsa's theory of historical time acceleration, the time between breakthrough scientific achievements that deduced humanity to a qualitatively new level of development has been shrinking throughout the whole history of humankind up to the point when these achievements happen so often that people do not have time to get used to it. VHS, DVD or IMAX, Sega, PlayStation or Oculus Rift virtual reality headset, home phone, pager or smarphone are not just different stages of development but different generations coexisting together. When one is touched by the image of a granny puzzled by complexity of a smartphone, he or she might not always imagine the way world could become even more complicated once the old age comes. The question is thus if it is realistic to expect from a cumbersome apparatus of the state a prompt reaction and regulation of innovations. Currently, we are witnessing a historical momentum of a shift from responsibility of states to tackle the dangers of technological development to responsibility of innovators to prevent their creation from causing harm.

We believe that the human right approach is can facilitate this shift the most. Whereas duty to protect against human rights violations has always been a an obligation of states, the universal nature of human rights makes them applicable to all, including private actors. Back in 2011, John Ruggie's breakthrough UN Guiding Principles on Business and Human Rights (UNGPs) armed international law with a tool for establishing companies' responsibility in the context of human rights. From the very beginning this Framework served as a common denominator for all the business sectors outlining a minimum moral benchmark of society's expectations from business activities. However, the necessity of hard law regulations and clarifications on how Protect, Respect and Remedy Framework should be implemented is

apparent. This is especially relevant for the ICT companies that lead the innovation process while, as we established above, it is hard for states to regulate and mitigate the dangers that it could bring to human rights. Whereas ICT companies have been using this gap for their commercial benefits, international, regional and national legal frameworks have been tightening corporate obligations in human rights sphere. When it comes to ICT companies, most of the human rights impacts are connected to the data governance aspect of business activities. Consequently, the question of this research paper is **what are the human rights obligations of ICT companies in the context of data governance**?

Before proceeding to the structure of the research, we would like to outline its scope. Firstly, despite the fact that data governance is characteristic for most of the businesses where employers govern information about their workers, for instance, we aim to concentrate on data governance in the context of specific relations between ICT companies and their users. For the purpose of this research, we define ICT companies as mobile, Web-based and telecommunication products and service providers that are entrusted with personal data of their users due to the mere nature of business activities (for example, such companies as Google, Apple, Sony, Facebook etc.). We also acknowledge that data governance might cause different human rights impacts, including freedom of speech and expression, right to information, freedom of assembly (through blocking announcements on social media about planned protests, for instance) etc. However, each right and freedom defines different forms of business obligations' implication. Thus, we decided to focus on the right to data privacy (also known as right to privacy, right to data protection, right to respect for private and family life or users' privacy depending on a legal framework). This decision was dictated by numerous revelations regarding data privacy breaches by companies which were entrusted with this data (for instance, the case of Cambridge Analytica, previous revelations of WikiLeaks and Snowden etc.). Data privacy was also chosen as a focus of this research as there is a clear lack of guidance on how exactly human rights due diligence or remediation should be exercised in the context of ICT sector including the problem of Big Data Analytics which will be discussed in this research in detail.

The structure of the research will be therefore based on the UNGPs. The First Chapter will concentrate on corporate responsibility to respect. According to the UNGPs Framework, the first responsibility of companies in relation to human rights is the corporate responsibility to respect. This prescribes companies to restrain from any actions that could infringe human rights. When it comes to the ICT companies and data governance, the first issue arising is the issue of data protection. Information and communication companies may breach their users' rights through collecting data without their informed consent, collecting data for reasons other than those that data subject agreed on or illegitimately transferring data of their users to the third

parties. Thus, the first paragraph of the First Chapter will focus on companies' performance on obligations rooted in the UN international law framework, European level of data privacy protection, namely, (a) Council of Europe and (b) European Union, as well companies' performance on obligations flowing purely from the UNGPs second pillar. As these obligations are not being perfectly fulfilled by information and communication technology companies, the research will not only cover existing positive practices but will also look into initiatives and suggestions on ways to overcome existing gaps. On that matter, the following solutions will be critically assessed: due diligence in the ICT sphere, transparent reporting on steps undertaken by companies in order to achieve data protection, civil society rankings and socially responsible lobbying and other most interesting suggestions of academics in this sphere (for instance, some researchers offer to introduce a uniform data processing algorithms that would allow to achieve full transparency regarding collection of data by companies and to inform users on purposes of data collection).

The second paragraph of the First Chapter will focus on a separate issue within the question of corporate responsibility to respect human rights in ICT sphere, namely, the issue of Big Data. The latter can be in short described as immense amounts of data collected about users and used for the purpose of Big Data Analytics. Despite numerous initiatives such as the Global Initiative Network and soft law developments such as Council of Europe Guidelines on Big Data, there is a high degree of uncertainty in regulation on that matter. Considering the shocking scale of Big Data uncontrollably collected on a regular basis from users all round the world, confirmed by examples such as the recent leakage of 87 million Facebook users' and their friends' personal information to Cambridge Analytica, it is important to understand the severity of damage to human rights it can bring. The research will look into ways of establishing clarity in the abovementioned obligations such as an international treaty, national regulations etc. For instance, some researchers believe that the nature of Big Data is so broad that it is impossible to encompass all the nuances in one treaty; thus, they suggest to create an overall 'moral code' that would restrict companies to certain values and force them to interpret their action in accordance to them (Mai, 2016).

The Second Chapter will discuss the third pillar of the UNGPs which requires remediation for human rights abuses. Despite the fact that strengthening this pillar appears to be at the top of agenda for all the business sectors (as outlined by Working Group on Business and Human Rights in 'Realizing access to effective remedy' as well as in OHCHR's Accountability and Remedy Project), ICT companies significantly underperform in creating grievance mechanisms. Thus, we aim to examine in the first paragraph of the Second Chapter both existing and suggested company and industry and multi-stakeholder mechanisms that would allow to

enhance companies' performance on data privacy protection. Moreover, considering the fact that implementation of these mechanisms' requirements could be quite challenging for the companies, we will also look into good practices amongst ICT sector in the second paragraph of the Chapter.

According to the UNGPs, it is not only companies that have obligations in the context of business activities. States are still standing at the core of human rights protection ensuring conformity of corporate activities with human rights. As a first pillar of the Guiding Principles Framework, the duty to protect is supposed to guarantee human rights implementation when private actors fail to do so, as well as to incentivise companies to comply with their responsibility to respect. What will happen, however, if a state is unwilling or unable to guarantee human rights or even causes or contributes to violations itself? The Third Chapter of the research will tackle this question from the perspective of ICT companies' operational context. For data governing companies, the biggest threat to users' data privacy in countries where human rights are at high risk is a state surveillance. As surveillance for national security purposes might be necessary in all states, in the first paragraph of the Chapter we will look into requirements for a legitimate state surveillance and, thus, identify when the clash between corporate responsibility to protect users' data and state interests should be resolved in favour of latter. Finally, the second paragraph will analyse what ICT companies do, if even they can do anything, when operating in countries where state surveillance is conducted in the illegitimate manner. For that purpose we will concentrate on three countries with different regimes, namely, China, Russia and the US in order to identify what leverage ICT sector might have on government in autocratic, semi-autocratic and democratic regimes.

While we entrust ICT companies with the most sensitive information that might not only endanger our privacy, once revealed, but even physical integrity in certain operational contexts, we do not even know what this information can be used for, what kind of predictions about us it can contribute to or even what exactly we consented to when clicking 'agree' button under the Terms of Service. At a time when businesses obligations are being defined, users should be actively showing their interest in ICT companies' diligence when assessing and preventing their human rights impacts. Currently, though, the model of responsible user in context of ICT companies activities does not seems to be realistic in the nearest future. Thus, the threats to data privacy should be addressed by companies to the best of their abilities. Whereas we hope that the future will bring more tools, which will be discussed in this research, to empower users and accelerate the beginning of the age of full users' control over their data, for now, from the age of Big Brother - greetings!

Chapter One: Responsibility to Respect

§1 Data Protection Obligations of ICT Companies

United Nations Level

The right to privacy has always played a crucial role within the concept of human dignity. This right is interrelated with other fundamental values of any democratic society such as freedom of expression and opinion. Granted by Article 12 of the Universal Declaration of Human Rights (UDHR), this right guarantees the protection of individual's privacy against arbitrary interference and attacks (1948). Article 17 of the International Covenant on Civil and Political Rights (ICCPR) placed the *unlawful* interference with the right to privacy under the ambit of Covenant's protection (1966). Derived from the International Bill of Human Rights, which became a symbol of international community's consensus on the core values of humanity, the right to privacy received a strong protection within the international law.

'Can the right to a minimum privacy be protected in the face of ever-present listening and seeing electronic devices?' questioned the then UN Secretary-General U Thant in 1968. Ironically, just one year later, on 29 October 1969, a message was sent from a computer at the University of California to the one in Stanford Research Institute which marked the beginning of the Internet history (Garton Ash, 2017). Asked half of a century ago, Thant's rhetoric question symbolised the formation of data protection paradigm in international law development, the importance of which has been swiftly rising ever since. However, despite the fact that the increased pace of technological development revealed the necessity of personal data protection, it was hard to place it within the extremely inflexible international law framework of the Cold War period.

Political controversies led to the UN efforts to 'renew the commitment pledged by states with the adoption of the UDHR' and to put the notion of data privacy within the broader right to privacy (Yilma, 2018, p.3). The ideological contradictions, however, did not allow to specify what exactly the right to data privacy implied. Moreover, states were reluctant to legally restrict their ability to use their citizens' data appealing to the sake of national interest. It is necessary to stress that the whole concept of International Bill of Human Rights was based on the broad definitions of fundamental rights and freedoms that would allow to achieve the compromise easier. Thus, the only regulation that was adopted on that matter were the Guidelines for the Regulation of Computerized Personal Data Files (1990). As a soft law instrument, this document did not impose any obligations on states in the context of personal data protection, nor has it identified responsibilities of private companies. However, even back then the Secretary General's

1974 Report offered the principle of 'legal responsibility of computer manufacturers and software developers regarding security of information systems', which was eventually not included, to be embodied in the Guidelines (Yilma, 2018, p.6).

Consequently, despite the presence of data protection provisions in a number of UN treaties (for instance, the Disability Rights Convention [2007]), it is barely possible to call the United Nations framework for data protection a strong legal mechanism. However, it can be beneficial for the purpose of our research at least in two ways. First of all, the abovementioned political controversies of the twentieth century explain the vagueness of the right to privacy wording in the International Bill of Human Rights. The minimum common denominator found in a formula of right to privacy for the sake of compromise did not amount to clear obligations of states in the context of surveillance.[1] Secondly, the interpretation of personal data protection as a part of a broader right to privacy contributes to understanding of the role of personal data within the international human rights law universe. For instance, the European Court of Human Rights (ECtHR) followed the UN approach and encompassed the right to data privacy within Article 8 of the Convention.

Obviously, international law of twentieth century did not have a mechanism for establishment of businesses responsibilities for data protection outside of the states' duty to protect. Nonetheless, the pace of technological development made its contribution to the international law narrative. In August 1981 a number of internet hosts was limited to 213 (Garton Ash, 2017). Before the Internet and modern technologies entered our houses, personal data was associated with records about citizens kept by state on computers. Back in 1980s a privacy pioneer Willis Ware talked about data protection in the context of computing technology as a 'record-keeping privacy' (1984, p. 315). According to him, without computing technology that allows to keep records in a compact way, the United States 'would literally have difficulty running a country of this magnitude with paper, pencil, and green eyeshades' (Ware, 1977, p. 356). Moreover, Ware did not see high 'technical threat in the commercial sector' as, according to him, 'in the private sector, we need *only* the corporate will to address the problem and the corporate commitment to put the issue on the same level of concern as that of protecting other valuable resources' (1984, p. 316, emphasis added). Ironically enough, it is exactly the lack of corporate will and commitment that served as a barrier for consensus on business responsibilities in the context of human rights up to 2011 when the international law was finally armed with the mechanism for business responsibility. That is, United Nations Guiding Principles. Indeed, the

[1] This will be further discussed in the third chapter.

Guiding Principles provided a framework for enhancing business obligations of ICT companies through legislative initiatives which will be discussed below.

Futuristic and theoretical in 1984, Ware's question about 'what might have happened if the [e-]mail service had been provided by a commercial vendor' (1984, p. 316) seems somewhat ridiculous nowadays. Clearly, personal data protection narrative changed so drastically in the last decades, that the necessity of its reconsideration inevitably arose in twenty first century. In 2013 the General Assembly adopted a resolution 68/167 which revived the data protection issue in the context of state surveillance as well as affirmed that 'the rights held by people offline must also be protected online' (para 3). The scale of data collection exercised by business entities reached such a high level that states had to push companies to transfer the users' personal data for the sake of national security. Acknowledging this shift, the 2014 OHCHR Report on the Right to Privacy in the Digital Age emphasised for the first time that 'there has been a delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries under the guise of self-regulation or cooperation' (para 42). Moreover, the Report notes that 'company risks being complicit in or otherwise involved with human rights abuses' even if it acts in accordance with the state's order to transfer users' data (Office of the United Nations High Commissioner for Human Rights [OHCHR], 2014a, para 43). Hence, despite the heavy emphasis on state surveillance triggered by WikiLeaks' and Snowden's revelations, the issue of private actors' role in the context of data protection and right to privacy was eventually brought up.

This tendency was continued by Human Rights Council within the panel discussion on the right to privacy in the digital age (OHCHR, 2014b). During the discussion delegations requested for business transparency and accountability in their conduct (para 54). The summary of this event had two vital conclusions in the context of business responsibility for data protection. Firstly, the standard-setting role of the United Nations was presented as a tool to support businesses in 'meeting their responsibility to respect and protect the privacy of users' and the encouragement of Member States to adopt the data protection standards in their domestic law (para 61). Secondly, during the discussion a number of NGOs 'called upon Council to establish a mandate for a Special Rapporteur on the Right to Privacy (SRRP)' which was eventually done in 2015 (para 57).

However, the biggest shift regarding the abovementioned standard-setting for businesses in the context of data protection within the UN framework is yet to come. In February 2018 the Workshop with the purpose of identifying and clarifying principles, standards and best practices regarding the promotion and protection of the right to privacy in the digital age, *including the responsibility of business enterprises in this regard* was held in Geneva (emphasis added). Its Concept Note did not only bring up into focus the companies' responsibilities outside

of the surveillance context but also put 'business enterprises … role vis-à-vis States' (OHCHR, 2018, para 15). This workshop was organised in accordance with Human Rights Council Resolution which called the UN Commissioner for Human Rights for the Report on the Workshop's topic to be submitted on Council's thirty-ninth session (September 2018) (Human Rights Council [HRC], 2017, para 10). Despite the fact that Resolution stresses State's 'obligation and ... primary responsibility to promote and protect human rights and fundamental freedoms' (HRC, 2017, para 2), it has clear references to business responsibilities regarding data protection:

1) The right to privacy in the digital age is included in the United Nations "Protect, Respect and Remedy" Framework (para 8).

2) Businesses should 'inform users about the collection, usage, sharing and retention of their data that may affect their right to privacy' (para 8).

3) Businesses should 'establish transparency and policies that allow for the informed consent of users' (para 8).

4) 'Business enterprises [should] work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption and anonymity' (para. 9).

Surely, these guidelines on exact implications of business responsibilities for data protection are yet to be clarified in the upcoming report. However, considering the standard-setting power of the UN, outlined above, these directions for the work of UN Commissioner for Human Rights give a clear hint of special attention from United Nations' legal rhetoric to ICT sector responsibilities. More importantly, it can be expected that these responsibilities will be considered without the connotation of businesses' role in state surveillance. Naturally, this shift could only be possible due to adoption of the UNGPs which served as a tool for raising the question of companies' responsibility for data protection outside of the states' duty to protect.

Hence, we have now established the roots of the data protection within the UN international law. Political controversies of the twentieth century caused the inclusion of right to personal data protection under ambit of the right to privacy rooted in its strong legal protection by the Bill of Human Rights. However, the broad definition of right to privacy did not allow to create clear implications of the data protection obligations of states including corporate obligations in the context of business activities which should be ensured by states. Moreover, the 1990 UN Guidelines for the Regulation of Computerized Data Files failed to compensate this gap. Despite remaining emphasis on data protection existence within the right to privacy, now in digital age, the personal data issues entered qualitatively new era within UN framework. Initially brought up within state surveillance revelations context, United Nations soft law has been paying

special attention to the role of businesses in data governance as well as companies responsibilities on that matter, facilitated by the UNGPs provisions.

