



SHERPA

Current Human Rights Frameworks

A. Andreou, S. Laulhe-Shaelou, D. Schroeder



Deliverable 1.5 - 27 April 2019

This project has received funding from the
European Union's Horizon 2020 Research and Innovation Programme
Under Grant Agreement no. 786641



Document Control

Deliverable	D1.5 Current human rights framework
WP/Task Related	WP 1: Representation and Visualisation
Delivery Date	27 April 2019
Dissemination Level	Public
Lead Partner	Aequitas
Contributors	UCLanCY
Reviewers	Rowena Rodrigues, TRI, Bernd Stahl, DMU
Abstract	This deliverable provides an overview of the legal framework around 11 key thematic areas which are faced with challenges because of SIS.
Key Words	Dignity, Digital Divide, Unemployment, Data Protection and Privacy, Accountability and Liability, Bias and Discrimination, Democracy, Control, Manipulation and Freedom of Thought, Security, Dual Use, Misuse, Health and Safety, Environmental Impact, Rights of SIS, Robots rights.

Revision History

The challenges were written separately from the main document and later integrated. The individual pieces were written as follows between **Dec 2018** and **Feb 2019**:

- Andreou: Bias and Discrimination, Democracy, Freedom of Thought, Control and Manipulation, Health, Environment
- Lulhe-Shaelou: Privacy and Data Protection, Accountability and Liability, Security, Dual Use and Misuse, Rights, including Robot Rights
- Schroeder: Dignity, Digital Divide, Unemployment.

Revisions were produced following in-group feedback in **March and April 2019**. Lulhe-Shaelou added material to Unemployment. The table shows the revision history of the report itself.

Version	Date	Author(s)	Reviewer(s)	Notes
1	12 April 19	Andreou, Lulhe-Shaelou, Schroeder	R Rodrigues	
2	15 April 19	Andreou, Lulhe-Shaelou, Schroeder	R Rodrigues	
3	24 April 19	Andreou, Lulhe-Shaelou, Schroeder	B Stahl	

Table of Contents

- Table of Contents 3
- Executive Summary 6
- Introduction 7
 - Objectives and Methodology 9
 - Report Structure 10
 - Current Legal Framework of Protection of Human Rights vis-à-vis SIS 11
 - How it all started 11
 - Fundamental and basic rights 12
 - The EU legal order 12
 - The freedom of data 13
 - Court rulings 14
 - Other authoritative sources of law 15
 - Smart Information Systems: Definitions and Remarks 15
 - Big data 15
 - Artificial Intelligence 16
 - Challenges to Human Rights and Ethics 17
 - A theoretical overview 17
 - Legal and ethical regulation 18
 - Equitable Solutions 18
 - Final Comments 19
 - References 19
- 11 Thematic Areas faced with Challenges because of SIS 20
- SIS, Dignity and Care for the Elderly 22
 - Overview 22
 - What is the challenge? 23
 - Current legal and ethical instruments 24
 - Hard law 24
 - Soft law 25
 - Discussion 26
 - References 27
- SIS and the Digital Divide 29
 - Overview 29
 - What is the challenge? 29
 - Current legal and ethical instruments 31
 - Hard law 31

Soft law	32
Discussion.....	32
References	33
SIS and Unemployment.....	35
Overview	35
What is the challenge?.....	35
Current legal and ethical instruments	37
Soft law	38
Discussion.....	38
References	39
SIS and Privacy and Data Protection	41
Overview	41
Current legal and ethical instruments (split in values and principles).....	43
Discussion.....	45
References	46
SIS and Accountability and Liability	48
Overview	48
Current legal and ethical instruments (split in values and principles).....	48
Discussion.....	50
References	52
SIS and Bias and Discrimination	53
Overview	53
Discrimination based on language/accent.....	54
Racial Discrimination.....	54
Gender discrimination	54
Bias and discrimination leading also to security risks.....	54
Current legal and ethical instruments (split in values and principles).....	55
Discussion.....	56
References	56
SIS and Democracy, Freedom of Thought, Control and Manipulation	58
Overview	58
Current legal and ethical instruments (split in values and principles).....	59
Democracy	59
Freedom of thought.....	59
Freedom of expression	59
Overarching rights.....	59
Discussion.....	60
Respect for the rule of law.....	60

Transparency.....	60
Accountability	60
Public perception and the role of the media	60
Understanding data collection and use	61
References	61
SIS and Security, Dual Use, and Misuse	62
Overview	62
Current legal and ethical instruments (split in values and principles).....	62
Discussion.....	65
References	66
SIS and Health	67
Overview	67
Current legal and ethical instruments (split in values and principles).....	68
Discussion.....	69
References	70
SIS and the Environment.....	71
Overview	71
Current legal and ethical instruments	71
Hard Law	73
Discussion.....	73
References	74
SIS and Rights, including Robot Rights.....	76
Overview	76
Current legal and ethical instruments (split in values and principles).....	76
Human rights.....	77
Robots’ rights	78
Discussion.....	79
References	80
Recommendations	81

Executive Summary

Smart Information Systems (SIS), which are a combination of big data analytics and Artificial Intelligence (AI), constitute an integral part of our lives. From Google search, Amazon’s Alexa, surgery robots, digital libraries, location-based devices, affective computing, and human machine symbiosis, almost everybody in high-income regions is affected by SIS on daily basis.