Other international frameworks that aim at data protection include the one of Organisation for Economic Co-operation and Development (OECD). A central regulation within it is indeed the Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data adopted in 1980 and revised in 2013. The Guidelines welcome non-Member States to adhere to them. Interestingly, despite the fact that the Guidelines provide a clear connection between data protection and privacy, they do not explicitly put data protection under the ambit of privacy as a right. The Guidelines adopted a principle-based approach which includes limiting data collection, data quality, purpose specification, openness (about practices and policies on data protection) etc. The distinctive feature of Guidelines is 'implementing accountability' for the controllers. However, provisions on accountability in a sense given to it by OECD seem to correlate more to responsibility to respect as provided by UNGPs. For instance, they require controller to introduce a 'privacy management programme' (in UNGPs- policy commitment) which should not only adopt Guidelines but also provide 'appropriate safeguards based on privacy risk assessment' (in UNGPs - due diligence) and include 'plans for responding to inquiries and incidents' (in UNGPs- processes to enable remediation). Surely, we do not claim that the Guidelines adopted UNGPs framework intentionally as they use a different language and provide for more measures to provide accountability in a sense given to it by Guidelines. Nevertheless, introducing measures corresponding to the UNGPs by OECD within the data protection framework is a form of acknowledgment of UNGPs' applicability and efficiency in the context of controller's activities. Despite OECD plays its role in international standard-setting, the Guidelines on Protection of Privacy did not constitute a powerful mechanism of data protection due to their soft and not enforceable nature (Mantelero, 2017).

European Level

a) Council of Europe

Perhaps it is the political difficulties in finding a compromise on data protection that made the biggest contribution to the formation of alternative personal data regulation at the European level. Like the Universal Declaration on Human Rights, the European Convention on Human Rights (ECHR) did not contain data protection provisions (1950). However, the Convention guaranteed the right to respect for private and family life. In case *S. and Marper v. The United Kingdom* [No 1581, 2008] the Court held that the 'mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8' (para 67).

Hence, following the aforementioned UN approach of encompassing data protection into the right to privacy, the European Court of Human Rights placed data protection under the ambit of Article 8 of the Convention. Despite the fact that the ECHR is purely directed at States' obligations, the Court's case law contains occasional provisions regarding businesses' obligations when acquiring and processing personal data that should be insured by states. For instance, in 2017 case *Bărbulescu v. Romania* (No 754) the Court held that dismissing the employee on the basis of his electronic communications and accessing their contents' breached the applicant's right to privacy. It was established that the company did not give a notice about personal data collection, nature of monitoring and degree of intrusion into Bărbulescu's personal life. However, a significantly more powerful instrument within Council of Europe's framework on data protection exists.

Since its adoption in 1981 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data has been remaining the leading instrument of personal data regulation in Europe. The distinctive features of this treaty include binding nature for its signatories supported by additional Protocol which requires the establishment of supervisory authorities (2001)[2], its openness to non-members of the Council of Europe and the principle-based approach. Despite the fact that the Convention 108 does not directly establish obligations for businesses, it does oblige states to apply Convention to the private sector, subject to their jurisdiction (*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1981, art. 3, para 1). That is, duties associated with processing data, outlined in the Convention, should be applied to business entities by states. At the same time, the treaty establishes certain duties for data controllers and processors. According to the Ad hoc Committee on Data Protection (CAHDATA) clarifications, 'controller' 'refers to the person or body having decision-making power concerning the purposes and means of the processing, whether this power derives from a legal designation or factual circumstances' (CAHDATA, para 22). A controller 'determines purposes and means' of data processing, that is, 'why' and 'how' it should be processed (European Commission [EC], n.d.). Thus, technically, the Convention indirectly establishes duties for companies which exercise controller's functions, even though these duties are meant to be enforced by states.

As we have already established, the pace of technological development drastically changed the approach to data protection which could not pass by the Convention 108. The process of Convention's modernisation has been lasting for the last seven years. In 2017 the Committee on Legal Affairs and Human Rights (CLAHR) noted that such a lengthy process

[2] The new modernised version of the Convention includes supervisory authorities in its main body.

threatens the Council of Europe's leading role in data protection on international law arena (para 4). On 128th session, which was held in Denmark in May this year, the final version of Modernised Convention was eventually drafted. The Protocol with amendments was opened for signature on 25 June 2018 (CAHDATA, 2018, para 6). Hence, in this research we will consider the new version of the Convention.[3]

As noted by Sophie Kwasny in an interview, Head of Data protection Unit of the Council of Europe, the modernisation aimed at four main components (Council of Europe Directorate General Human Rights and Rule of Law [CoE DGHRRL], 2018). Firstly, the range of controllers' obligations was widened. Thus, among the obligations of businesses, which exercise functions of the controller, the CoE names the duty to obtain free, informed, specific and unambiguous consent of the user, duty to process data proportionally to the explicit, specified and legitimate purpose, fairly and in transparent manner. Controllers are also obliged to maintain the quality of data collected, that is, adequate, relevant, not excessive, accurate, up to date and allowing to identify its subject for no longer than is necessary (*Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data* [Modernised Convention 108], 2018, art. 4). The second modernisation vector was directed at broadening the spectre of data subject rights. Because controller is responsible for granting these rights, each right of a subject has a corresponding duty for a controller. For instance, companies should grant their users access to information about their data processed by controller, grant the opportunity to object processing data on them etc. (*Modernised Convention 108*, 2018, art. 9).

Apart from that, trying to reaffirm its status as a leading global instrument in data protection, the Convention embodied approaches widely discussed by academics in the recent years. As noted by Kwasny, modernisation introduced privacy by design (PbD) concept (Schaar, 2010, p. 267). According to Article 10 of the modernised Convention, 'controllers ... shall design the data processing in such a manner as to prevent or minimise the risk of interference with … rights and fundamental freedoms' (2018). This provision falls within the core idea of the PbD, namely, the consideration of data privacy on design stage of new technologies (Kroener and Wright, 2014, p. 355). This approach strengthens proactive and preventative dimensions of data protection rather than reactive and preventive ones. Article 10 also requires controllers to 'examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing'. This correlates to what Inga Kroener and David Wright call 'privacy impact assessment' (PIA). They believe that a companies

[3] It is necessary to say, that despite the basic principles are preserved, the text of the Convention was changed very significantly. See the table of amendments: https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958.

with good practice PIA asses possible privacy impacts, consider stakeholders opinion, prepare recommendations and action plans and prepare a report on PIA (Kroener and Wright, 2014, p. 361). Clearly, 'examination of likely impact' implements the responsibility to respect, embodied in the UNGPs framework. Another concept implemented within the modernised version of the Convention according to Kwasny is the privacy by default. This means that the all the technical innovations should have maximum privacy settings once introduced to public without any manual input from users. The explanatory report on amending protocol puts it as a 'privacy friendly standard configurations' that would allow to reduce the amount of data processed and enhance its proportionality towards the legitimate aim (Council of Europe [CoE], 2018, para 89).

Another obligation flowing from the Convention 108 in its amended version is an obligation of controllers to 'take specific security measures, both of technical and organisational nature' (CoE, 2018, para 62). Moreover, controllers should be required to inform the supervisory authorities on data protection about any breaches that undermine the security of personal data (CoE, 2018, para 65). This is especially relevant in light of recent revelations involving Facebook and Cambridge Analytics. Other vector of modernisation outlined by Kwasny include the establishment of a monitoring mechanism and strengthening controller's accountability. The latter will be discussed in greater detail in the second chapter of this research.

b) European Union

Finally, another component within the European framework for data protection which needs special attention is the EU regulation on that matter. Adopted in 1995, the Data Protection Directive (DPD) stands at the roots of the EU data protection system. Back then there were only 15 countries in the European Union (EC, 2016), however, all of them were signatories of the Convention 108. According to the latter, parties had a right to expand the instruments that would grant the protection provided in the Convention. Hence, concentrating mostly on the specification of the Convention's principles, the DPD added its own twist to data protection introducing the requirement to establish supervisory authorities. Interestingly, the Council of Europe also adopted an Additional Protocol envisaging the establishment of a monitoring authority in 2001. Eventually, supervisory authorities evolved into a powerful institute which can be clearly seen from the provisions of the General Data Protection Regulation (GDPR). Nevertheless, the legal power of the Directive still laid under the soft law ambit.

We hope that to this point we managed to show the importance of historical context to the formation of the data protection law at least within the UN framework. Consequently, it can be argued that the historical momentum, at which the technological advancement stood at the moment of EU data protection law formation, predetermined its form. Already in 1995, when the

amount of internet users amounted to 16 million (Internet World Stats, 2018), the DPD's efficiency in the context of data protection online was questioned. By the end of 2000, however, this number grew to 360 million. Moreover, the UN approach of data protection incorporation into the right to privacy proved to be difficult to implement. That is how the right to data protection found its place at the heart of the EU primary law (European Union Agency for Fundamental Rights [EU AFR], 2014, p. 20). The Charter of Fundamental Rights of the European Union does not only guarantee 'the respect for private and family life (Article 7), but also establishes the right to data protection (Article 8)' (EU AFR, 2014, p.20). This right is also envisaged by Article 16 (1) of the Treaty on the Functioning of the European Union. Naturally, this approach does not only distinguish EU system from ECHR and UN ones, but also sets data protection at the level of fundamental rights protection.

Perceived to be one of the most prominent systems in data protection sphere, EU legislation made a successful attempt to catch up with technological development pace through adoption of the GDPR in 2016. Embodied in numerous emails on privacy and data protection policies updates, received by users all over the world from ICT companies and not only, the Regulation entered into force on 25 May 2018. This quiet revolution in the world of data protection has a tremendous meaning for the future of data protection and, more importantly, for the businesses obligations and accountability. Lasting for years, the European data protection reform aimed at setting the unified standards for data processing regulation amongst Member States. That explains the detailed nature of the GDPR which distinguishes it from the principle-based Convention 108.

It is necessary to notice that one of the aims of Convention 108 modernisation was 'to ensure consistency and compatibility with other data protection legal frameworks, in particular the one of the EU'. Thus, the strong connection between modernised CoE Convention and GDPR is apparent. For instance, the modernised Convention 108 now includes the supervisory authority requirement in its main body (not in the Additional Protocol). Moreover, the Regulation incorporated European case law developments. For instance, GDPR included in Article 17 a provision on right to erasure ('right to be forgotten') which was introduced by the European Court of Justice in 2014 (*Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja*, No C-131/12). According to A. Mantelero, the GDPR has also reinforced the basic principles encompassed in the Directive 95/46/EC reaffirming the convergence created by the latter (2017, p. 286). He notes that following the Directive's tradition, the EU data protection is still heavily based on the users rights, 'notice and consent' model and 'the principles of purpose limitation and data minimization' (Mantelero, 2017, p. 286). However, apart from these provisions the GDPR contains the whole chapter on controller's and processor's

obligations. Moreover, these duties are supported by the fine up to 20 000 000 EUR (European Parliament and the Council, 2016, art. 83). Furthermore, despite the direct application of the GDPR to the Member States, it took two years for the document to enter into force unlike the DPD. Hence, following the aim of this research we will not analyse the discussed above principles established both on CoE and EU levels, nor will we analyse the extent to which the new Regulation encompassed the European case law on that matter. Instead, we will focus on novelties brought by the GDPR in the context of businesses obligations outlined outside of the scope of the users' rights.

According to the GDPR, 'appropriate technical and organisational measures' should be implemented by the controller in order to 'ensure and to be able to demonstrate that processing is performed in accordance with this Regulation'. These should include, for instance, data protection by design and by default, definitions of which were outlined above. In general, unlike UNGPs, the GDPR does not perceive the adoption of data protection policies as an obligatory measure. At the same time, acknowledgment 78 of the Regulation prescribes that 'the controller should adopt internal policies ... which meet in particular the principles of data protection by design and data protection by default'. Also, controllers are required to keep record of data 'processing activities under [their] responsibility'. They should also cooperate with the supervisory authority. The latter obligation implies among other things duty to notify authorities in case of data breach within the defined amount of time. Interestingly, in cases when data breach *is likely to cause violation* of users' rights, companies are obliged to notify the data subject too (emphasis added). Another set of obligations encompassed by the Regulation is connected to granting personal data security. The recommended measures ensuring the 'level of security appropriate to the risk' (such as destruction, loss alteration etc.) include pseudonymisation and encryption, regular assessment of security measures effectiveness, ensuring data processing confidentiality, integrity, availability and resilience and the ability to restore the access to data.

The Data protection impact assessment was already discussed in the context of CoE law. However, the GDPR provides a significantly more detailed approach to PIA. The Regulation envisaged a necessity of impact assessment in situations of high risks that the data processing could bring to data subjects' rights, for instance, when a new technology is implemented. This should be exercised before the beginning of an actual processing. The GDPR in particular stresses the necessity to exercise the PIA in situations like systematic automated processing of personal aspects which might produce legal effects. Supervisory authorities are responsible for publishing a list of data processing scenarios which need an obligatory PIA. Moreover, when the impact assessment revealed a high probability of rights violations, the

controller is obliged to obtain a consultation from the supervisory authority. The acknowledgment 89 stresses that previously DPD required notification of personal data processing in all the cases. Now this was cut to specific cases only. That proves the importance that this institution gained according to GDPR. However, the Regulation went even further in the context of control over controller prescribing companies to designate a data protection officer. Presumably, data officer is an adaptation of supervisory authorities integrated into corporate realm. Thus, companies are recommended to consult the data protection officer when exercising the PIA. Finally, the other way of demonstrating compliance with the EU data protection requirements offered by the Regulation are codes of conduct and protection certification mechanisms. However, they are now only recommended to be encouraged by Member States and do not constitute an obligation.

Finally, the GDPR aims to resolve issues connected to the transnational data flow. The Regulation does not only apply to companies established in the European Union but also to controllers offering goods or services to or monitoring behaviour of data subjects in the EU. These controllers are required to designate a representative in the Union. On the other hand, any activities of the establishment of controller in the Union should be exercised in compliance with regulation even if they take place outside of the EU. In general, the GDPR prohibits personal data transferring to countries without 'adequate level of data protection'. If this is not recognised at the European level (by the Commission), the controller might still transfer data after all the precautions and guarantees taken and the authorisation of supervisory authority is received.

While European approach to data protection as a fundamental right is argued to be the most prominent, this is not the only one. With a significant number of world's biggest data governance ICT companies situated in the US, the legal regime of data protection there is significantly different. The US approach is enabling the user as a new economic actor who can sell his data under conditions proposed by the company. According to the Federal Trade Commission Act, companies must ensure personal data security and comply with their own policies that they are obliged to disclose (2006). Thus, most of the data protection breach claims are based on the infringement of a data policy that the customer agreed with. This is completely different from the data protection right understanding which envisages protection despite any provisions foreseen in a contract between company and user. To bridge this difference, the Safe Harbour Privacy Principles for data transfers between EU and US were developed. Nonetheless, the case of *Schrems v Data Protection Commissioner* (No C-362/14, 2015) brought before CJEU led to abolishment of this agreement as the Court found the US level of data protection inadequate. This case, however, deserves a more detailed look as it serves as a powerful illustration to what an individual can be capable of in the context of transboarder flow of

personal information. After Snowden's revelations uncovered that EU citizens private data was given to US surveillance authorities even by those companies that were perceived to be 'safe', Max Schrems filed a complaint against Facebook Ireland to prevent it from transferring users data to Facebook US (which was suspected of giving users data to the US government). When the case reached CJEU, the Court held that the US failed to ensure an adequate level of protection for personal data of European citizens and thus were denied the Safe Harbour favourable conditions of transborder data flows between the US and EU. Despite the 2016 EU/US Privacy Shield agreement was eventually endorsed with stricter rules than in Harbour Privacy, this case highlighted existing controversies of European and US systems. In this context the potential of corporate responsibility to respect human rights standard global acceptance appears to be even stronger as it allows to bridge similar controversies.

Hence, the European data protection framework provides a variety of approaches. The European Convention of Human Rights and case law of the ECtHR interprets data protection as a part of the right to respect for private and family life. This can be interpreted as a restrictive interpretation of the data protection as the Court has to narrow the application of it to the limits of Article 8 even though it claims to understand personal data protection as stated in Convention 108. The Council of Europe Convention in its modernised version, on the other hand, acknowledges the right to protection of personal data as a separate right in its integrity with other rights. Despite its progressive nature and direction at strengthening accountability and powers of supervisory authorities, it is based on principles (f. ex. transparency, legitimate aim, consent etc.) more than it gives direct regulations on controller's obligations. Finally, the GDPR is based on EU's approach to data protection not just as a separate but also as a fundamental right encompassed by the EU Charter of Fundamental Rights and implemented in constitutions of Member States. Aiming at unification of data protection regulations within the Union, the EU Regulation is meant to be more precise when establishing controller's obligations. Moreover, the GDPR has direct force and accountability measures directly applicable to businesses exercising controller's functions. However, despite high degree of differentiation, all these approaches are united by one common denominator; being a separate right or a part of right to privacy, data protection is seen as an element of human dignity.

UNGPs and Good Practice Multi-Stakeholder Initiatives

As Timothy Garton Ash pointed out, once every user counted, the 'population' of Facebook would exceed the one of China (2017, p. 1). Despite the fact that, as shown above, business obligations regarding personal data processing are encompassed by numerous international, regional and national legal instruments, it is naïve to assume that all the threats to

data protection coming from private sector are addressed by them. Indeed, the line between the state's duty to protect human rights and corporate responsibility to respect them remains unclear. However, taking into consideration the tremendous impact that companies might have on human rights, it is barely possible to assume they cannot be held accountable for human rights infringement in cases that are not directly regulated by states. As one well-known moralist said, with greater power comes great responsibility. In our case, the responsibility to respect data privacy.

This triggered a few initiatives on the UN level that were aimed at establishment of business responsibilities. These initiatives, however, were declined both in 1980s (*UN Draft Code of Conduct on Transnational Corporations*) and in 2000s (*Draft UN Norms on Human Rights Responsibilities of Transnational Corporations and other Business Enterprises*). It is against this background that the mandate of Special Representative of the Secretary General (SRSG) on Human Rights and Business was established in 2005. It is hard to overestimate the importance of SRSG John Gerard Ruggie enormous work. Not only was the UN 'Protect, Respect and Remedy' Framework, prepared under the SRSG' command, approved by the Human Rights Council in 2008, but the mandate was extended in order to create recommendations on its implementation (European Parliament, Directorate-General for External Policies, 2017, p. 12). Performing this task, the SRSG presented the United Nations Guiding Principles on Business and Human Rights which were unanimously endorsed by the UN Human Rights Council in 2011.

Despite some criticism, the UNGPs framework can definitely be recognised as the most significant international legal platform for the business responsibilities in human rights sphere. However, considering the failure of the abovementioned initiatives of a similar nature, it is important to outline distinctive features of the UNGPs that make them stand out in the line of these initiatives. D. Bilchitz and S. Deva name three main components of the UNGPs in this regard. The first one is an approach of comprehensive consultations undertaken by the SRSG during the process of UNGPs drafting involving not only businesses but human rights NGOs as well. This element was criticised due to the lack of human rights violations victims representation. Despite fair ground for the criticism, this decision was most likely made in order to enhance the probability of compromise. The other distinctive feature of UNGPs is what Bilchitz and Deva call 'bottom-up' approach which is based on extensive participation of multinational companies(MNCs) in creation of the Principles. This is especially relevant in the context of the ongoing arguments on the binding nature of Guiding Principles which will be discussed below. The final feature is the 'principled pragmatism' embodied in intention to combine undisputed nature of human rights and 'pragmatic' approach that would be accepted by

the business. Despite Ruggie's vision of this approach as a key to the compromise, it was highly criticised as degrading the absolute nature of human rights. Prescribing companies to respect human rights instead of establishing an obligation to do so, the SRSG aimed to achieve less resistance from companies towards new norms. However, this search for the compromise on principles was criticised heavily by those who rather see human rights principles compromised. Nevertheless, it is hard to deny the impact the UNGPs have been having on convergence between business and human rights worlds nor to undermine their global standard-setting role.

The 'Protect, Respect and Remedy' Framework operationalized by the UNGPs is based on three pillars of the same name. While the duty to protect lays within the ambit of states' obligations, the corporate responsibility to respect (R2R) human rights sets the minimum standard of social expectations for business actors. The duty to provide remedy flows from state's obligation to protect and corporate R2R both for states and companies respectively. The second pillar, namely, R2R is especially applicable in the context of tech companies obligations arising from data governance. As Principle 11 states, the corporate responsibility to respect means restraining from causing or contributing to human rights violations and addressing the impact that company caused or contributed to. According to the UNGPs, this includes three main stages: policy commitment, human rights due diligence and enabling remediation. Whilst the responsibility of ICT companies to provide remediation will be considered in greater detail in the second Chapter, it is important to concentrate on the first two abovementioned elements of the R2R.

The Guiding Principles, as already mentioned, only provide minimum standards of societal expectations from business activities in the context of human rights. The Implementation Guide on Corporate Responsibility to Respect, adopted by the OHCHR in 2012, reaffirms that 'further work will be needed to develop such operational guidance, which will vary depending on the sector, operating context and other factors' (p. 4). This is especially relevant for the ICT companies activities which need additional guidance on implementation of the UNGPs. In order to adjust the UNGPs requirements for ICT sector, a few international initiatives were formed. Thus, this part of the research will concentrate mostly not on generic requirements of UNGPs but will look into challenges and particular approaches to their embodiment in the context of ICT activities.

Principle 16 of the UNGPs prescribes companies to implement human rights policy commitment. It also provides five basic requirements to the policy commitment, namely, senior level approval, external and internal expertise application, stipulation of human rights expectations from relevant parties, public availability and reflection in company's internal policies. The OHCHR's Interpretation Guide points out that the term 'policy commitment' is

rather generic and can take various forms depending on the company (Facebook Principles, Google's Code of Conduct, Microsoft's Global Human Rights Statement). Its central role is, however, to build a 'human rights skeleton' against which company can build its activities internally and externally. Despite the fact that corporate R2R covers the whole spectrum of internationally recognised human rights, certain impacts might prevail. Thus, depending on operational context, it could be beneficial to outline the most salient human right issues in the commitment. For ICT sector, according to the Implementation Guide, this includes freedom of expression and privacy. According to the European Commission Interpretative Guide, the commitment should be revised of necessity. Taking into consideration the pace of discussed above technological development, this recommendation is especially relevant in the operational context of the ICT companies.

When it comes to defining the content of the policy, companies are expected to commit to all human rights in general as a minimum. It could be beneficial for the ICT sector to include into their commitment reference to established international principles and initiatives. One of the most well-known initiatives relevant for data governing companies is the Global Network Initiative and its Principles on Freedom of Expression and Privacy which prescribes companies to protect their users against illegal or arbitrary interference with the right to privacy of their users including on government's request if it contradicts international human rights law. Other initiative is the UN Global Compact which was created before the UNGPs. According to Principles 1 and 2, 'businesses should support and respect the protection of internationally proclaimed human rights' and '... make sure they are not complicit with human rights abuses'. The UNGC 'Note on relationship between Global Compact Principles on human rights and UNGPs' states that UN Guiding Principles develop UNGC provisions (UNGC, 2014). However, Global Compact initiative also envisages positive obligations for business, that is, responsibility to promote human rights. Other initiatives include United Nations Global Pulse Privacy and Data Protection Principles, Principles for Digital Development, Business for Social Responsibility, the Responsible Business Alliance Code of Conduct (formally Electronic Industry Citizens Coalition Code) etc.

Outlining the most salient human rights risks in the policy commitment could also be quite beneficial for preventing these risks. EC Guide recommends ICT companies to start with engineers and developers that are most capable of predicting the issues connected to human rights. The Gide also recommends to involve stakeholders in order to develop the commitment. Apart from that, there always should be a 'human rights focal point' or 'human rights champion' within the headquarters of the company who will be responsible for embedding of the policy (Shift, Oxfam and Global Compact Network Netherlands, 2016, p. 44). Moreover, companies are

also expected to communicate their policy commitment. That should be done using 'appropriate methods' which include visualisation of information in an intelligible form. As we have already discovered, right to privacy is threatened the most in the context of ICT operation. Thus, communication about users' privacy should have a special attention. The Guide suggests, for instance, to allow users to choose privacy settings and to include information about company's policy on personal data access on public request. Another tool to communicate the policy commitment is the Terms of Service. Finally, the Guide envisages 'human rights by design' approach as a part of ICT corporate responsibility. That also means the presence of at least one team member in each development unit who accomplished a training on implementation of human rights.

The Business and Social Responsibility initiative highlighted the importance of policy commitment application in the context of business relationships. Indeed, a number of human rights violations flowing from data governance is connected to the way personal information is used by the third parties. The recent incident with Facebook and Cambridge Analytica when the latter gained access to 87 million profiles using the quiz taken by 300 000 Facebook users serves as a colourful illustration to this statement. Integrated into the companies 'DNA', human rights policies could serve as a shield against contractors with low level of human rights protection. Facebook's Code of Conduct, for instance, envisages possible termination of business relationships on basis of incompliance with Code's standards.

The second segment of the R2R is the due diligence. The main aim of this process is to identify, prevent, mitigate and account for the human rights risks. According to the Principle 17 of the UNGPs, this process includes for stages, namely, assessing actual and potential human rights impacts, integrating and acting upon findings, tracking responses and communicating how impacts are addressed. In general, Guiding Principles do not require due diligence to be a separate process as it might be included in other 'risk-management systems'. The only requirement provided by the UNGPs is company's focus on risks for affected stakeholders rather than for the company. However, according to some findings, the 'stand-alone' due diligence is more affective in the context of preventing human rights negative impacts.

As a first stage of due diligence, the human rights impact assessment (HRIA) is targeted at revealing not only the company's actual or potential human rights effects directly connected to its business activities but also those impacts that arise from company's business relationships. According to the OHCHR, for ICT companies this means assessment of adverse human rights impacts resulting from their terms of service and policies for customer data (OHCHR, 2014, para 45). The EC Guide classifies the latter impacts into 'contribution' that can take various forms, including encouragement or incentivising, and 'direct linkage of human right impacts to

company's products or services through business relationships' (EC, 2012, p. 32). In ICT reality most of the products that were created for a good purpose can also be misused by business contractors and customers. Thus, the assessment of possible implications flowing from such a 'dual use' is a responsibility of the company. The Guide suggests to evaluate these risks on a pre-sale stage, integrate human rights provisions into the contracts, exercise ongoing due diligence after the product is introduced and assess human rights risks within supply chains. In general, according to BSR recommendations, the HRIA on a product level is more crucial than site- or geography-level for ICT sector. The UNGPs require to conduct HRIA regularly, as an ongoing process which should take place before the start of any business activity. The EC Guide gives a special recommendation on the way due diligence should be conducted in the context of ICT companies activities. In particular, this process should not only consider the full life cycle of the product or service but also pay attention to its updates (EC, 2012, p. 30). The Guide also stresses the importance of human rights by design approach which could be a perfect solution for the fast-evolving nature of ICT technologies. Apart from that, it is recommended to ensure meaningful consultations with stakeholders (both obviously affected and those that are indirectly influenced, for instance, by chilling effects) and networked consultations. According to the UN Commissioner on Human Rights, in the context of ICT companies this includes ' meaningful transparency about how their data are being gathered, stored, used and potentially shared with others, so that they are able to raise concerns and make informed decisions' (OHCHR, 2014, para 46). As BSR Guidance points out, whereas companies themselves understand more about application of their product, the stakeholders can give valuable recommendations on possible or actual human rights implications of this product. However, the stakeholder engagement still remains a challenge to ICT sector due diligence.

The next stage of the due diligence process is marked by the UNGPs as 'integrating and taking appropriate action' (2014, Principle 19). In essence, this stage can be called central to the corporate R2R as it aims to actually prevent or mitigate human rights risks. Thus, its importance requires not only appropriate budget allocation but also designated responsibility on the highest managerial level. In the context of data governance the EC Guide recommends to take certain steps in order to guarantee personal information security, namely, informing users about purpose of data collection and where it is stored, store data for appropriate period of time, encrypt communications by default, create 'opt-out' mechanisms etc. Interestingly, these recommendations correlate to the modern GDPR requirements. As discussed above, corporate responsibility exceeds human rights impacts caused by company's direct actions. However, covering business relationships, due diligence might provide a strong leverage that companies can use to influence other parties. For instance, following the above mentioned clause of contract

termination on a basis of human rights violations, Facebook has recently suspended around 200 apps that misused customers data (Kuchler and Cocco, 2018). It is nevertheless important to take into consideration all the impacts that such a suspension might cause. Oxfam and Shift note that if negative human rights impacts occur in linkage with company's products, the company does not have a responsibility to remediate this harm, however, it does have a duty to use available leverage in order to mitigate these impacts. Surely, leverage mechanisms are not restricted to contract termination and can take numerous forms including multi-stakeholder collaborations, bilateral agreements, company's capacity building etc. Nevertheless, companies often use the leverage concept to distance themselves from negative impacts when leverage mechanism is not apparent. However, most of the human rights violations happen in the absence of company's control over suppliers, users or government's requirements. Thus, companies are recommended to be creative in order to avoid reputational damage and choose one of the mechanisms listed above.

The third stage of human rights due diligence is tracking the effectiveness of company's performance on human rights. In short, tracking means getting a feedback which can be obtained through internal reporting, grievance mechanism or other external and external sources UNGPs, Principle 20). EC Guide for ICT companies lists among these sources customer surveys, media monitoring and internal audits. Tracking indicators can be generally split in qualitative and quantitative. While the number of applications brought before grievance mechanism points could be interpreted as quantitative indicator, extensive feedbacks from affected stakeholders and online community consultations belong to a qualitative group. Oxfam and Shift Guidance stresses that ICT is one of the few sectors where companies are responsible for tracking relationship within the value chain (Shift, Oxfam and Global Compact Network Netherlands, 2016, p. 81). Namely, companies might be forced by state to hand over particular user's data if this user is suspected to infringe laws which falls under the ambit of state-citizen relationship. This Guidance also suggests to include the following information into the tracking mechanism: company's input into the human rights R2R (for instance, relevant trainings of the employees), incidents and the outcomes or general impacts that company has due to its activities. Tracking company's performance is a crucial step that correlates to the 'knowing' element of the 'knowing and showing' formula envisaged by the UNGPs. Knowing its weak and strong points, companies can improve their performance on corporate responsibility to respect. Finally, tracking can serve as a leverage mechanism within integrating and acting framework as, knowing their activities could be tracked in relation to the company's services and products, business partners have higher initiative to adhere to human rights standards.

The final stage of the due diligence process is communicating company's performance or, as UNGPs put it, 'account for how companies address human rights impacts' (Principle 21). It is the 'showing' component that is supposed to provide 'sufficient info' to evaluate company's performance to the external stakeholders. The EC Guide notes that companies with high probability of severe human rights impacts should report on the way they address them formally. In the ICT data governance operational context that implies communication on the way companies address data protection and privacy issues. Similarly to the other stages of due diligence process, communicating implies establishing official responsibility and stakeholders involvement. Communicating might include not only general information on company's performance but also its response to particular cases. For instance, the EC Guide recommends companies to notify users on data breaches, thefts or leakages of personal information and the ways they address these issues. Reporting might be restricted by confidentiality principles or potential risks for stakeholders. The EC Guide marks 'materiality' of the issues (the level of significance that dictates the necessity of disclosure) as a tool for striking the balance between communicating and confidentiality. In general, reporting on human rights performance enhances trust both from investors' and customers' perspective. Consequently, companies have an initiative to participate in international reporting initiatives such as UN Global Compact's Communication on Progress and UN Global Reporting Initiative (GRI). These initiatives developed standards for reporting on human rights responsibility. For instance, GRI 412 standard prescribes companies to report on HRIA which includes reporting on operations that were subject to HRIA, trainings for staff and contracts that include clauses on human rights. GRI also has a standard 418 on Customer Privacy which is directly applicable to ICT sector. According to it, companies should disclose the number of complaints about data losses or privacy breaches, number of identified leaks, thefts and losses of data.

Despite the outlined above standard-setting role of the United Nations, its power to establish direct human rights obligations for companies is somewhat dubious. Reports state that the implementation of the UNGPs is remaining at the low level (Working Group on the issue of human rights and transnational corporations and other business enterprises, 2018, p. 15). At the same time, as outlined above, good practices on corporate responsibility to respect for ICT sector are not undefined. Consequently, the question on binding nature of UNGPs' R2R for companies is rooted in the legal nature of UNGPs per se. According to the Guiding Principles, their provisions are based on existing human rights obligations of states flowing from international law. Whereas the source of the state's duty to protect human rights and remedy their violations is easy to find, direct obligation of companies to respect human rights does not seem to have any obvious roots in international law. Nevertheless, UNGPs claim responsibility to respect to be 'a

global standard of expected conduct for all business enterprises ... [existing] independently of States' ... obligations ... and over and above compliance with national laws and regulations protecting human rights' (Commentary on Principle 11). Thus, the question is, what are the roots of such a global standard. This issue is especially relevant for the ICT sector due to the rapid development of technology which brings new threats to human rights and cannot be immediately addressed by a legislator.