Meanwhile, human rights and ethics discussions about SIS are taking place *whilst* the technologies are already omnipresent. The UK House of Lords, the UNESCO, the European Commission and the Pope, are only a few examples of those working on the human rights and ethics aspects of SIS.

This report analyses 11 specific challenges from a human rights perspective to move the debate to a concrete level, namely:



Dignity and Care for the Elderly



Digital Divide



Unemployment



Privacy and Data Protection



Accountability and Liability



Bias and Discrimination



Democracy, Freedom of Thought et al



Security, Dual Use and Misuse



Health



Environment



Rights, including Robot Rights

The main value of this report are the concrete discussions presented in the light of human rights frameworks, each of which outlines the main positions taken on each challenge, a requirement for moving forward with solutions.

In addition, two sets of existing recommendations are endorsed in the light of the analysis presented in this report. The five principles of the Data for Humanity Initiative and the European Commissions’ seven essentials for achieving trustworthy AI.



Introduction

Introduction

Smart Information Systems (SIS), which are a combination of big data analytics and Artificial Intelligence (AI), constitute an integral part of our lives. There is a plethora of examples which demonstrate this including, but not limited to Google search, Amazon's Alexa, healthcare and surgery robots, and social network data analysis for advertising purposes.

The role and relevance of data itself is manifested in, *inter alia*, the countless number of blogs and websites on the internet, profiles on social networking websites, digital libraries (Cato, 2014), bio-ICT,¹ the Internet of Things,² neuro-ICT, autonomous machines such as robots, vehicles and drones, location-based services and devices, quantum technology,³ cloud computing,⁴ affective computing,⁵ human machine symbiosis, personal computers, smart devices and others.

The technology industry has made lucrative use of big data to assess markets, predict consumer behaviour, identify trends and train machine-algorithms (Latonero, 2018). Moreover, the pace of technological developments and the way in which personal data collected within these SIS are being processed, affect each of us every day, in a variety of ways (Handbook on European data protection law, 2018) (Fig 1.).



Fig. 1 – Benefits of SIS

The benefits of SIS are several, with the task of enumerating and extrapolating on all of them going beyond the scope of the current analysis. Instead, three significant examples are outlined for demonstration purposes.

Firstly, the use of big data may assist in decision-making in real time, which has proved particularly useful for crises, where comprehensive timely information does not exist. Examples of this include crowd sourced maps after the Haiti earthquake in 2009 to millions of tweets related to Hurricane Sandy in New York (Latonero, 2018). The collection, analysis and/or

¹ ICT stands for information and communications technology

² 'An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment' (Madakam et al., 2015)

³ Quantum technology can offer much more than compact and fast computers and can give rise to a new kind of programming paradigm based on quantum principles (Fernandez, 2009)

⁴ *Cloud computing provides a paradigm shift of business and IT, where computing power, data storage, and services are outsourced to third parties and made available as commodities to enterprises and customers* (Antonopoulos and Gillam, 2017)

⁵ Affective computing is trying to assign computers the human-like capabilities of observation, interpretation and generation of affect features (Tao and Tan, 2005)

dissemination of such data through social networks were central vehicles for saving human lives in the two disasters.

Secondly, SIS can also support human rights fact-finding by providing a basis for estimating the probability that an individual belongs to a group that has been subjected to human rights violations. For example, the capability of access to millions of mobile phone records in a large city may reveal patterns of calls by individuals that suggest human trafficking for commercial sexual exploitation (Latonero, 2018).

Thirdly, healthcare is another area which has been positively impacted by SIS as such systems help patients live longer and healthier lives. From advances in robotics for prosthetic limbs to surgical robots and smart hospitals, the examples are numerous. SIS have also allowed patients to access health care without having to physically leave their home, opening windows of opportunity for, amongst others, persons inhabiting rural and isolated areas and persons with mobility problems. With the advances in wearable technology, patients can check metrics such as their pulse, oxygen levels and blood pressure and can upload this data directly to a mobile patient portal accessed by the patient's doctor. As well as facilitating access to health care and doctor-patient communication, the regular input and analysis of such data can serve to predict, for example, heart disease risks (Jobs for Work 4.0 – The Future of Employment, n.d.). As well as the aspect of patient care, embedded sensors in smartphones and applications are increasingly being used in health research, rendering the implementation of large-scale experiments outside the laboratory feasible (Brodie et al., 2018).