According to the OHCHR, the UNGPs are based on 'existing standards and practices for States and businesses' (United Nations Global Compact Office and Office of the United Nations High Commissioner for Human Rights, 2011). However, J. Nolan believes that the UNGPs themselves are of a soft law nature which makes them 'an international instrument other than treaty that contains ... standards ... of expected behaviour' (p. 139). According to her, despite their soft nature, UNGPs still have a high potential to 'result in incremental change' (p. 140). 'Soft law', she says, does not 'necessarily [mean] soft results' (p. 140). Moreover, she notes that the choice of a soft law instrument for the regulation of business and human rights issues is not a coincidence but rather an overall trend which is characteristic for this sector and is embodied in cooperation between public and private sector. The difference between hard and soft law is in intention to create legally binding obligations. While hard law creates these obligations, soft law often takes a form of principles or guidelines which are not legally binding per se. However, they do have force due to the consent achieved between companies. For instance, many of the above mentioned multi-stakeholder initiatives have force for those companies that work within the regulated sector 'by the degree of consensus and acceptance linked to them' (p. 144). Nolan notes that the usage of soft law mechanisms for business and human rights issues marks the 'networked governance' in this sphere which covers the scrutiny of previously mentioned initiatives, NGOs, users and other stakeholders. Within this framework, formed around soft law instrument, the role of the state as a policeman fades and a strong emphasis on market's regulatory role is being established. Moreover, companies might have a motivation to comply in order to avoid the endorsement of harsher regulations. Indeed, the soft law can be more powerful if it prerequisites the hard law or supplements it. On the one hand, the possibility of UNGPs' norms implementation into the national legislation might trigger more incentives amongst businesses to comply with them voluntary, on the other hand, there is no hope for a creation of any legally binding international mechanism in the nearest future. Presumably, this is why the number of companies that do not comply fully with UNGPs remains high. However, the UNGPs definitely have more binding nature than other international initiatives on social sustainability due to the context in which they were endorsed, namely, the role of the UN Human Rights Council and UN

Commission on Human Rights (now Council). Consequently, in order to achieve 'bindingness' of the responsibility to respect, a mixture of soft and hard law approaches is required.

Hence, in a situation of hard law shortage, there should be some additional incentives that could explain why companies should or eventually will implement the UNGPs framework in their activities apart from the somewhat abstract social license to operate concept. Despite the fact that the whole Protect, Respect and Remedy Framework is aimed at protection of individuals, Ruggie used an economic language for the second pillar stressing the economic and reputational damage that the human rights violations could bring to the company. Indeed, infringements of users data privacy might result in significant material damage to the company. According to Ponemon Institute's research in 2010, each data privacy breach costs a company around US$3,425,381 (Human RIghts and Business Dilemmas Forum, n. d.). Moreover, the Institute concluded that the these costs keep on rising. Adding to that, case law illustrates a changing understanding of data compensation in favour of users. The connection of human rights infringements and reputational is obvious too. Moreover, a company can gain reputational bonus for its leading role in business and human rights sphere (for instance, Microsoft made such an attempt in 2010s). Another Ponemon Institute's questioner, most of the users care for the company's reputation on data privacy protection. Businesses might also face operational risks in case of failure to respect human rights (employees might choose another, more trustworthy employer). For instance, about 10 Google employees quitted their posts as a protest against cooperation with the US military forces (Business and Human Rights Resource Centre, 2018). Other risks include investors' law suits for share prices drops flowing from data privacy breaches (which has recently happened to Facebook due to the Cambridge Analytica case) (Advocates for International Development, 2018). Apart from that, as outlined above, different national legal regimes on data protection might have contradicting approaches. Thus, in order to avoid risks connected to these issues, companies should adhere to international standards. In general, in the context of dubious legal nature of the UNGPs and lack of its enforcement on international level, economic incentives might turn out to be the most promising (Kuner et al., 2013, p. 65).

§2 Big Data: Business and Human Rights Issues

In 2010 a documentary called 'Erasing David' was released by a British moviemaker David Bond. Questioning 'what could other people do with my data?', David tried to disappear so that none could find him. However, already in 18 days a team of private detectives managed to track him having just David's full name as a starting point (Garton Ash, 2017, p. 311) . Living in the digital era, we do not only consciously entrust our personal information but also unwillingly give it to data governing companies and unknowingly leave 'the data breadcrumbs' such as

metadata behind us. These immense amounts of data, often uncontrollably aggregated and managed by companies while not directly targeted by personal data protection legislation, are called 'Big Data'. It is sometimes perceived that benefits that big data brings to society outweighs its potential harms (Ying and Grandison, 2016, p. 86). Moreover, the sphere of Big Data appears to be so obscure and spanless, that its full regulation seems barely possible. However, despite invisibility of Big Data collection and processing, the potential human rights impact can hardly be overestimated. Big Data Analytics (BDA) that set basis for automated decision making might lead to 'rational discrimination' (Baruh and Popescu, 2015, p. 584) and build assumptions about 'certain strands of people' (McDermott, 2017, p. 5). For instance, COMPAS data analytics based programme, created by the US government in order to detect re-offenders, falsely flagged black people as twice more likely to commit crime again (Fenech, 2018). The most relevant human right issue in a Big Data context is right to privacy. Poor anonymisation techniques can lead to re-identification of a data subject which might not only affect his or her privacy but also endanger physical security in some cases. Moreover, a potential data breach might lead to self-censorship and hence to restriction of freedom of speech. Consequently, the question is, what are the human rights obligations of ICT companies in the context of Big Data governance and how different they should be from obligations concerning processing of personal data.

Before proceeding to the above mentioned question, it is important to outline what is understood by the notion of Big Data. This does not appear to be easy due to the numerous complementary and contradicting interpretations of this term. Indeed, the mere existence of these interpretations confirm the sophisticated and multilayered nature of Big Data. According to Forbes journalist Gil Press, there are at least 12 variations of Big Data definition (Press, 2014). In 2001 the META Group published a report that set commonly accepted features of Big Data which was later called '3 Vs', namely, immense volume of data collected, variety of data modalities (audio, images etc.) and forms of organisation (structured or not structured) and high velocity of data real-life streaming (Ying and Grandison, 2016, p. 87). Later, other 'Vs' were added to the already mentioned ones, such as 'value', 'veracity' etc. Other academics add 'rational nature' and 'potentially exhaustive scope' to this list (McDermott, 2017, p. 4). According to McKensey Global Institute, Big Data consists of datasets that have such an immense volume that their capture, storage, management and analysis go beyond capabilities of a 'typical database software' (Angelopoulos et al., 2016). As Ira Rubinstein puts it, Big Data is 'data mining on steroids' (2013, p. 76). Obviously, these datasets are not collected for no reason. The true value of Big Data lays in an 'implicit, previously unknown and potentially useful information' that can be extracted from it (Rubinstein, 2013, p. 76). Despite many academics put the knowledge

discovery element within the definition of Big Data per se, we would prefer to place this feature under the ambit of 'Big Data Analytics' notion.

Not only possible implications of Big Data for human rights are apparent but so is its difference from personal data and principles of its protection. As noted in the first paragraph, personal data is commonly defined as information related to identifiable subject. Big Data, on the other hand, consists of three types of attributes, namely, sensitive metadata that effectively identifies an individual, quasi-identifiers that can reveal identity if taken together with additional information and benign data which is perceived to be non-identifying (Ying and Grandison, 2016, p. 87). Classic principles applicable to data protection are difficult to apply in the Big Data context. Considering the fact that Big Data often collects information not only about users but also about individuals around them (sometimes, if these individuals are not even using the service that collects data), the core personal data processing principle of user's meaningful consent is hard to comply with.

Moreover, according to the above mentioned definition of Big Data Analytics, the latter is aimed at producing new knowledge. The potential outcome of the BDA is often obscure or even unpredictable. Consequently, it is barely possible to comply with a clear notice principle in the context of Big Data, as companies often do not realise the outcomes of data collection and processing. This obviously makes an additional negative contribution to the problem of meaningful consent. Data governing platforms such as Facebook manage a quasi-public information that seems to be public at a first glance (Latonero, 2018, p. 152). Despite social media profile is often publicly accessible, it does not mean that an individual automatically allows it to be used for BDA as he or she cannot predict the outcome of analytics when publishing personal information and thus cannot evaluate possible impacts. Another privacy challenging aspect of BDA are predictive analytics. In 2012 a man came to the Target shop complaining about his daughter receiving promotions on products for pregnant women. Apparently, the store collected information about items ordered by the daughter and predicted her pregnancy before anyone else did. Despite she entrusted the store with information on her purchases, she could not possibly imagine such an outcome. If informational privacy is rooted in individual's 'ability to determine flow of information' (Latonero, 2018, p. 151) about him- or herself, how can it be granted when even companies processing this information cannot predict where it is 'flowing'?

Another issue is the minimisation principle which is barely applicable to Big Data, the whole concept of which is based on data maximisation and aiming to achieve exhaustive scope. According to S. Ying and T. Grandison, the more datasets are included in BDA, the less privacy protection can be achieved (2016, p. 89). Hence, they conclude, 'there is no privacy when it

comes to Big Data' (p. 90). Despite this statement sounds somewhat overly pessimistic, the issue of immense data volume is indeed hard to tackle. Another problem flowing from it is a 'contextual integrity of personal information' (Baruh and Popescu, 2015, p. 586). Devoid of context, Big Data analytics can show erroneous patterns, such as 'correlation between the changes in the S&P 500 stock index and butter production in Bangladesh' (Angelopoulos et al., 2016, p. 10). With all this, BDA serves as a source of actionable information that can undermine individual's rights and at the same time often cannot be appealed. In order to overcome the myth of Big Data absolute objectivity, Jens-Erik Mai suggests to not interpret it from 'surveillance model' perspective which perceives Big Data to be an accurate reflection of the reality, but rather treat it through the 'capture model' prism which interprets Big Data as a 'simplified reality' changed by the mere fact of data capturing (Mai, 2016, p. 7). Consequently, all the above mentioned differences between Big Data and personal data reveal a necessity of different obligations for companies that deal with BDA.

Despite the absence of clear regulations on ICT companies obligations in the context of Big Data governance, the importance of the issue could not have been ignored by legislators. At the EU level, the recently adopted GDPR mentions right of users to appeal decisions based on automated data processing. The leading role in 'automatic processing of personal data ... in a world of Big Data', however, was taken by the Council of Europe which released Guidelines on the protection of individuals in 2017. Despite acting within the framework of modernised Convention 108, the Committee acknowledged Big Data challenges mentioned above and tried to tackle them. For instance, Guidelines suggest to interpret the notion of control above the mere individual control and consider it to be a 'multiple-impact assessment of the risks related to the use of data'. The Guidelines underline responsibilities of data processors which makes perfect sense in the context of Big Data. They also apply a broader approach to the use of data extending it over the data and privacy protection and introduce the concept of 'ethical and socially aware use of data'. Another vital requirement is preventive policy adoption and risk-assessment. These provisions fit the UNGPs framework in the context of ICT companies (the Guidelines require data controllers and processors 'to identify risks, develop appropriate measures including "by-design" and "by-default" approaches and monitor the application of these measures'). However, the Privacy, Ethical and Social Impact Assessment (PESIA) concretizes and expands the Human Rights Impact Assessment offered by UNGPs. The results of PESIA should be communicated to individuals in order to comply with consent, notice, purpose limitation and transparency principles. Controllers are also required to use diverse techniques including anonymisation in order to protect users privacy. Moreover, the Guidelines prohibit the usage of Big Data for automated decisions without proper consideration of context. In general, the Guidelines provide

quite broad recommendations on Big Data governance and acknowledge necessity of further development of their provisions in 'specific fields of application of Big Data'. However, the mere fact of bringing Big Data issues on international law agenda is quite promising.

Notwithstanding the importance of the CoE Guidelines, it is important to notice that both academics and practitioners have already been discussing and implementing the ways in which Big Data governing companies can comply with their responsibility to respect human rights. According to Michelle Chibba and Ann Cavoukian, good practices on Big Data governance should be based on consultation, cooperation and collaboration. Like in case with personal data protection, companies should endorse special commitment (for instance, Online Trust Alliance or IOT Trust Framework). Companies should ensure the security of data through the whole life-cycle of the service, application or other data processing. Interestingly, many academics point out that companies should be held accountable for Big Data governance breaches when they do not comply with their own commitments (for instance, Rubinstein 2013, p. 83; Chibba and Cavoukian, 2013, p. 3). This correlates to the US approach to data protection discussed in the first paragraph of this chapter. However, it can be explained through the absence of any uniform regulation on Big Data which one could appeal to in cases of privacy breaches.

Anonymisation stands at the core of most suggestions regarding Big Data and privacy protection. However, there are arguments concerning the best way of such anonymisation. Some researchers believe that even simple encryption (encoding information in such a way that makes it accessible only for those who have a decryption key) under the condition that the keys are stored outside of personal data service and ensured by multi-factor authentification (Rubinstein 2013, p. 83). That is why Apple iPhone privacy system is considered one of the safest. In the *FBI vs. Apple case* (2016), which eventually did not reach the final stage of the court, the company explained that the encryption key used to encode or decode all the metadata stored on iPhone is tied to a personal code that is created by user. K-anonymity is one of the first and most common techniques of datasets anonymisation. The idea behind is quite simple. In this case, sensitive information is replaced in such a way that there are at least k-1 other users that would have identical data once sensitive attributes are deleted. However, it is could be possible to re-identify individuals if some additional information is available. It is the k-anonymity model that made Ying and Grandison conclude that the very nature of Big Data is incompatible with privacy due to the numerous datasets aggregation. Despite a few developments of k-anonymity were introduced (l-diversity in which a group of sensitive data is homogenous and t-closeness which 'treats the values of an attribute distinctly by taking into account the distribution of data values for that attribute'), its apparent disadvantages caused severe criticism. Another approach is differential privacy which deals with personal data security within datasets through introducing

some distraction or noise into them. Moreover, data is obtained not directly but through a 'software guard' which re-affirms the security of data (Jain, Gyanchandani and Khare, 2016, p. 13). There are other options for data anonymisation which we will not consider in detail within this research. However, companies should choose best techniques for de-identification depending on particular context and dataset features.

Another suggestion on data privacy enhancing that has been gaining popularity in the recent years is an 'individual's empowerment' (Rubinstein 2013, p. 81). The core idea of this concept is allowing users to manage their own privacy. The user-centrality approach aims at selective data disclosure and control of purpose and duration of primary and secondary usage. In this context, companies would be held accountable for a breach of agreement between them and individuals. Tackling the problem of privacy shrinking inversely to the datasets number increase, this model suggests 'small data analytics approach' (Angelopoulos et al., 2016, p. 9). Stored on user's side, data can be analysed by companies through a simple search for relevant attributes. At the same time, users would preserve their right to opt out from data sharing. However, despite Chibba and Cavoukian's view of individual's empowerment as a 'single most effective check against privacy abuses', there is a number of difficulties concerning implementation of this approach (Chibba and Cavoukian, 2013, p. 3). First of all, it might be not clear why companies would willingly empower their users to such extent. Trying to answer this question, I. Rubinstein argues that user-centred model could allow to achieve higher quality data, enhance consumer's trust and decrease compliance costs. She suggests that this approach could be especially attractive to new players entering the market with limited access to Big Data. Nevertheless, even if we assume that companies would implement user empowerment approach, users themselves might be not incentivised enough to be responsible for their data governance. Baruh and Popescu talk about 'awareness paradox' when awareness about privacy violations causes 'virtual identity suicides' through social media profiles deletion instead of fighting to enhance privacy (Baruh and Popescu, 2015, p. 586). This blurs the signals from users about lack of privacy protection as mostly those users who are not disturbed by these violations keep on using the service. Thus, academics offer an introduction of 'adaptive privacy system' that would allow to not only customise all privacy settings based on user's general preference but would also recommend what's best (Baruh and Popescu, 2015, p. 588). This technique could help to overcome users restricted rationality, however, the implication of individual empowerment approach does not seem to happen in the nearest future.

Despite high potential that such a 'propertisation' might have for the protection of human rights in the context of Big Data governance, it might shrink positive implications flowing from the usage of open data and data transferred by companies to NGOs for human

rights protection purposes. As we established above, international law struggles to set a universally binding framework even for the 'corporate respect for human rights'. However, when it comes to Big Data, companies governing it could be the only ones capable of effectively addressing human rights issues. For instance, Amnesty International has developed a Digital Verification programme that aims at verifying digital evidence of human rights violations such as videos and posts on social media. However, it would be more productive if the companies such as Youtube, Facebook or Twitter could present BDA on that themselves. A colourful example of good practice on that matter is a dengue study which was conducted in Pakistan thanks to Telenor company's revelations on data that they operated as it was the only telecommunication company operating in rural areas where the disease was flourishing. This case is nevertheless unique as the company managed to present all relevant information in the form of actual maps without revealing any details on individuals' personalities. In case with Ebola, for instance, a more granulated dataset was required which could endanger the right to privacy. Thus, there cannot be a uniform framework for tackling situations of that kind. The options are, however, the limited release of data (on a detailed request of the researchers) or remote access through an intermediary who is responsible for preserving data privacy in such context. There are also international initiatives such as UN Global Pulse or UN Development Group that try to set obligations for companies processing or transferring Big Data in order to tackle human rights violations.

Chapter Two: Business Obligations in the Context of Access to Remedy

§1 Corporate Remediation: Business Incentives and General Requirements to Operational-Level Grievance Mechanisms

According to the UNGPs, remediation is a third pillar of the 'Protect, Respect and Remedy' framework. At the same time, this pillar flows from the first two and, consequently, is applicable to both businesses and States. Thus, remediation in the context of human rights impacts caused by business activities can be generally split in three major groups: state-based judicial remedies, state-based non-judicial remedies and non-state-based grievance mechanisms (GMs). The importance of remediation was highlighted by Working Group on Business and Human Rights not only in the context of UNGPs but also in its connection to the Sustainable Development Goals (Herbert Smith Freehills, 2017). Consequently, it is not surprising that in the recent years the importance of remediation framework development has been widely acknowledged and discussed at the UN level. The main initiatives on the matter include OHCHR Accountability and Remedy Project launched in 2014. The project is aimed at both judicial and State-based non-judicial mechanisms. As the latter include National Contact Points established in accordance with OECD Guidelines for Multinational Enterprises, OECD Watch Effective Remedy Campaign falls perfectly within these tendencies. It is apparent though, that both of these initiatives are not targeting the non-State-based mechanisms (OECD Guidelines fall under the ambit of State's international law commitments, whilst judiciary is a traditional State's internal function). Indeed, the corporate level grievance mechanisms are not explored enough and seem to not currently get enough attention from the international law. It does not, however, mean that there is no guidance or corporate obligations on that matter.

As pointed out above, the UNGPs pay special attention to corporate responsibility to remedy human rights impacts. Even those companies that adopt the best human right policies and conduct meaningful due diligence might still contribute to adverse human rights impacts. Thus, the corporate responsibility to respect cannot be fully exercised without implementation of measures that could remedy the impacts. According to the comment to Principle 25, 'the term grievance mechanism is used to indicate any routinized ... process through which grievances concerning business-related human rights abuse can be raised and remedy can be sought'. In the context of business activities company's obligations to remedy could be split in two categories, namely, obligations imposed on a company due to a binding decision of a State-based authority and those exercised by company on its own. In this Chapter we will concentrate on the latter category as the first one is eventually flowing from the State's duty to protect, whereas this research is focused on business human rights obligations originating from the corporate

responsibility to respect. Grievance mechanisms can be split into those 'administered by a business alone or with stakeholders' and by 'industry association or a multi-stakeholder group' (UNGPs, Principle 28). GMs can be established both within the company or be entrusted to the external organs. According to the UN OHCHR Interpretative Guide, companies with high-risk business activities as well as big companies should rather establish their own GMs (2012).

Due to the ongoing discussions regarding 'bindingness' of the UNGPs, analysed in the first Chapter, as well as lack of international law attention to the non-state-based grievance mechanisms, it is important to outline what other incentives, beyond purely legal, companies have to comply with the third pillar of the UNGPs. To begin with, corporate-level GMs have apparent procedural advantages. With the opportunity to directly contact the company on the human rights impact matter granted to affected stakeholders, there is no need to comply with lengthy procedures applied in courts. This allows the matter to be addressed in a prompt manner. Promptness of the operational-level GMs (OLGMs) is tightly connected to the reduced costs that the OLGMs could bring to both parties. OLGMs allow to resolve the issue internally so that the media coverage on the issue, as well as reputational damages it could bring to the company, are minimised. Considering the fact, that companies should remedy human rights impacts only if it caused or contributed to them (in case of direct linkage to company's activities, leverage mechanisms are allowed), the company is risking to be taken to the court anyway which will cause more costs. From the stakeholder's perspective, procedural costs of OLGMs appear to be lower than other grievance mechanisms too.

Another advantage of the OLGMs is their transnational reach. Yet again, in the context of multinational enterprise business activities, it could be hard to establish jurisdiction. Moreover, in accordance with some international private law provisions, customer might have a choice of the country he or she wants to sue the company in. This might not only result in confusion but also lead to stricter fines in a country where the plaintiff filed the complaint. Following company's activities, rather than jurisdictions, grievance mechanisms could be a solution to the issue of multiple jurisdictions. Surely, this is especially relevant in the context of internet companies, as the nature of internet *per se* is based on the idea of absence of borders. Moreover, as a good grievance mechanism takes into account the local peculiarities of the operational context, it enhances promptness and reduces costs even further. In any case, company's grievance mechanism does not preclude nor exclude individual's access to other remediation mechanisms.

According to the UNGPs' definition of grievances as an 'injustice evoking an individual’s or a group’s sense of entitlement', human rights concerns do not have to amount to actual violations in order to be subject to OLGMs (Commentary on Principle 23). On the

contrary, company-level grievance mechanisms aim to prevent human rights impacts from escalation and remedy them at the early stage. According to John Ruggie, grievance mechanisms might significantly contribute to company's due diligence as they point to the gaps existing in its approach to human rights which can enhance identification and prevention of human rights impacts in the future (United Nations General Assembly, 2010). Moreover, multi-stakeholder initiatives discussed in the first Chapter often require companies which commit to them to report on the grievance mechanisms performance. These reports should include, for instance, information on how many complaints regarding alleged human rights impacts were communicated to the OLGM, how many of them were resolved etc. Thus, reporting not only on quantitative but also on qualitative indicators of grievance mechanisms performance could amount to the industry sector standard due to the special attention of multi-stakeholder initiatives. These initiatives might serve as a stronger framework for corporate human rights protection, provide a platform for company's empowerment in the context of leverage required by the UNGPs, contribute to mutual progress and monitoring while taking into consideration distinctive features of a particular sector and its operational context.

Despite the fact that we have mentioned above some initiatives dedicated to the development of the State-based grievance mechanisms at the international law level, it does not mean that all the states are ready, willing and able to fulfil their responsibility to protect human rights in the context of business activities. In countries where human rights are under threat, big companies should bare moral duty to provide remediation for the impacts they caused. Thus, foreseeing instruments for remediation does not appear to be damaging for company's reputation as incapable of not contributing to adverse impacts. On the contrary, that contributes to the positive image of the company as it cares for its activities' stakeholders. Consequently, all the incentives we described above and all the advantages of OLGMs implementation prove it to be a valuable decision for any company in the ICT sector not only from legal perspective but also from reputational, financial, ethical and other points of view.

However, we are not trying to claim that there are no legal requirements to the way OLGMs should be constructed at all. The UN Guiding Principles established eight criteria applicable to good and effective grievance mechanisms without which it is barely possible to fulfil the corporate responsibility to respect to its maximum. While discussing these requirements we will also analyse discussions that preceded their adoption in order to better understand their meaning. The first feature of a good OLGM is legitimacy. Whilst the core idea of a mechanism as a fair one was preserved in UNGPs, initially, Ruggie meant it to be a separate and independent body organised by company which could not be interfered with while exercising the grievance process. However, during discussions it got clear that this could become a problem for small and

medium enterprises as they might not have facilities to establish such a body independently from company's management. Thus, the final version of this requirement is rather a 'perceived legitimacy' which means that the OLGM should 'enable trust'.

Another feature is accessibility which initially required the mechanism to be publicised. However, discussions revealed a significant difference exists between 'being known' and 'being publicised'. Often people do not care for such mechanisms unless they find themselves in a situations when they are needed. Consequently, the final version requires the information to be known to all the stakeholders it is intended to at the moment when it is needed. Moreover, companies should assist those who face obstacles with assessing this information. Tightly connected with 'to be known' requirement, next feature listed by UNGPs is predictability. Despite the fact OLGMs have a more flexible procedure than the courts do, for instance, it should still be clear and known as well as its types, outcomes and means of monitoring. It can be acceptable to provide information on indicative time frame to achieve the balance between flexibility and formalism. It is also recommended to obtain a feedback from stakeholders on that matter. Apart from that, parties should have 'reasonable access to sources of information, advised expertise for fair information and respectful terms' (Rees, p.9). Surely, companies do not always have a power to ensure that, however, they should do everything to make it a 'reasonable access'. Thus, the OLGMs should be equitable.

Another requirement is transparency, both regarding the process to aggravated individual and the performance of the grievance mechanism for wider groups of stakeholders, which contributes to the confidence in its effectiveness (how the mechanism is actually working), unlike predictability which provides just general information on how the mechanism should work. Another crucial requirement for the effective OLGM is its right-compatibility which requires the outcomes and remedies to be in accordance with the international human rights law. Grievance mechanism is also required to be a source of continuous learning, which was not initially proposed by the Special Representative but was suggested by the Corporate Social Responsibility initiative. This feature requires companies to improve the grievance mechanisms and use them to identify issues that could be prevented in the future. This correlates with what was pointed out above, namely, that OLGMs contribute to company's human rights due diligence. The final feature recommended purely for the operational-level mechanisms is that they should be based on engagement and dialogue. On the one hand, this means that stakeholders should be consulted when grievance mechanisms are on stage of design. On the other hand, it also means that dialogue should be used as means to address the issues. In general, remediation should not be a unilateral process exercised by company only but should rather be a suggestion which can be disagreed upon and discussed with the complainant.

§2 ICT Sector Grievance Mechanisms Case Study

The requirements towards operation-level grievance mechanisms, outlined in the first paragraph of this chapter, are universally applicable to all the sectors of business activity. However, it is acknowledged that these provisions need sector-specific approach (UN Working Group on Business and Human Rights, 2017). Indeed, the ICT sector has a number of distinctive features that require specific application guidance. At the same time, personal data leakages and data misuse by ICT companies became a new reality which makes the issue of remediation even more relevant in this sphere. Nevertheless, according to the Ranking Digital Rights initiative, 'at present, grievance and remedy mechanisms [ICT] companies offer are totally inadequate to match the enormous influence these platforms wield' (2017). Moreover, the multi-stakeholder initiatives existing in ICT sector do not provide for effective grievance mechanisms. A number of ICT companies participating at the UN Reporting Framework mentioned internal grievance mechanisms for their employees as well as channels for customers to complain about privacy issues caused by other users and third parties. However, none of these companies reported on grievance mechanisms for customers who discovered a misuse of their data by company itself. At the same time, as we discovered above, companies are supposed to primarily remedy the impacts they caused or contributed to, whereas impacts that are directly linked to company's activities are covered by obligation to use leverage. Thus, the idea of the company-level grievance mechanisms in the data governance context is remediation for company's failure to protect data privacy or misuse of data collected. Whereas the attention was drawn to the content regulation by companies online and freedom of expression consequences of such regulation, OLGMs for privacy issues are not covered as much.

The reason for the lack of practice on OLGMs for communicating privacy impacts caused by business activities to users of ICT services lays in the very nature of such impacts. The main problem flowing from data gathering by ICT companies on massive scale is unawareness of data subjects. OLGMs can only be applied by a company that acknowledges impacts it causes. However, if even the mere fact of data collection and processing might not be visible, how can the company acknowledge privacy impacts and provide remedy for it? This is directly linked to the issue of informed consent, discussed in the previous chapter, which is now getting closer attention at the European level of regulation. Moreover, the mere absence of information about violations of data privacy already constitute the violation of the company's obligation to remedy. The roots of the problem lay in company's incentives to provide users with information on data collection as ICT sector's revenue is significantly enhanced by selling users data (Seth, 2018). Consequently, the more cases like Cambridge Analytica are brought before courts and result in

significant losses for ICT companies, the more incentives these companies will have to create OLGMs for privacy breach complaints. That is why the enforcement of all the legislation initiatives, discussed in the first chapter, at UN, CoE and EU levels are crucial for creating a framework in which companies would feel they could benefit from OLGMs even more. For instance, the US courts do not only award compensation to plaintiffs but also to all the users that could be potentially impacted by data privacy violation committed. Surely, that could significantly increase company's appreciation of grievance mechanisms.

In the last decade a number of data leakages and privacy breaches happened in data governing companies from various sectors (Armerding, 2018). However, most of these cases we know about due to the scope of these violations which did not allow to suppress the media coverage and litigation. The distinctive feature of ICT sector, as already mentioned, lays in 'invisibility' of data gathering and processing. We have now discussed models of individual empowerment that would allow users to track and manage their personal data gathering and usage by companies which are only at the beginning of their development (see Chapter I, §2). However, we have also discovered the new provision of GDPR, according to which, users have a right to get information from a company about all the data that was collected about them. Apart from that, there are certain indicators that might signalise to an average user that his or her data privacy might have been breached by the company. Hence, the question is, what are the possible mechanisms currently available to customers whose data privacy was allegedly breached.

In order to address this issue from the perspective of an illustrative example, my decided to conduct a simple experiment. Recently, a friend of mine had a conversation with his colleague about safari in Kenya. He had never seriously thought about this type of vacation, all the more so, he had never browsed anything on that topic before the conversation happened. However, while checking his Instagram few hours later, he noticed an advertisement suggesting a safari trip in Kenya. As a probability of coincidence was quite low, he thought immediately that the Instagram app installed on his Samsung phone was listening to the conversation while in background mode. The question that any user would ask in a situation like this is 'What do I do now?'. As we discovered earlier, deleting the app or committing 'virtual reality suicide' would not be the best option both from the perspective of the 'awareness paradox' negative impacts and from my friend's social life perspective. So what should he do then? The most apparent move would be to report an alleged privacy breach to Instagram. However, Instagram privacy and security division of the help center offers a closed list of issues available for reporting. Despite personal information misuse by other customers is extensively covered by offered options, the issue my friend faced was not the one on the list. The Samsung help center, which we contacted on behalf of my friend asking if Samsung settings might allow apps to bug their users, suggested

to contact Instagram on that matter (which, as we found out, is somewhat problematic). Whom should I contact next? The App Store? The software provider? In a situation with many parties involved, it might seem easier to sue Instagram. However, like any other average customer, my friend cannot even be sure that bugging his phone through the app in a background regime is possible. Considering the costs of court proceedings he might face, he would either keep using the app and try to not discuss sensitive issues next to his phone or he might choose an 'awareness paradox' behavioral model. However, would that not be much easier if the app provided a channel for such complaints? If we assume that my friend chooses to go to the court, regardless of how certain he is his privacy was breached, what reputational damage would it bring to Instagram due to the media coverage regardless of the case outcome? More importantly, this entire example reveals how disproportionate the balance of power can be regarding the individual's rights protection against company's impacts on data privacy.

The case of Cambridge Analytica which was mentioned multiple times in this research shows how damaging the failure of company to effectively remedy data privacy breach could be. Instead of informing users about Cambridge Analytica's misuse of personal data obtained from 87 million users without their consent, Facebook preferred to keep that as a secret, once it was informed that this data was deleted. Only after it was revealed that data was still used for targeted advertisement for political purposes, the case got extensively covered in media and led to Zuckerberg testifying before US Congress and European Parliament. Eventually, the costs brought by the incident to the company amounted to at least $60 billion (The Quint, 2018). After this, Facebook launched a 'Data Abuse Bounty' campaign to award anyone who reports any misuse of data by the app developers (Greene, 2018). That is how Inti De Ceukelaire reported that data of more than 120 million monthly users was illegitimately collected and misused by the service Nametests.com which provided various tests of a 'what would you look like if you were an Arab princess?' type, for which he was awarded $ 8000 (Inti De Ceukelaire, 2018). Clearly, this example, together with understanding of the importance of corporate responsibility to respect human rights in general, should incentivise companies like Facebook to create similar channels where abuses or impacts can be reported. Another positive example is a hotline 'Tell Us' created by Siemens. Unlike Instagram's reporting system, 'Tell us' does not have a closed list of issues that can be communicated on and encourages users to report any misuse of their data (Access, 2015).

Chapter Three: Balancing out Business Obligations and State's Duty to Protect

§1 Criteria for Legitimate State Surveillance

Numerous threats of the modern world make it challenging for states to exercise their duty to protect citizens against human rights abuses. At the same time, according to international law, states are not only responsible for investigation of crimes and remediation of human rights abuses, but also for prevention of such crimes. A core obligation of states, duty to protect flows from legal philosophers' picture of social contract as a source of state's sovereignty and the consent of governed as an inalienable part of it. However, technological development brought a new dimension into the rhetoric of state sovereignty, namely, the cyberspace sovereignty. Whereas the limits of 'consent of networked' (MacKinnon, 2012) given to ICT companies by their users are still under discussion, states do not differentiate citizens identities online and in real life when exercising duty to protect. However, there is a difference indeed.