Despite the above significant benefits, chosen for the purpose of this introduction to concisely demonstrate how SIS can contribute to the protection of what is of utmost importance, namely human life and well-being, a critical and intricate question arises when evaluation SIS in their entirety, namely what challenges do SIS pose, if any, to human rights and ethics. The relevance of this question is enhanced by the omnipresence of SIS in our daily lives and the fact that this omnipresence will continue to exist and grow on a multitude of levels in the future.

Objectives and Methodology

The present analysis is concerned with determining challenges created by SIS with regard to human rights, setting out the legal and ethical framework relevant to tackling each challenge, both current and future. The first step was to determine eleven thematic areas faced with SIS-related challenges. Desktop research covering academic and grey literature revealed that the following challenges are discussed regularly (Fig. 2).

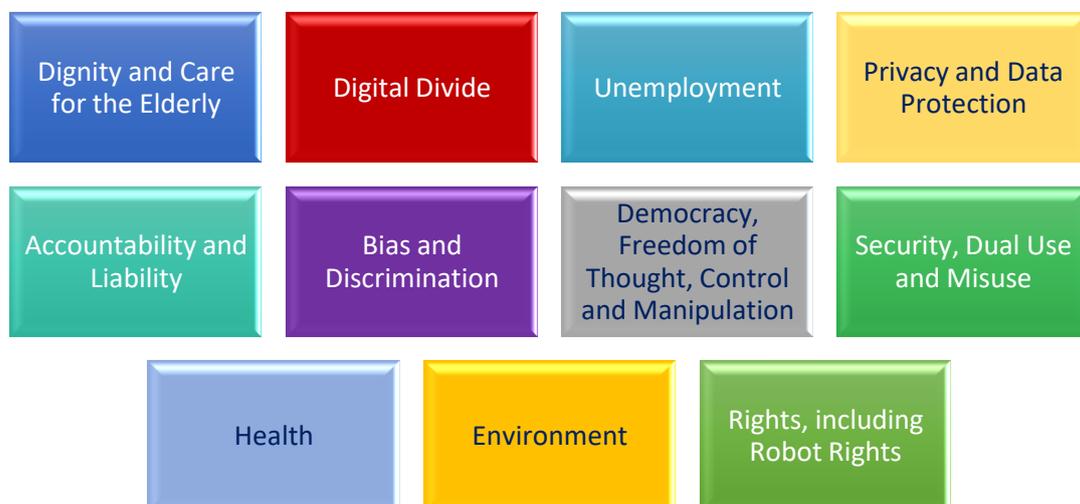


Fig. 2 – Challenges of SIS for Human Rights analysed in this Report

The approach allowed for a conceptualisation of each thematic area/challenge and the determination of potentially optimal solutions for the implementation of the Charter of Fundamental Rights of the European Union and other hard and soft legal instruments which aim at providing a fair, just and equitable society founded on principles of human rights.

The analysis was premised on a distinction between human rights principles enshrining the values and spirit of the protection of human rights through a broad legal and ethical framework at the global level, and human rights rules implementing these values and spirit following a rule-based approach through harder or softer instruments at the international, European and transnational level. The order of the challenges discussed in this Report reflects the level of complexity of the legal analysis, from more general philosophical considerations to various shades of hard and soft law analysis at the national, European and international level. Challenges presented at the start outline fundamental issues which call for renewed legal solutions around human values of dignity and respect, while later challenges identify the need for further regulation and coordination around key legal principles such as equality, freedom, civil and socio-economic rights, all encapsulating current and future technologies.

The proposed rule-based approach adopts a particular focus on the European Union and its Member States, as the EU is arguably the most accomplished model of global and multi-disciplinary integration, in a comparative perspective (compared to other models of integration in particular and/or units of integration such as key countries in the field of SIS).

It should be understood that such a legal and ethical framework of protection is defined broadly and malleably, so as to encompass the role of law and ethics in the multiple societal challenge that SIS poses to human rights. Movements such as ‘Law in Context’, Socio-legal Studies or Critical Studies look at law in the modern world, linking it very closely to ethics, whereas other movements such as Law and Philosophy, Law and Anthropology, Law and Politics or Law and Economics, analyse law from an external perspective. As SIS touch upon multiple aspects of modern society in a global setting, law was approached in this project ‘from the outside’, through an ethical, scientific and/or technical lens, thereby potentially creating a combined ‘Law, Ethics and Technology’ cluster.

This approach drives the project to a fair account of the current protection of human rights in the field of SIS through a careful delimitation of the applicable instruments of hard law, soft law and/or principles of (self-)regulation at international, European and transnational levels. It is important to note that through the desktop research on the legal and ethical framework of the protection of human rights vis-à-vis SIS, legal/instrumental overlaps were identified in terms of, for example, relevant legal instruments and types of solution proposed. These were therefore intertwined in the establishment of a blueprint of current and future practice in relation to the interrelationship of human rights, law, ethics and SIS, presented in this Report.