The practice of communications tracking was established after the World War II (Sumner, 2016). In *Taylor-Sabori v. the United Kingdom* case (No. 47114/99, 2002), the ECtHR ruled that the UK did not fulfil the criteria of legality, required for communications interception, as there was no clear legislation on pager messages interception. Sixteen years after, when communication technologies went way beyond pager in all senses possible, including the extent of data governed, states fail to fulfil this criteria even more so. However, as Sir John Sawers, former head of MI6, noted, 'security and privacy are not a trade-off, but go together' (Watney, 2015, p.369). After the WikiLeaks revelations caused an explosion of public discussions, it seems clear that state surveillance needs more regulation. In the current reality, in order to effectively prevent crimes, states need to access data entrusted to an ICT company by its users. When national security or crime prevention is at stake, companies have to obey state's requirements to retain data about suspected users. However, it is not always this type of issues that states are guided by when requesting data on their citizens. While we agree that state surveillance might be necessary for protection of democratic values, the process and reasons for conducting it must be regulated in accordance with international law. Hence, in order to understand ICT companies obligations in context of illegitimate state surveillance, it is necessary to outline what is understood by the legitimate surveillance.

Unlike UDHR and ICCPR, the ECHR outlines exceptions from the right to respect for private and family life (Article 8) in the context of public authorities activities:

> *'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the*

country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

However, even the ECtHR's Guide on Article 8 acknowledges the 'succinct' nature of legitimate aims listed above (ECtHR, 2017, p. 10). The Court practice evaluates interception cases individually through interpretation of state's reasoning for surveillance as compatible or not compatible with the legitimate aims. This approach does not contribute to legal certainty and predictability. After Julian Assange proved the world that this uncertainty gives a leeway for bulk surveillance, a number of discussions were held at the UN and European levels in order to identify basic requirements towards state surveillance with greater degree of precision. As Privacy International (PI) encompassed all these discussions in a handy Guide on International Law and Surveillance (2017), we will list the core principles of legitimate state surveillance named by it together with some illustrations from case law.

The first principle is the principle of legality. This does not only mean that state surveillance measures should be foreseen by domestic law, but also requires this law to be compatible with international human rights obligations of states (UNGA, 2014). National law should be consistent with the rule of law and should include assurances against arbitrary interference (*Taylor-Sabori v. The United Kingdom*, No. 47114/99, 2002). Legality also includes accessibility requirement, as according to the OHCHR, secret rules and interpretations do not amount to law as they lack its quality of publicity (OHCHR, 2014). This requirement is dictated by the level of discretion that public authorities possess when exercising surveillance. According to the ECtHR, 'minimum protection flows from certainty' (*Malone v. The United Kingdom*, . No. 8691/79, 1984). Hence, accessible legislation on interception should outline the scope and manner in which the discretion should be exercised. Another requirement flowing from the principle of legality, according to PI, is foreseeability. The law should be precise on interception procedure, its time limits as well as include safeguards and be public (Human Rights Committee [HRC], 2015). Surely, that would be a mistake to assume that foreseeability implies notification of users when their social network communications are intercepted as it would frustrate the aim of surveillance (*Weber and Saravia v. Germany*, No. 54934/00, 2006). However, information on procedure of interception should be clear.

The second principle is necessity. It is the state's responsibility to not only prove that surveillance measures are useful, reasonable and desirable to achieve the legitimate aim, but also demonstrate 'in specific and individualised fashion the precise nature of the threat' and 'direct and immediate connection between the expression and the threat' (*John Doe (Kidane) v. The Federal Democratic Republic of Ethiopia*, No. 16-7081, paras. 14-15). Hence, only necessary interception can be considered non-arbitrary as it has reasons and proportionality behind it. As

quoted above, surveillance should be necessary in a democratic society. The ECtHR splits such necessity in two levels, namely, general consideration of necessity, when surveillance would have a strict necessity in any democratic society for protection of democratic values, and particular consideration, when these measures are absolutely necessary for a particular case (*Weber and Saravia v. Germany*, No. 54934/00, 2006). The third principle tightly connected with the necessity is proportionality. States should always give preference to the 'least intrusive measures' that would still allow to achieve the objective of interception (Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 2014).

The fourth principle of a legitimate state surveillance is a principle of adequate safeguards. The core idea is that the nature of state surveillance presumes secrecy of interception up to the point when it is stopped. Hence, the legislator should make sure that enhanced safeguards are in place. States are obliged to ensure that personal information is not obtained by parties which are not authorised to do so in accordance with international standards (U.N. Human Rights, 1988). That also includes states by themselves. When taking measures against illegitimate privacy interferences, states should set a minimum standard against abuses through defining the nature of offences that allow interception, limit of duration for such interception, precautions when transferring obtained information to other parties etc. in domestic law (U.N. Human Rights, 1988). When surveillance is over, an individual should be notified about the interception conducted against him so that he can appeal the procedure of interception or it necessity, proportionality etc. (*Roman Zakharov v. Russia*, No. 47143/06, 2015). Adequate safeguards principle includes the requirement of reasonable suspicion affirmed by a warrant. It also includes the presence of an effective oversight like 'prior authorisation, subsequent review, judicial involvement and overall overview of the surveillance system' (Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 2014). Other requirements that PI included into their guide in the context of adequate safeguards are such as data retention safeguards, transparency and safeguards in intelligence sharing and data transfers. Finally, state surveillance mechanisms should be balanced out with the access to remedy principle.

Technological developments of the twenty-first century enhanced states' ability to conduct mass surveillance which basically implies interception of a number of people without clear reasons to suspect each of individuals. We have now seen that most of the principles of legitimate state surveillance are not compatible with the blank interception. As European Court of Human Rights put it, such surveillance is not based on factual indicators that prove an intercepted person to be connected to a wrongful act (*Klass and Others v. Germany*, App. No.

5029/71, 1978). Hence, mass surveillance is generally forbidden, however, it does not mean it does not exist in some states. However, mass surveillance is not feasible in the modern world without retention of users data from ICT companies. 'Dataveillance' exercised by companies on request of a state enhances their responsibility to ensure such surveillance is legal. As mass surveillance and storage of personal data 'just in case' cannot be considered legitimate, both states and companies facilitating it should be held accountable. In case of Zakharov vs Russian Federation the claimant discovered that all the major Russian telephone companies SIM-cards were equipped to intercept communications by FSB (Russian intelligence service). The ECtHR held that even though Zakharov failed to prove his communications were intercepted, the mere possibility of such interception entitled him to get remediation. Interestingly, the same approach was taken by the US Supreme Court regarding Facebook when it discovered company's data surveillance practices which were not foreseen by its Terms of Service. Not only plaintiffs but all the users who wished to bring a claim were considered by court to be entitled to get remediation. The difference is, however, the purpose of the dataveillance. Whereas in case of Facebook company used data for commercial purposes and was thus legally responsible for it, in Zakharov's case telephone companies were complying with domestic law and could not be held accountable by it. That is why the corporate responsibility to respect human rights needs more definition in high-risk states operational contexts.

To sum up, it is important to notice that whereas mass surveillance requests from governments should be clearly unacceptable for companies, most of the principles for legitimate state surveillance in cases other than blank interception require case-by-case evaluation. Considering the fact that countries have a margin of appreciation regarding measures they implement for national security protection, it is even more complicated for companies to identify if requirements are met. According to Watt, creating an international treaty in cyberspace context could be a solution for this issue (2017). However, she also notes that it is barely feasible considering the fact that many countries are reluctant to subject the state surveillance to the international law regime. As we know, countries which perpetrate the most, are least inclined to international cooperation. At the same time, the UN level discussions mostly have a 'soft' nature and thus do not create direct obligations for states. However, international law can still ensure some parts of legitimate surveillance (for instance, bilateral treaties like US - EU safe harbour agreement which was replaced by the Privacy Shield Agreement ensure the requirement of safeguards for transferring information to the third parties). Nonetheless, the current state of international law in the context of state surveillance does not provide clear procedure on the way it should be done to be considered legitimate, nor it provides detailed guidelines for companies in cases of conflict between domestic law and international human rights law. However, if a

company enters market of a state where human rights are at high risk, these risks should be carefully assessed by it. That is when the importance of due diligence and data privacy impact assessment gets contextual implication. Moreover, policy commitments to sector-specific initiatives could provide mutual empowerment and experience sharing among companies.

§2 Case Study: Sharing Data with a Government in the Name of National Security. Digitally Facilitated Repressions

Nowadays a significant number of big multinational enterprises conduct their business globally. Despite the fact that the UNGPs claim corporate human rights obligations universal, one cannot deny that operational context might have significant impact on the extent and actual feasibility of these obligations' implementation. Indeed, whereas some countries provide a friendly regulatory framework towards the exercise of business obligations, others seem to be quite opposite of that. According to the Principle 23 of the UNGPs, companies should 'comply with all applicable laws and respect internationally recognised human rights, wherever they operate' as well as 'seek ways to honour the principles of internationally recognised human rights when faced with conflicting requirements'. In essence, the Guiding Principle require companies to 'seek ways' to adhere to international human rights law even if state's legislation contradicts it. Even though this logic seems to be most favourable, in reality a number of issues arise. We have already discussed implementation problems that the UNGPs framework faces in countries with relatively high level of human rights protection. Surely, these problems intensify and overflow with new issues in states which do not provide their citizens with effective tools to appeal government's decisions. Nevertheless, companies that chose to operate in high-risk states are not exempted from responsibility to respect human rights. According to the OHCHR, companies should take the risk of involvement into human right abuses 'as a matter of legal compliance, irrespective of the status of the law where the business activity is taking place' (2012, p.80). Now, when we identified what should be considered as a lawful state surveillance, the question is, what ICT companies do (if even they do anything at all) in order to adhere to data privacy international standards in countries, where privacy is under threat due to unlawful state surveillance.

The first country to be looked at is the United States. Despite the fact that the US are a democratic state, the surveillance practices adopted by it were heavily criticised for the lack of control and clarity. Given that the core of the criticism was government's abuse of authority in the name of security, the case of the US mass surveillance scandal might illustrate the way companies might exercise their leverage in order to change legislator's approach to national security protection in an operational context of democratic society. After the unspeakable

tragedy of 9/11 the US announced a 'war on terror'. The consequences of this included the attempt to expand the imminent threat concept to defend the pre-emptive use of force by the US, denial to terrorists in enjoyment of rights as prisoners of war declared by President Bush and adoption of the Patriot Act which allowed FBI to obtain any information without a court order. Dictated by outrageous terrorist attack, these measures established, as Ash calls it, an emergency state that never ends (2017).

The Electronic Communications Privacy Act (ECPA) adopted in 1986 came in quite handy for the achievement of the purposes of war on terror as it allowed enforcement authorities to collect e-mails and other data from companies without a warrant. Surely, such procedure is not compatible with the principles of a legitimate state surveillance outlined above. Moreover, the Foreign Intelligence Surveillance Act (FISA) Amendments Act (2008) gave protection to the ICT companies against customers lawsuits in cases when users privacy was violated due to the legal request from the government. However, we have already shown that ICT companies have incentives to protect their users privacy apart from legal grounds only. That is why a number of ICT companies like Microsoft, Google, Facebook and others united for a Digital Due Process initiative, the purpose of which was to change the outdated ECPA and introduce court warrant to the process of data retention by authorities. In 2011 the initiative success was marked with amendments it required. However, WikiLeaks revelations discovered the extent of mass surveillance, conducted by the US and National Security Agency (NSA) in particular, as well as ICT companies involvement into it, which led to further initiatives that required to establish a legitimate process of state surveillance. In 2013 an initiative of eight ICT companies including Apple, AOL, Facebook, LinkedIn, Twitter, Yahoo and Microsoft was established. Its aim was to urge governments to change their surveillance practices towards more legitimacy. ICT companies drew attention of US Committee on the Judiciary to necessity of accountability and oversight strengthening for the US surveillance practices. Eventually, the USA Freedom Act was passed by the Senate in 2015 which ended bulk collection of phone calls metadata while preserving the right of the government to mandatory retain this metadata from companies on case-by-case basis under Foreign Intelligence Surveillance Court supervision. Surely, there are still equations on the legitimacy of the US state surveillance practices and their exceptionalism approach. However, the example of the US shows that ICT companies might have significant leverage on the government surveillance policy. Nonetheless, as already mentioned, the US is a democratic state which significantly enhances the chances of ICT sector leverage success.

The example of China could provide a colourful illustration to the way state surveillance works in states where national security is interpreted so broad that it includes any kind of dissent from the official agenda. Chinese system of surveillance, according to

MacKinnon, works at two levels (2012). The outer level is represented by what is called the great Chinese firewall, which filters any politically sensitive websites coming from outside of the country. The inner layer is built on domestic companies which are obliged to comply with oppressive national legislation or endure sanction otherwise. Endangering state security has been serving as an official reasoning for imprisonment of political, ethnical and religious dissidents. Surely, such an interpretation of national security does not correlate with the principles of legitimate state surveillance. However, agreeing to the national legislation requirements is the only way for a company to overcome the Chinese firewall. For instance, when entering Chinese market in 2000-s, Google had to agree to censor its search engine Coogle.cn. Nevertheless, in 2010 Google had to stop providing search engine service in China due to a number of cyber attacks on Gmail accounts (the company did not completely leave the market though as it is still providing other services).

MacKinnon notes that the obscurity of relations between state and private sector in surveillance is a key component of China's networked authoritarianism. How can an ICT company act in compliance with human rights in an operational context like China's? In 2004 Chinese authorities requested information on a political activist who had a Yahoo China account. Without a warrant, Yahoo transferred personal data to the government which used information from the account to imprison its owner for 10 years for purely political reasons. The question arises then if it would not be better to quit the market, governed by the oppressive regime. Despite only 1 per cent of the hole Chinese population knows how to use Virtual Private Network (VPN) and other tools to bypass the firewall, services like Facebook and Twitter became a platform for Chinese political activism. MacKinnon illustrated the power of foreign ICT companies in China by the case of a blogger Guo, who managed to post on Twitter about his arrest by authorities asking for help. This tweet caused such a significant reaction that Guo was eventually released. Even complying with censorship requirements, foreign companies like Google and Microsoft 'have provided Chinese netizens with much freedom of information over these years' (MacKinnon, 2012, p.138). At the same time, a company like Yahoo 'which gives up information is unforgivable' (MacKinnon, 2012, p. 138). Consequently, one can argue that ICT companies should stay in a country with high-risk of human rights abuses unless it can maintain the 'red lines' of surveillance that it vowed not to cross in order to not betray the trust of its users and to not contribute directly to digitally facilitated repressions. When it comes to leverage in countries like China, ICT sector is powerless. China has developed its own ICT giants like Baidu, Alibaba and Tencent, which are all listed on stock markets overseas. Foreign investors thus indirectly sponsor surveillance practices which these companies contribute to at the inner surveillance level. While it is hard to count on domestic companies to use leverage against

autocratic government, the reaction from outside the country does not seem to follow any time soon.

Another country we would like to look into is Russia. Recent developments in Russian legislation, which entered into force this July, require Web-based companies, telecommunication operators and internet providers to store data of Russian citizens on the territory of Russia. The types of data that are required to be stored are such as text messages, voice information (including calls), images, sounds, videos and other electronic messages all of which should be kept by companies for around six months. In essence, this legislation targets prevention and detection of terrorism and extremism. However, despite the fact that this agenda reminds the one of the US, there are significantly more concerns when it comes to Russia. There are a few reasons for that, namely, the lack of opportunities for the ICT companies to use leverage to change official agenda, FSB (Russian intelligence service) abuse of authority and its power to obtain information without warrant and the use of this information not only against extremists but also against political opposition. Examples of opposition leaders' (for instance, Navalny and Khodorkovsky) website blockages prove government's attempts to expand its power to the digital sphere. Inspired by opposition through services like YouTube and Facebook, recent protests against official agenda led to hundreds of people arrested. Thus, recent regulation on 'undesired organisations' which call to participation in protests, unauthorised by state, was adopted. In this context, cases of data transfers by ICT companies to FSB could have serious consequences for users. MacKinnon provides an example of Yandex (biggest Russian search engine and browsing service with Yandex.wallet and other branches) which confirmed that it transferred financial data of users who contributed money to Navalny's fund to the authorities without any proper warrant even. Now, when regulation obliges companies to provide the abovementioned data, illegitimate state surveillance and data privacy breaches might significantly increase in scale. However, as already mentioned, ICT companies currently serve as a platform for opposition in Russia which makes it quite important for companies to look for the ways to protect privacy as much as it is possible in this operational context. That could be extremely challenging as companies like LinkedIn and Telegram which refused to comply with the new regulation were already banned from Russia.