Report Structure

This report has three main parts, namely:

1. Introduction
2. Eleven thematic areas faced with challenges because of SIS
3. Recommendations

Current Legal Framework of Protection of Human Rights vis-à-vis SIS

At first glance, the current landscape of the protection of human rights vis-à-vis SIS may appear complex and over-populated, especially if one adopts a non-legal reading of this landscape. Thus, this Report uses an extroverted and synthesized reading of human rights vis-à-vis SIS, turned towards the implementation of core global values and ideas into instruments of hard or soft law as well as practices of standards, policies, guidelines and codes, not all of which are legally binding strictly speaking. Among the key actors in this landscape are the courts of law, in particular those located at the European level and acting as supranational and/or federal law makers. From this landscape unfolds a series of global challenges which are emblematic of the tension between human rights and SIS.

How it all started

The journey into the legal landscape of the protection of human rights starts at the international level, with the formulation of globally shared values and ideals of protection of human rights during the aftermath of the Second World War. Beyond basic fundamental rights such as the right to human dignity and equal rights, the right to security of a person, or the right of recognition as a person, the United Nation Universal Declaration of Human Rights of 1948⁶ provides inter alia for the right to non-arbitrary interference with one's privacy, family, home or correspondence and to non-attacks upon one's honour and reputation (Article 12), the right to freedom of thought, conscience and religion (Article 18) and the right to freedom of opinion and expression (Article 19).

These **basic fundamental rights and freedoms** are reiterated in the International Covenant on Civil and Political Rights of 1976,⁷ as well as enshrined in equivalent European legal instruments, such as the European Convention for Human Rights⁸ (ECHR) and the EU Charter of Fundamental Rights⁹ (EUCFR), including as follows:

Table 1 - Selection of Rights and Freedoms with potential relevance to SIS – European perspective

Rights	ECHR	EUCFR
Right to human dignity		Article 1
Right to the integrity of the person		Article 3
Right to liberty and security	Article 5	Article 6
Right to respect for private and family life	Article 8	Article 7
Protection of personal data		Article 8
Freedom of thought, conscience and religion	Article 9	Article 10
Freedom of expression and information	Article 10	Article 11
Prohibition of discrimination	Article 14; Article 1, Protocol 12	Article 21
Right of property	Article 1, Protocol 1	Article 17
Right to education	Article 1, Protocol 2	Article 14
Right to free election	Article 3, Protocol 1	Articles 39-40
Freedom of movement	Article 2, Protocol 4	Article 45
Freedom to choose an occupation and right to		Article 15

⁶ <http://www.un.org/en/universal-declaration-human-rights/index.html>

⁷ <https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>

⁸ https://www.echr.coe.int/Documents/Convention_ENG.pdf

⁹ http://www.europarl.europa.eu/charter/pdf/text_en.pdf

engage in work		
Freedom to conduct a business		Article 16
Rights of the child		Article 24
Rights of the elderly		Article 25
Integration of persons with disabilities		
Right to health care		Article 35
Consumer protection		Article 38
Right to good administration		Article 41
Right of access to documents		Article 42
Freedom of movement and residence		Article 45

Fundamental and basic rights

Depending on the legal instruments at stake, rights and freedoms may be recognized as fundamental or basic rights or may be related or derived rights, expressly or not. In other words, there are more *actual* rights than what the texts provide. That is the reason why it is appropriate to examine the EU legal framework where the list of express (provided in legal instruments) and implied rights (developed through other sources of law such as courts' decisions, guidelines or policies) appears to be the longest, both at the conceptual and applied level. It is important to note that lists of rights are not exhaustive and that they are subject to the interpretation of courts at the national and supranational level (international and European). As a result, human rights broadly speaking are a very dynamic category of the law, where the courts play a crucial role in the modernization of the legal framework, acting as a catalyst for further reform of legal instruments. The issue therefore is not one of existence of a right, but one of effective enjoyment of that right through human rights and fundamental freedoms.

The EU legal order

Examining the EU legal order as the main illustration of friction/overlap between human rights and SIS also has other advantages. First of all the EU legal order as an autonomous legal order, away from both international law and national law, has its own set of values and ideals as well as rules for implementation. These can be found in a common set of legal instruments, referred to as primary (EU Treaties, EU Charter) and secondary legislation (directives, regulations), applicable and effective across the EU and its Member States, thereby facilitating their examination (all these instruments are legally binding).

Echoing the EU Charter of Fundamental Rights, Article 2 of the Treaty on the European Union¹⁰ provides a non-exhaustive list of Union shared values, in particular respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities (Fig. 3).



¹⁰ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT>

Fig. 3 – Values from Article 2 of the Treaty on the European Union

The Treaty on the Functioning of the European Union (TFEU),¹¹ implementing the spirit of these rules, also sets out several provisions which are arguably directly or indirectly related to SIS, from a security perspective (combating computer crime, Article 83 TFEU), but also and mainly through a right-based approach putting fundamental rights at the centre of the EU architecture.

Core to the EU legal order is the freedom of movement of all factors of production, i.e. persons, goods, services and capital, to be balanced if need be with the protection of public interests such as national security, public order, but also mandatory requirements entailing the respect inter alia for the fundamental rights and freedoms set out in Table 1. This means that such rights and freedoms in the EU legal order benefit from an elevated status and operate both as rights and as safeguards through legally binding legal instruments, as applied and interpreted by the EU Courts and by other EU law actors.

The freedom of data

Technology therefore cannot occur in a vacuum. The freedom of data in the EU in particular cannot be absolute but is framed through a set of EU-specific principles, values and rules. In the event of a friction or overlap, a balancing exercise among the various interests at stake takes place (proportionality test), usually orchestrated by the EU Courts or by national courts guided by EU law. This multi-level mechanism arguably constitutes one of the main differences with other supranational sets of principles and rules, at the international and European level: the power of enforcement of EU laws and court decisions is strong, certainly within the EU legal order but also arguably beyond, influencing international norms.

An illustration of the extra-territoriality of EU law in the field of SIS is provided by the General Data Protection Regulation (GDPR),¹² an instrument of secondary legislation in the EU legal order, directly applicable and effective in all the Member States as of 25 May 2018. In a nutshell, the GDPR sets out principles relating to the processing of personal data in the EU and beyond if these data travel outside of the EU. Such data must be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of the personal data.¹³

The GDPR sets out principles relating to the processing of personal data in the EU and beyond if these data travel outside of the EU.



The GDPR also sets out provisions regarding the lawfulness of processing – when is processing necessary, i.e. proportionality test (Article 6) as well as a series of express rights, some of them newly created and unique to the EU legal order:

¹¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012E/TXT>

¹² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

¹³ Article 5 GDPR.

- Transparency of information, communication and modalities for the exercise of the rights of the data subject (Article 12);
- Right to information to be provided where personal data are collected from the data subject (Article 13);
- Right to information to be provided where personal data have not been obtained from the data subject (Article 14);
- Right of access by the data subject (Article 15);
- Right to rectification (Article 16);
- Right to erasure or 'right to be forgotten' (Article 17);
- Right to restriction of processing (Article 18);
- Right to notification obligation regarding rectification or erasure of personal data or restriction of processing (Article 19);
- Right to data portability (Article 20);
- Right to object (Article 21);
- Right not to be subject to an Automated individual decision-making, including profiling (Article 22).

The GDPR also contains some rights implied in its long Recital, as applications/manifestations of more general principles or fundamental rights, including:

- The right to technology neutrality deriving from the freedom of expression and non-discrimination (Recital 15);
- The right to the specific protection of sensitive data in relation to fundamental rights and freedoms, such as data revealing racial or ethnic origin, deriving from the principle of non-discrimination (Recital 51);
- The right of concise information to the public or to the data subject, easily accessible and easy to understand, in clear and plain language, deriving from the right to information (Recital 58);
- The right, in case of a data breach, that the data controller must notify the Supervisory Authority and the data subject without undue delay, as an application of the right to information (Recitals 85 and 86);
- Right to compensation in the case of infringement of the GDPR (Recital 146)

The GDPR with its accompanying Directive were implemented into national law in all the EU Member States, giving rise to new sets of rights at the national level. Some countries have decided to go beyond the scope of the GDPR itself by introducing new provisions or new rights, such as in France or in the UK. The reason for this is that sources of law for Member States of the EU are multiple: beyond directly applicable and effective provisions of EU law, these countries are influenced by legal instruments of the Council of Europe (turned into national laws in certain countries and/or ratified as international Treaties) as well as by the case law of the two European Courts: the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR).

Court rulings

Both Courts have issued several rulings in the field of SIS of relevance to this report. The CJEU for example created the right to be forgotten before it was embedded in the GDPR, in the case of *Google Spain and Google*.¹⁴ There is another pending case before the CJEU, considering whether Google could be forced to remove results not only from Google Spain but also from all Google

¹⁴ Case C-13/12 *Google Spain and Google*

domains.¹⁵ With respect to data portability to a third country, the CJEU also ruled before the entry into force of the GDPR that the fact that a Data Protection Commissioner found that a third country has adequate level of data protection does not mean that a supervisory body of a Member State cannot examine concerns of an individual concerning his rights and freedom.¹⁶ This judgment is reflected inter alia in Article 45 of the GDPR on data transfers on the basis of an adequate decision. The ECtHR has ruled inter alia on the right to rectification regarding ethic origin¹⁷ or on retention of data.¹⁸ By way of comparison the US Supreme Court ruled on the tracking of location data of customers of mobile phone companies.¹⁹