To sum up, despite the fact it could be quite challenging for the ICT companies to comply with international human rights law in operational contexts like those of Russia, China and even the US, they should use all the leverage they have to contribute to positive changes as well as do their best to minimise their contribution to the human rights abuses. Companies should be obliged to act responsibly in high-risk countries for one simple reason: they willingly made a decision to enter a problematic market, seeking for profit. Thus, this decision should also

include considering the human rights aspect of the issue. While Zuckerberg's radical transparency approach, which requires people to be as open to each other as possible, might work in states like US, in other countries sudden change of privacy settings without proper notice could endanger physical security of users whose information was exposed. Despite the fact that there are no clear directions on how to strike the balance between human rights and oppressive national legislation, companies might still be interested to do their best to avoid financial, reputational and other types of damages that their involvement into human rights violations could bring once it is exposed to the international community. The decision to leave the market is not a silver bullet too as it could cause significant damage to the citizens in countries where ICT companies provide a platform for opposition.

Conclusion

One of Zuckerberg's favourite books is the one of Peter Huber called Orwell's Revenge, which criticises the novel '1984'. The overarching idea of this book is 'Orwell was wrong'. Indeed, author's vision of future does not fully correlate with reality we exist in. The core difference is that whereas novel's scene takes place in a state where all the technologies are controlled by government, data governance in the modern world is built by ICT companies or, as Garton Ash calls them, 'Big Cats'. We are now entering a new era when data governing companies are not only looked after by states and international community in order to punish them for human rights violations, but are also awarded with human rights obligations, namely, responsibility to respect them. While conversion has not fully happened, however, states and inter-governmental organisations should create an enforcement framework for implementation of corporate obligations to protect data privacy.

The UN level of data privacy is formed by the political controversies of the twentieth century, which caused its inclusion under the ambit of the right to privacy, rooted in its strong legal protection by the Bill of Human Rights. However, the broad definition of right to privacy did not allow to create clear implications of the data protection obligations of states including corporate obligations in the context of business activities which should be ensured by them. Moreover, the 1990 UN Guidelines for the Regulation of Computerized Data Files failed to compensate this gap. Despite remaining emphasis on data privacy existence within the right to privacy, now in digital age, the personal data issues entered qualitatively new era within UN framework. Initially brought up within state surveillance revelations context, United Nations soft law has been paying a special attention to the role of businesses in data governance as well as companies responsibilities on that matter, facilitated by the UNGPs provisions.

The European level of data privacy protection is represented by slightly different approaches. The European Convention of Human Rights and case law of the ECtHR interprets data protection as a part of the right to respect for private and family life. This can be considered to be a restrictive interpretation of the data protection, as the Court has to narrow the application of it to the limits of Article 8, even though it claims to understand personal data protection as stated in Convention 108. The Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data in its modernised version, on the other hand, acknowledges the right to protection of personal data as a separate right in its integrity with other rights. Despite its progressive nature and direction at strengthening accountability and powers of supervisory authorities, it is based on principles (f. ex. transparency, legitimate aim, consent etc.) more than it gives direct regulations on controller's obligations. Finally, the GDPR is based on

EU's approach to data protection not just as a separate but also as a fundamental right encompassed by the EU Charter of Fundamental Rights and implemented in constitutions of Member States. Aiming at unification of data protection regulations within the Union, the EU Regulation is meant to be more precise when establishing controller's obligations. Moreover, the GDPR has direct force and accountability measures directly applicable to businesses exercising controller's functions. However, despite high degree of differentiation, all these approaches are united by one common denominator; being a separate right or a part of right to privacy, data protection is seen as an element of human dignity.

Despite progressive nature that the CoE Modernised Convention and EU's GDPR brought, a transborder instrument for data privacy is needed due to existing gaps in regulations, difference in approaches and degree of protection across the globe (for instance, the US approach of consumer as an economic actor and the EU one - of data privacy as a part of human dignity). Adopted in 2011, UNGPs set a solid ground for creation of universal corporate obligations from the human rights approach. Some MNCs have already undertaken human rights policy commitments and implemented them in their business activities. ICT sector multi-stakeholder initiatives became a tool for companies' mutual empowerment and set up industry-wide standards which are applied to contractors and suppliers. despite overall requirements of the UNGPs need specification in the context of ICT companies, these initiatives together with good practices have already established some guidance on Guiding Principles implementation. For instance, it is beneficial for companies to conduct Human Rights Impact Assessment, required by the UNGPs as a part of due diligence, on a product level, adopting privacy-by-design and privacy-by-default approaches. Due diligence should involve stakeholders and be ongoing to accompany the whole cycle of the product from its creation to closure. Integration and taking appropriate action as a part of due diligence requires companies to use leverage mechanisms in their contractual relations creatively, obtain informed consent from users and empower them with tools of control over personal information. Companies should also track the effectiveness of their due diligence and communicate performance to the stakeholder. The latter means that once user's privacy is breached, the company should notify him or her on leakage and how the problem was addressed. However, how realistic is that?

If questions arise when it comes to UNGPs framework implementation in the context of personal data governance by ICT companies, the phenomenon of Big Data brings even more challenges to it. It is not only personal data that is being collected but also metadata, 'digital breadcrumbs', that we unknowingly leave. However, this information is used for the Big Data Analytics which can lead to assumptions built about us, 'rational discrimination' effect and even serve as a basis for decisions of legal significance. While possible human rights impacts arising

from Big Data processing are apparent, there is a significant lack of regulation on corporate obligations in this context. Recent CoE Guidelines on Big Data made a significant step towards bridging this gap. Despite progressive nature if these Guidelines, they are still based on principles established by the Convention 108. The interpretation of user's control, for instance, resulted in multiple-impact assessments requirement. Despite the fact that innovations like Privacy, Ethics and Social Impact Assessment, results of which should be communicated to users, data security responsibility of controller and processor (anonymisation techniques, for instance) etc. are extremely progressive, a separate instrument for Big Data regulation is needed. The reason for that is a difference between personal data and metadata which cannot be regulated based on the same principles.

The third pillar of the UNGPs, namely, remediation, received a special attention at the UN level in the context of state-based judicial and non-judicial mechanisms. However, the corporate-level grievance mechanisms were bypassed by this attention. We argue that operational-level GMs can be more effective for the human rights violations prevention as they offer a prompt solution to impacts which have not amounted to violation yet. They also contribute to due diligence processes. Despite the fact that there are recommendations on how OLGMs should work, they are not always implemented by the ICT companies in reality. The problem is that in order to establish grievance mechanism for a human rights impact, a company should acknowledge that impact. However, when it comes to privacy breaches, information becomes available to the public only in cases of mass data leakages. Thus, it might be more convenient for companies to hush them up. That is why law enforcement in sphere of companies responsibilities is crucially important. The more cases like Cambridge Analytica will lead to significant financial and reputational damages, the more incentives companies will have to provide operational-level grievance mechanism to resolve the issues internally.

Corporate responsibility to respect human rights is especially relevant in the context of states which lack power to protect their citizens against human rights violations. However, states might also exercise excessive power while protecting its national interests (the US, for instance). Whereas national security can be guarded by state surveillance under condition of compliance with requirements to its legitimacy, some states expand the notion of national security to political oppositionists and other activists whose opinion is perceived as dissident (China and recently Russia). Despite the fact it could be quite challenging for the ICT companies to comply with international human rights law in operational contexts like those of Russia, China and even the US (or resorting to Ash's classification, 'Big Dogs' states), they should use all the leverage they have to contribute to positive changes as well as do their best to minimise their contribution to the human rights abuses. Companies should be obliged to act responsibly in high-risk countries

for one simple reason: they willingly made a decision to enter a problematic market, seeking for profit. Thus, this decision should also include considering the human rights aspect of the issue. While Zuckerberg's radical transparency approach, which requires people to be as open to each other as possible, might work in states like US, in other countries sudden change of privacy settings without proper notice could endanger physical security of users whose information was exposed. Despite the fact that there are no clear directions on how to strike the balance between human rights and oppressive national legislation, companies might still be interested to do their best to avoid financial, reputational and other types of damages that their involvement into human rights violations could bring once it is exposed to the international community. The decision to leave the market is not a silver bullet too as it could cause significant damage to the citizens in countries where ICT companies provide a platform for opposition.

In the world of Big Cats and Dogs balancing out their interests against each other, it seems like individuals have no right to say. However, the power of 'the Mouse' is more significant than it seems. Understanding what we consent to instead of skipping Terms of Services, fighting for better privacy protection, being cautious about where targeted advertisement is coming from etc. could change companies' perception of the role of users. Indeed, individual empowerment could serve as a powerful tool for data privacy protection once the problem of a 'lazy user' is overcome. The human rights approach to corporate responsibilities does not only correlate with the border-free nature of the Internet, but also puts an individual and his or her dignity in the at the core of a system. However, more initiatives from the legislator's side are need to achieve it. GDPR's provisions, according to which, individuals can request information about them from data controllers is a huge step forward but it is just the beginning.

If not about his prediction of future, then about the tremendous influence that technologies and those who master them can have without proper control on our daily life, freedom of thoughts, expression and privacy - was Orwell wrong in the end?

Bibliography

ACCESS (2015) *Siemens: Tell Us* [Online] Access. Available from: http://accessfacility.org/siemens [Accessed 10/07/18].

ANGELOPOULOS, S. et al. (2016) Small fish in a big pond: an architectural approach to users privacy, rights and security in the age of big data. In: *37th International Conference on Information Systems, Dublin, Republic of Ireland.* pp. 1-20.

ARMERDING, T. (2018) *The 17 biggest data breaches of the 21st century* [Online] CSO. Available from: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html [Accessed 10/07/18].

ARONSON, J. (2018) The Utility of User-Generated Content in Human Rights Investigations. In: LAND, M. and ARONSON, J. (eds.*) New Technologies for Human Rights Law and Practice.* Cambridge: Cambridge University Press, pp. 129-148.

BARUH, L. and POPESCU, M. (2017) Big data analytics and the limits of privacy self-management. *New Media & Society*, 19 (4), pp.579-596.

BAXI, U. (2017) Towards socially sustainable globalization: reflections on responsible contracting and the UN guiding principles on business and human rights. *Indian Journal of International Law*, 57 (1), pp.163-177.

BERG, K. (2018) Big Data, Equality, Privacy, and Digital Ethics. *Journal of Media Ethics,* 33 (1), pp. 44-46.

BHAIMIA, S. (2018) The General Data Protection Regulation: the Next Generation of EU Data Protection. *Legal Information Management*, 18 (1), pp.21-28.

BILCHITZ, D. and DEVA, S. (2018) The human rights obligations of business: a critical framework for the future. In: LAND, M. and ARONSON, J. (eds.*) New Technologies for Human Rights Law and Practice.* Cambridge: Cambridge University Press, pp. 243-269.

BONNITCHA, J. and MCCORQUODALE, R. (2017) The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights. *The European Journal of International Law,* 28 (3), pp. 899–919.

BRABANT, S. and SAVOUREY, E. (2017) A Closer Look at the Penalties Faced by Companies*. France's corporate duty of vigilance law.*

BRAYNE, S. (2017) Big Data Surveillance: The Case of Policing. *American Sociological Review,* 82 (5), pp.977-1008.

BSR (2012) *Applying the Guiding Principles on Business and Human Rights to the ICT Industry: Version 2.0: Ten Lessons Learned*. [Online] BSR. Available from: https://www.bsr.org/reports/BSR_Guiding_Principles_and_ICT_2.0.pdf [Accessed 10/07/18].

BUHMANN, K. (2016) Public Regulators and CSR: The 'Social Licence to Operate' in Recent United Nations Instruments on Business and Human Rights and the Juridification of CSR. *Journal of Business Ethics*, 136(4), pp.699-714.

CEUKELAIRE, I. (2018) *This popular Facebook app publicly exposed your data for years* [Online] Medium. Available from: https://medium.com/@intideceukelaire/this-popular-facebook-app-publicly-exposed-your-data-for-years-12483418eff8 [Accessed 10/07/18].

CHIBBA, M and CAVOUKIAN, A. (2015) Privacy, consumer trust and big data: Privacy by design and the 3 C'S. *ITU Kaleidoscope: Trust in the Information Society*, pp.1-5.

CRABTREE, A. (2016) Enabling the new economic actor: data protection, the digital economy, and the Databox. *Personal and Ubiquitous Computing*, 20 (6), pp.947-957.

DAVITTI, D. (2016) Refining the Protect, Respect and Remedy Framework for Business and Human Rights and its Guiding Principles. *Human Rights Law Review*,16, pp. 55–75.

DEL ROWE, S. (2018) Businesses Need to Know GDPR. *Customer Relationship Management*, 22 (1), p.14.

DIMITROVA, A. and BRKAN,M. (2018) Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair, *Journal of Common Market Studies*, 56 (4), pp.751-767.

EC (2016) *From 6 to 28 members* [Online] EC. Available from: https://ec.europa.eu/neighbourhood-enlargement/policy/from-6-to-28-members_en [Accessed 10/07/18].

EC (n. d.) *What is a data controller or a data processor*? [Online] EC. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en [Accessed 10/07/18].

EL OUAZZANI, Z. and EL BAKKALI, H. (2018) A new technique ensuring privacy in big data: K-anonymity without prior value of the threshold k. *Procedia Computer Science*, 127, pp.52-59.

ELBERT, I. (2018) *Guest post: Why investors should care about business and human rights in the digital age* [Online] Advocates For International Development. Available from: http://www.a4id.org/policy/guest-post-investors-bhr-digital-age/ [Accessed 10/07/18].

ELIANTONIO, M., GALLI, F. and SCHAPER M. (2016) A balanced data protection in the EU: conflicts and possible solutions. *Maastricht Journal of European and Comparative Law*, 23 (3), pp.391-403.

ESTEVE, A. (2017) The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. *International Data Privacy Law,* 7(1), pp. 36-47.

FENECH, M. (2018) *The "new green"? Business and the responsible use of algorithms* [Online] OpenGlobalRights. Available from: https://www.openglobalrights.org/the-new-green-business-and-the-responsible-use-of-algorithms/ [Accessed 10/07/18].

GARTON ASH, T. (2017) *Free speech: ten principles for a connected world.* London: Atlantic Books.

GERRY, F. (2014) Using Data to Combat Human Rights Abuses. *IEEE Technology and Society Magazine*, 33(4), pp.42-43.

GLOBAL PARTNERS DIGITAL (2018) A Rights-Respecting Model of Online Content Regulation by Platforms. [Online] Global Partners Digital. Available from: https://www.gp-digital.org/publication/a-rights-respecting-model-of-online-content-regulation-by-platforms /[Accessed 10/07/18].

GREENE, C. (2018) *Data Abuse Bounty: Facebook Now Rewards for Reports of Data Abuse* [Online] Newsroom. Available from: https://newsroom.fb.com/news/2018/04/data-abuse-bounty/ [Accessed 10/07/18].

GREENLEAF, G. (2013) 'Modernising' data protection Convention 108: A safe basis for a global privacy treaty? *Computer Law and Security Review: The International Journal of Technology and Practice*, 29 (4) pp. 430-436.

HARWELL, D. (2018) *Google to drop Pentagon AI contract after employee objections to the 'business of war'*[Online] The Washington Post. Available from: https://www.washingtonpost.com/news/the-switch/wp/2018/06/01/google-to-drop-pentagon-ai-contract-after-employees-called-it-the-business-of-war/?noredirect=on&utm_term=.2ed2f0377b82 [Accessed 10/07/18].

HERBERT SMITH FREEHILLS (2017) *Corporate human rights infringements: are remedies effective?* [Online] Herbert Smith Freehills. Available from: https://www.herbertsmithfreehills.com/latest-thinking/corporate-human-rights-infringements-are-remedies-effective [Accessed 10/07/18].

HRBDF (n.d.) *Maintaining privacy* [Online] The Global Compact. Available from: https://hrbdf.org/dilemmas/Privacy/#.W0pogNUzbSH [Accessed 10/07/18].

HUO, Y., MA, L. and ZHONG, Y. (2018) A Big Data Privacy Respecting Dissemination Method for Social Network. *Journal of Signal Processing Systems*, 90 (4), pp.467-475.

ICS (n. d.) *What is Privacy by Design & Default?* [Online]. Available from: https://www.ics.ie/news/what-is-privacy-by-design-a-default [Accessed 10/07/18].

INTERNET WORLD STATS (2018) *Internet growth statistics: Today's road to e-Commerce and Global Trade Internet Technology Reports* [Online]. Available from: https://www.internetworldstats.com/emarketing.htm [Accessed 10/07/18].

JAIN, P., GYANCHANDANI, M. and KHARE, N. (2016) Big data privacy: a technological perspective and review. *Journal of Big Data*, 3 (1), pp.1-25.