Other authoritative sources of law

Other authoritative sources of law in the field of SIS include relevant UN Resolutions,²⁰ instruments of the Council of Europe²¹ or other transnational instruments targeting multi-national companies in particular, including high-tech companies (Jenkins, 2001).²²

It appears from the above analysis of the current legal and ethical framework of human rights vis-vis SIS that multiple scenarios and challenges are possible. AI can be used to manipulate election results or breach privacy of data and there have been reports that AI might be discriminatory or biased in certain occasions. Ways to protect children and other vulnerable groups vis-à-vis AI and data collection are crucial. Questions of security vs. privacy arise, to be balanced with other interests at stake. On the other hand the EU wants to create an environment that will attract investments in AI and wants to capitalise on its leadership in robotics. Proposed AI guidelines should therefore look at the impact on human rights, among others, privacy, dignity, non-discrimination and socio-economic rights (European Commission, 2018).²³ All these are challenges set out in this Report, giving value to personal and other data in a digital environment, set to avoid a major ‘data crisis’, a new generation of crises.

Smart Information Systems: Definitions and Remarks

In order to establish the conceptual and semantical framework for the topics under consideration, this section provides definitions and makes some important, preliminary remarks. It thereby serves as a foundation for the subsequent analysis of the challenges that SIS pose to human rights so as to achieve an equitable balance of issues at stake and a protection and promotion of human rights and ethics.

Big data

Big data refers to ‘datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze’ (SARFATY, 2017) as well as to datasets which are utilised for predicting

Big data refers to ‘datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze.



¹⁵ Case C-507/17 Google (pending)

¹⁶ Case C-362/14, *Maximilian Schrems v Data Protection Commissioner*

¹⁷ *Ciubotaru v. Moldova*, No. 27138/04

¹⁸ *Brunet v. France*, No. 21010/10, 18 September 2014

¹⁹ *Carpenter v. United States*, No. 16-402 (US Supreme Court)

²⁰ <https://ccdcoe.org/sites/default/files/documents/UN-141119-TheRightToPrivacyInTheDigitalAge.pdf>

²¹ Convention on Cybercrime No.185 <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>; Convention No.108 on data protection https://edps.europa.eu/data-protection/our-work/publications/legislation/council-europe-convention-no-108-data-protection_en.

²² <http://www.unrisd.org/80256B3C005BCCF9/search/E3B3E78BAB9A886F80256B5E00344278>

²³ <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe>

certain outcomes and providing insight to particular themes (Richards and King, 2014).

Big data involves collecting data from numerous digital sources and sensors (Latonero, 2018). The value of big data is indisputable, with it being used for, inter alia, distinguishing behavioural patterns and profiling an individual in relation to, for example his or her needs and his or her relationships with others (Boyd and Crawford, 2011). With regards to big data's role in our lives, it is indicative to mention that we create 2.5 quintillion bytes of data every day (Cato, 2014). This data can be collected, processed, analysed, and visualised in order to collect social insights and patterns.

Behavioural indicators, at either the aggregate or individual level, can be used for observation, decision-making, and direct action (Latonero, 2018). Beyond that, Cato, who argues that big data is the metadata behind the content, stresses that thinking about the amount of content available on the internet is mind boggling. However, he holds that the amount of metadata out there equals the amount of content available on the internet multiplied by eleven (Cato, 2014). Richards and King talk about the 'big data revolution' which they consider to be the 'latest stage of the information revolution,' which has radically altered the functioning of our society and our lives (Richards and King, 2014). Boyd and Crawford argue that big data can create better tools, services and public goods and help us to understand online communities and political movements and will alter how human behaviour, culture and communication are investigated. Moreover, big data is viewed by them as a powerful tool with which we can address various societal ills, offering the potential of new insight into diverse areas such as cancer research, terrorism, and climate change (Boyd and Crawford, 2012).

Artificial Intelligence

Artificial intelligence (AI) is defined as:

'The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages' (Oxford Dictionaries, 2019).

It is worth clarifying that human intelligence generally follows a structure known as the 'perception–cognition–action information processing loop' in that they perceive, consider what to do, balance options and subsequently make decisions. AI is created to follow the same sequence with the machine appraising the context and then processing data through 'optimization and verification algorithms, with a choice of action made in a fashion similar to that of humans' (Cummings, 2017). Moreover, AI - which has been around for about six decades and is steadily developing due to factors ranging from the sheer amount of data to better computers and may now 'quickly discern patterns that humans cannot - make predictions more efficiently and recommend better policies (Cho, 2018).

Even though there is 'nearly universal agreement among modern AI professionals that AI falls short of human capabilities in a critical sense' algorithms have superseded human ability in domains such as chess playing (Bostrom and Yudkowsky, 2014). It is therefore not an exaggeration to support the argument of some scholars who maintain that, due to the broad capabilities of AI, which have, at times, superseded those of human experts, the possibility of AI to further surpass human performance in an expanding arena of fields will be a reality in the near future. In other words, AI is increasingly able to impact upon human opportunities and activities in a growing number of areas. Scholars such as Liu and Zawieska interpret this as a fundamental change and inversion in power relationships (Liu and Zawieska, 2017).

AI refers to computer systems that perform tasks, which normally require human intelligence.



```
var args =  
while ( 1--  
args[1]
```

Challenges to Human Rights and Ethics

A theoretical overview

Latonero argues that new information and communication technologies bring both benefits and costs to any given domain and holds that the potential risks in applying the technologies associated with big data analytics deserve greater consideration (Latonero, 2018). Among the possible, non-exhaustive list of dangers posed by SIS to human rights and/or ethics are privacy incursions, invasive marketing, tracking of protesters and suppression of speech (Boyd and Crawford, 2012). Richards and King talk of accentuated social change occurring at a great speed, supporting that the magnitude of the big data revolution is such that human comportment, attitudes and activities are impacted by predictions offered by the analysis of big data on themes ranging from dating to voting. They also give further examples of particularly crucial data sets on, for example, search, location and purchase history and also facial recognition which have already been accessed by governments and companies (Richards and King, 2014). Boyd and Crawford warn of the potential negative impacts of new technologies and, in particular, the impact relating to, for example, analysing data received from social media connections, telephones and State records. Through this sphere, big data is viewed as a troubling manifestation of a Big Brother regime where liberty and fundamental rights are threatened (Boyd and Crawford, 2012).

Big data is viewed as a troubling manifestation of a Big Brother regime where liberty and fundamental rights are threatened.



Moreover, Boyd and Crawford argue that big data is the kind of data that encourages the practice of apophenia, namely seeing patterns where none exist, simply because massive quantities of data can offer connections that radiate in all directions. Due to this, it is crucial to pose questions about the analytic assumptions, methodological frameworks and underlying biases embedded in big data (Boyd and Crawford, 2011). Similarly, ethical data collection protocols that protect privacy in the human rights context, such as obtaining informed consent, are extraordinarily difficult to utilise when deploying big data analytics (Latonero, 2018).

To illustrate the above normative discussion, the Cambridge Analytical scandal is useful, as it led not only to a breach of privacy but also a severe manipulation of an electorate (Common, 2018). In this case, Facebook gave Cambridge Analytica unauthorized access to personal data of more than 87 million Facebook users. The data company then developed the 'ability to 'micro-target' individual consumers or voters with messages most likely to influence their behaviour' (Isaak and Hanna, 2018). This is starkly demonstrative of the ways in which SIS interact, and threaten, democracy and freedom of thought and are relevant to issues of control and manipulation, thematic areas which are all developed in this gap analysis.

AI is already the source of challenges to existing human rights protection today, and these challenges have been articulated as issues that are contained within certain spheres of activities or in relation to enumerated legal protections (Liu and Zawieska, 2017). At the same time, taking personal data into consideration, 'individuals have little idea concerning what data is being collected, let alone shared with third parties' (Richards and King, 2014). Beyond human rights, from an ethical point of view, we are faced with intricate questions including how to avoid harm caused to humans by machines and understanding the potential challenges for ensuring a safe operation of AI as it approaches humans in terms of intelligence levels (Bostrom and Yudkowsky, 2014).

Individuals have little idea concerning what data is being collected, let alone shared with third parties.



Legal and ethical regulation

The benchmark for ascertaining the content and threshold of human rights protection in relation to how to tackle the challenges under consideration will emanate from principles developed in, *inter alia*, the Universal Declaration of Human Rights and the European Convention on Human Rights and rules embedded in the Charter of Fundamental Rights of the European Union and relevant European and national primary and secondary legislation. For purposes of demonstration, reference is made to the issue of privacy with the General Data Protection Regulation constituting a central vehicle for the enjoyment of the right to privacy. This Report also assesses ethical instruments such as the UNESCO Universal Declaration on Bioethics and Human Rights, which addresses ethical issues related to medicine, life sciences and associated technologies, as applied to human beings, taking into account their social, legal and environmental dimensions. Given the nature of SIS and the type and extent of their impact on a broad range of areas which can potentially affect human rights, both the legal and ethical frameworks need to be examined before equitable solutions can be given.

Equitable Solutions

Technology is neither good nor bad; nor is it neutral and its interaction with our social ecology is such that technical developments frequently have environmental, social, and human consequences (Boyd and Crawford, 2012). With this knowledge, it is essential to find an equitable solution vis-à-vis safeguarding human rights and ethical norms on the one hand and upholding technological development on the other.