JAIN, P., GYANCHANDANI, M. and KHARE, N. (2018) Differential privacy: its technological prescriptive using big data. *Journal of Big Data*, 5(1), pp.1-24.

JØRGENSEN , R. (2018) Human Rights and Private Actors in the Online Domain. In: LAND, M. and ARONSON, J. (eds.*) New Technologies for Human Rights Law and Practice*. Cambridge: Cambridge University Press, pp. 243-269.

JØRGENSEN, R. and DESAI, T. Right to Privacy Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google. *Nordic Journal of Human Rights*, 35(2), pp.106-126.

KITTICHAISAREE, K. and KUNER, C. (2015) *The Growing Importance of Data Protection in Public International Law.* [Online] EJIL: Talk! Available from: https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/[Accessed 10/07/18].

KNUCKEY, S. and JENKIN, E. (2015) Company-created remedy mechanisms for serious human rights abuses: a promising new frontier for the right to remedy? *The International Journal of Human Rights*, pp.1-27.

KOKOTT, J. and SOBOTTA, C. (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3 (4), pp. 222-228.

KOŠČÍK, M. and MYŠKA, M (2018) Data protection and codes of conduct in collaborative research. *International Review of Law, Computers & Technology*, 32 (1), pp. 141-154.

KROENER, I. and WRIGHT, D. (2014) Strategy for Operationalizing Privacy by Design. *The Information Society*, 30 (5), p.355-365.

KUCHLER, H. COCCO, F. (2018) *Facebook suspends 200 apps in wake of Cambridge Analytica scandal* [Online] Financial Times. Available from: https://www.ft.com/content/84a7145e-577f-11e8-bdb7-f6677d2e1ce8 [Accessed 10/07/18].

KULESZA, J. (2014) Transboundary data protection and international business compliance. *International Data Privacy Law*, 4 (4), pp.298-306.

KULESZA, J. International law challenges to location privacy protection. *International Data Privacy Law*, 3 (3), pp. 158-169.

KUNER, C. et al. (2013) The business of privacy. *International Data Privacy Law*, 3 (2), pp.65-66.

LAM, C. (2017) Unsafe Harbour: the European Union's demand for heightened data privacy standards in Schrems v. Irish data protection commissioner. *Boston College International and Comparative Law Review*, 40 (3), pp.1-13.

LATONERO, M. (2018) Big Data Analytics and Human Rights: Privacy Considerations in Context. In: LAND, M. and ARONSON, J. (eds.*) New Technologies for Human Rights Law and Practice*. Cambridge: Cambridge University Press, pp. 149-161.

LOWE, D. (2016) Surveillance and International Terrorism Intelligence Exchange:Balancing the Interests of National Security and Individual Liberty. *Terrorism and Political Violence*, 28 (4), p.653-673.

LYTVYNENKO, A. (2016) Approaches towards judicial and scientific definition of the 'personal data protection' discipline maxims, their explanatory and correlation, *Scientific Journal 'Science Rise'*, 8/1(25), pp. 66-73.

Maastricht Journal of European and Comparative Law, 23(3), pp.550-567.

MACKINNON, R.(2012) *Consent of the networked: the worldwide struggle for Internet freedom*. New York: Basic Books.

MACKINNON, R., REED, L. and ULLMAN, I. (2017) Submission to UN Special Rapporteur for Freedom of Expression and Opinion David Kaye: Content Regulation in the Digital Age [Online] Ranking Digital Rights. Available from: https://rankingdigitalrights.org/wp-content/uploads/2018/01/RDR-2018-David-Kaye-Submission.pdf [Accessed 10/07/18].

MAI, J-E. (2016) Big data privacy: The datafication of personal information. *The Information Society*, 32 (3), p.192-199.

MANTELERO, A. (2017) Regulating big data: The guidelines of the Council of Europe in the context of the European data protection framework. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 33 (5), pp.584-602.

MCDERMOTT, Y. (2017) Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, 4 (1), pp. 1-7.

MCPHALI, K. and ADAMS, C. (2016) Corporate respect for human rights: meaning, scope, and

MEHTA, B. and RAO, U. (2016) Privacy Preserving Unstructured Big Data Analytics: Issues and Challenges. *Procedia Computer Science*,78, pp.120-124.

MENON, S. and SARKAR, S. (2016) Privacy and Big Data: Scalable Approaches to Sanitize Large Transactional Databases for Sharing. *MIS Quarterly*, 40(4), pp.963-983.

MILANOVIC, M. (2015) Human rights treaties and foreign surveillance: privacy in the digital age. *Harvard International Law Journal*, 56 (1), pp. 81-146.

MITTELSTADT, B. (2017) From Individual to Group Privacy in Big Data Analytics.

NEGLIA, M. (2016) The UNGPs — Five Years on: From Consensus to Divergence in Public Regulation on Business and Human Rights. *Netherlands Quarterly of Human Rights*, 34 (4), pp.289-317.

NOLAN, J. (2018) The corporate responsibility to respect human rights: soft law or not law? In: LAND, M. and ARONSON, J. (eds.*) New Technologies for Human Rights Law and Practice.* Cambridge: Cambridge University Press, pp. 243-269.

NOWAK, M. (2014) The Right of Victims of Human Rights Violations to a Remedy: The Need for a World Court of Human Rights, *Nordic Journal of Human Rights*, 32 (1), pp. 3-17.

O'CONNOR, B. The final countdown to GDPR. *Accountancy Ireland*, 49 (4), pp. 52-54.

ORWELL, G. (1950) *Nineteen Eighty-Four*. New York: New American Library.

PATIL, T., PATNAIK, G.and BHOLE, A. (2017) Big Data Privacy Using Fully Homomorphic Non-Deterministic Encryption. *2017 IEEE 7th International Advance Computing Conference*, Jan. 2017, pp.138-143.

PENNEY, J. (2017) Internet surveillance, regulation, and chilling effects online: a comparative case study. *Internet Policy Review*, 6 (2), pp. 1-39.

PRESS, G. (2014) *12 Big Data Definitions: What's Yours*? [Online] Forbes. Available from: https://www.forbes.com/sites/gilpress/2014/09/03/12-big-data-definitions-whats-yours/#61507c213ae8 [Accessed 10/07/18].

PRIVACY INTERNATIONAL (2017) *The Guide to International Law and Surveillance* [Online] Privacy International. Available from: https://privacyinternational.org/feature/993/guide-international-law-and-surveillance [Accessed 10/07/18].

RALL, K. et al. (2016) Data Visualization for Human Rights Advocacy. *Journal of Human Rights Practice*, 8(2), pp.171-197.

REES, C. *(*2011*) Piloting Principles for Effective Company-Stakeholder Grievance Mechanisms: A Report of Lessons Learned.* Cambridge: Harvard Kennedy School.

REIDENBERG, J. (2014) The Data Surveillance State in the United States and Europe. *Wake Forest Law Review,* 49 (2), pp.583-608.

RUBINSTEIN, I. (2013) Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law*, 3 (2), pp.74-87.

SCHAAR, P. (2010) Privacy by Design. *Identity in the Information Society*, 3 (2), pp.267-274.

SCHARTUM, D.(2016) Making privacy by design operative, *International Journal of Law and Information Technology*, 24, pp. 151–175.

SETH, S. (2018) *How Much Can Facebook Potentially Make from Selling Your Data?* [Online] Investopedia. Available from: https://www.investopedia.com/tech/how-much-can-facebook-potentially-make-selling-your-data/ [Accessed 10/07/18].

SHIFT (2015) *Human Rights Due Diligence in High Risk Circumstances.* [Online] Shift. Available from: https://www.shiftproject.org/resources/publications/human-rights-due-diligence-high-risk-circumstances/ [Accessed 10/07/18].

SHIFT, OXFAM AND GLOBAL COMPACT NETWORK NETHERLANDS (2016*) Doing Business with Respect for Human Rights: A Guidance Tool for Companies*. [Online]. Available from:https://www.businessrespecthumanrights.org/image/2016/10/24/business_respect_human_rights_full.pdf [Accessed 10/07/18].

SORIA-COMAS, J. and DOMINGO-FERRER, J. (2016) Big Data Privacy: Challenges to Privacy Principles and Models. *Data Science and Engineering,* 1 (1), pp.21-28.

STRANG, K. and SUN, Z. Big Data Paradigm: What is the Status of Privacy and Security? *Annals of Data Science,* 4(1), pp.1-17.

SUMNER, S. (2016) *You - for sale: protecting your personal data and privacy online*. Amsterdam: Syngress.

TAYLOR, L. (2016) The ethics of big data as a public good: which public? Whose good? The shifting order of discourse. *Accounting, Auditing & Accountability Journal*, 29 (4), pp.650-678.

THE QUINT (2018) *What the Cambridge Analytica Data Breach Cost Facebook* [Online] The Quint. Available from: https://www.thequint.com/news/india/what-has-the-cambridge-analytica-data-breach-cost-facebook [Accessed 10/07/18].

VAN DIJK, N. et al. (2018) Right engineering? The redesign of privacy and personal data protection. *International Review of Law, Computers & Technology,* 32(2-3), pp.230-256.

VARNEY, M. (2016) Effective Redress of Grievance in Data Protection: An Illusion? *Maastricht Journal of European and Comparative Law*, 23 (3), pp.550-567.

WANG, X. (2017) *Privacy Concerns of Big Data in Social Network Industry.* Dissertation (MSc), University of Nottingham.

WANG, X. (2017) *Privacy Concerns of Big Data in Social Network Industry.* Dissertation (MSc), University of Nottingham.

WARE, W. (1977) Computers and Personal Privacy. *Proceedings of the American Philosophical Society*, 121 (5),pp. 355-359.

WARE, W. (1984) Information systems security and privacy. *Communications of the ACM*, 27 (4), pp. 1-26.

WARE, W. (1986) Emerging privacy issues. *Computers & Security*, 5(2), pp.167-167.

WATNEY, M. (2015) Intensifying State Surveillance of Electronic Communications: A Legal Solution in Addressing Extremism or Not? *10th International Conference on Availability, Reliability and Security*, pp.367-373.

WATT, E. (2017) *Cyberspace, Surveillance, Law and Privacy*. Thesis (PhD), University of Westminster.

WU, D., YANG, B. and WANG, R. (2016) Scalable privacy-preserving big data aggregation mechanism. *Digital Communications and Networks*, 2, pp. 122–129.

YILMA, K. (2018) The United Nations data privacy system and its limits. *International Review of Law, Computers & Technology*, pp.1-25.

YING, S. and GRANDISON, T. (2016) Big Data Privacy Risk: Connecting Many Large Data Sets, *IEEE 2nd International Conference on Collaboration and Internet Computing*, pp.86-91.

YOO, J. (2014) The legality of the national security agency's bulk data surveillance programs. *Harvard Journal of Law and Public Policy*, 37 (3), pp.901-930.

HUBER, P. (2015) *Orwell's revenge: the 1984 palimpsest*. New York: Free Press.

Table of Legislation

CoE Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (8.11.2001) No. 181.

CoE (Committee on Legal Affairs and Human Rights) Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and its explanatory report (15 November 2017) Doc. 14437.

CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (28.01.1981) No. 108.

CoE Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data (23 January 2017) T-PD(2017)01.

CoE Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (17-18 May 2018) CM/Inf(2018)15-final.

EC ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights (2011) [Online]. Available from: https://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf [Accessed 10/07/18].

EU (the European Parliament and the Council) Regulation on 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) (27 April 2016) Official Journal of the European Union, L 119/1.

EU FRA Rights and CoE Handbook on European data protection law 2018 edition (2018) [Online] Availiable from: https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf [Accessed 10/07/18].

European Parliament (Directorate-General for External Policies Policy Department) Implementation of the UN Guiding Principles on Business and Human rights (2017) [Online] EU. Availiable from: file:///C:/Users/1/Downloads/QA0417103ENN.en.pdf [Accessed 10/07/18].

Federal Trade Commission Act (2006) 15 U.S.C. 41 et seq.

FRA Opinion on Improving access to remedy in the area of business and human rights at the EU level (10 April 2017) No.1/2017.

HRC Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci (8 March 2016) UN Doc A/HRC/31/64.

HRC Report of the United Nations High Commissioner for Human Rights on Improving accountability and access to remedy for victims of business-related human rights abuse (10 May 2016) UN Doc A/HRC/32/19.

HRC Report of the Working Group on the issue of human rights and transnational corporations and other business enterprises on the sixth session of the Forum on Business and Human Rights (23 April 2018) UN Doc A/HRC/38/49.

HRC CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (8 April 1988) UN Doc HRI/GEN/1/Rev.1

ICCPR (HRC) Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee (17 August 2015) UN Doc CCPR/C/GBR/CO/7.

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171

OHCHR Concept note on the expert workshop with the purpose of identifying and clarifying principles, standards and best practices regarding the promotion and protection of the right to privacy in the digital age, including the responsibility of business enterprises in this regard (19 & 20 February 2018) [Online]. Available from: https://www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf [Accessed 10/07/18].

OHCHR The corporate responsibility to respect human rights: an interpretive Guide (2012) HR/PUB/12/02.

UN WORKING GROUP ON BUSINESS AND HUMAN RIGHTS (2017) Reflections on the theme of the 2017 Forum on Business and Human Rights [Online]. Available from: https://www.ohchr.org/Documents/Issues/Business/ForumSession6/ExplainingThemeLaunchingBlog.pdf [Accessed 10/07/18].

UNDG Data privacy, ethics and protection guidance note on big data for achievement of the 2030 agenda (n. d.) [Online] UNDG. Available from: https://undg.org/wp-content/uploads/2017/11/UNDG_BigData_final_web.pdf [Accessed 10/07/18].

UNGA (HRC) Note by the Secretariat on Improving accountability and access to remedy for victims of business-related human rights abuse: explanatory notes for guidance (12 May 2016) UN Doc A/HRC/32/19/Add.1.

UNGA (HRC) Report of the Office of the United Nations High Commissioner for Human Rights: Summary of the Human Rights Council panel discussion on the right to privacy in the digital age (19 December 2014) UN Doc A/HRC/28/39.

UNGA (HRC) Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie on Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework (21 March 2011) UN Doc A/HRC/17/31.

UNGA (HRC) Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie on Business and human rights: further steps toward the operationalization of the “protect, respect and remedy” framework (9 April 2010) A/HRC/14/27.

UNGA (HRC) Resolution on the right to privacy in the digital age (23 March 2017) UN Doc A/HRC/RES/34/7.

UNGA (HRC) Resolution on the right to privacy in the digital age (7 April 2017) UN Doc A/HRC/RES/34/7.

UNGA Convention on the Rights of Persons with Disabilities (adopted 30 March 2007, entered into force 3 May 2008) UN Doc A/RES/61/106, Annex I

UNGA Guidelines for the Regulation of Computerized Personal Data Files (14 December 1990) UN Doc A/RES/45/95.

UNGA Note by the Secretary-General on Promotion and protection of human rights and fundamental freedoms while countering terrorism (23 September 2014) UN Doc A/69/397.

UNGA Report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age (30 June 2014) UN Doc A/HRC/27/37.

UNGA Report of the Special Rapporteur on the right to privacy (2016) UN Doc A/71/368.

UNGA Resolution on the right to privacy in the digital age (10 February 2015) UN Doc A/RES/69/166.

UNGA Resolution on the right to privacy in the digital age (18 December 2013) UN Doc A/RES/68/167.

UNGA Universal Declaration of Human Rights (10 December 1948) UN Doc 217 A (III).

Table of Cases

Barbulescu v. Romania - 61496/08 [2016] ECHR 61 (12 January 2016)

Gabriele Weber and Cesar Richard Saravia v. Germany - 54934/00 [2006] ECHR 1173 (29 June 2006)

John Doe (Kidane) v. The Federal Democratic Republic of Ethiopia, Brief of Amici Curiae, United Nations Human Rights Experts in Support of Plaintiff-Appellant and Reversal, D.C. Ct. App., Case No. 16-7081 [2016], pp. 14-15, 17-18 (1 November 2016)

Klass and Others v. Germany - 5029/71 - Chamber Judgment [1978] ECHR 4 (06 September 1978)

Malone v. the United Kingdom - 8691/79 [1984] ECHR 10 (2 August 1984)

Mario Costeja Gonzalez v Google Spain and Google (Judgment of the Court) [2014] EUECJ C-131/12 (13 May 2014)

Roman Zakharov v. Russia - 47143/06 (Judgment (Merits and Just Satisfaction) : Court (Grand Chamber)) [2015] ECHR 1065 (04 December 2015)

S. and Marper v. the United Kingdom - 30562/04 [2008] ECHR 1581 (4 December 2008)

Schrems v. Data Protection Commissioner [2015] EUECJ C-362/14 (06 October 2015)

Taylor-Sabori v. the United Kingdom - 47114/99 [2002] ECHR 691 (22 October 2002)