As the UN Special Rapporteur on Privacy stated: ‘the nature of trans-border data flows and modern information technology requires a global approach to the protection and promotion of human rights and particularly the right to privacy’ (Human Rights Council, 2017).

In relation to ethics, as Bostrom and Yudkowsky argue: ‘when AI algorithms take on cognitive work with social dimensions—cognitive tasks previously performed by humans—the AI algorithm inherits the social requirements’ (Bostrom and Yudkowsky, 2014). Moreover, Boyd and Crawford argue that, given the rise of big data as a socio-technical phenomenon, it is necessary critically to interrogate its assumptions and biases (Boyd and Crawford, 2012). Richards and King, in a similar vein, hold that big data, broadly defined, are producing ‘increased powers of institutional awareness and power that requires the development of big data ethics.’ To this end, they argue that the current construction of the digital society should incorporate the principles and values dear to us (Richards and King, 2014).

Critically, some people’s approach to SIS fails to incorporate the principles that are essential for any democratic society such as privacy, identity and free choice and ‘our big data society risks abandoning these values for the sake of innovation and expediency’ (Richards and King, 2014). In brief, an appropriately aligned regime needs to be developed to confront technological power directly in order to ensure the continuity of human rights protection (Liu and Zawieska, 2017). In this effort, it is important to remember that regulatory strategies need to be devised that are capable of taking into account the prospect of a power reversal between human beings and AI, before the widespread societal adoption of AI. It is also important to remember that there is a tendency towards isolated considerations, which leads to a fragmented understanding of the true nature of the issue. The possibility that a larger structural shift is taking place is coveted by the fact that an incomplete portrait has been painted, and this truncated understanding prevents progressive developments of human rights protections (Liu and Zawieska, 2017).

Final Comments

SIS constitute a central aspect of modern life, with an impact on several levels and frameworks. This Report looks at the meaning of the identified challenges in the framework of law and ethics and discusses how to ensure adequate protection and promotion of principles, which are paramount for the functioning of a democratic society. Through desktop research, liaison with researchers working with, inter alia, future scenarios and stakeholders and through the common methodology as to the approach of human rights in the two-fold manner of principles and rules, this output provides a multilevel conceptualisation of the interplay between SIS, human rights and ethics.

All images for this report were either bought from istock, bought in groups of icons or were licence-free for non-commercial purposes.

References are presented per section rather than at the end.

References

- Antonopoulos, N. Gillam L. (2017). *Cloud Computing: Principles, Systems and Applications*
- artificial intelligence. (2019). In: *Oxford Dictionaries*. [online] Oxford University Press. Available at: https://en.oxforddictionaries.com/definition/artificial_intelligence [Accessed 22 Apr. 2019].
- Bostrom, N. and Yudkowsky, E. (2014) "The ethics of artificial intelligence," in Frankish, K. and Ramsey, W. M. (eds) *The Cambridge Handbook of Artificial Intelligence*. Cambridge: Cambridge University Press, pp. 316–334.
- Boyd, D. and Crawford K. (2012). 'CRITICAL QUESTIONS FOR BIG DATA'. *Information, Communication & Society*, 15:5, 662-679
- Boyd, D. And Crawford, Kate. (2011) 'Six Provocations for Big Data A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011.
- Brodie, M., Pliner, E., Ho, A., Li, K., Chen, Z., Gandevia, S. and Lord, S. (2018). Big data vs accurate data in health research: Large-scale physical activity monitoring, smartphones, wearable devices and risk of unconscious bias. *Medical Hypotheses*, 119, pp.32-36.
- Cato, A. (2014). Big Data? Big Deal. *Australian Law Librarian*, 22(4), pp.222-224.
- Cho, R. (2018). *Artificial Intelligence—A Game Changer for Climate Change and the Environment*. [online] State of the Planet. Available at: <https://blogs.ei.columbia.edu/2018/06/05/artificial-intelligence-climate-environment/>
- Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, COM(2018) 237 final.



```
elif operation == "MIRROR_X":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end -add
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = mirror_ob
print("Selected" + str(modifier_ob.name))
bpy.context.scene.objects.active = modifier_ob
```

11 Thematic Areas faced with Challenges because of SIS

As mentioned in the introduction, the present analysis is concerned with determining challenges created by SIS on human rights, setting out the legal and ethical framework relevant to tackling each challenge, both current and future. To achieve these objectives, the first step was to determine, through desktop research, eleven thematic areas faced with SIS-related challenges. Those are:



Dignity and Care for the Elderly



Digital Divide



Unemployment



Privacy and Data Protection



Accountability and Liability



Bias and Discrimination



Democracy, Freedom of Thought et al



Security, Dual Use and Misuse



Health



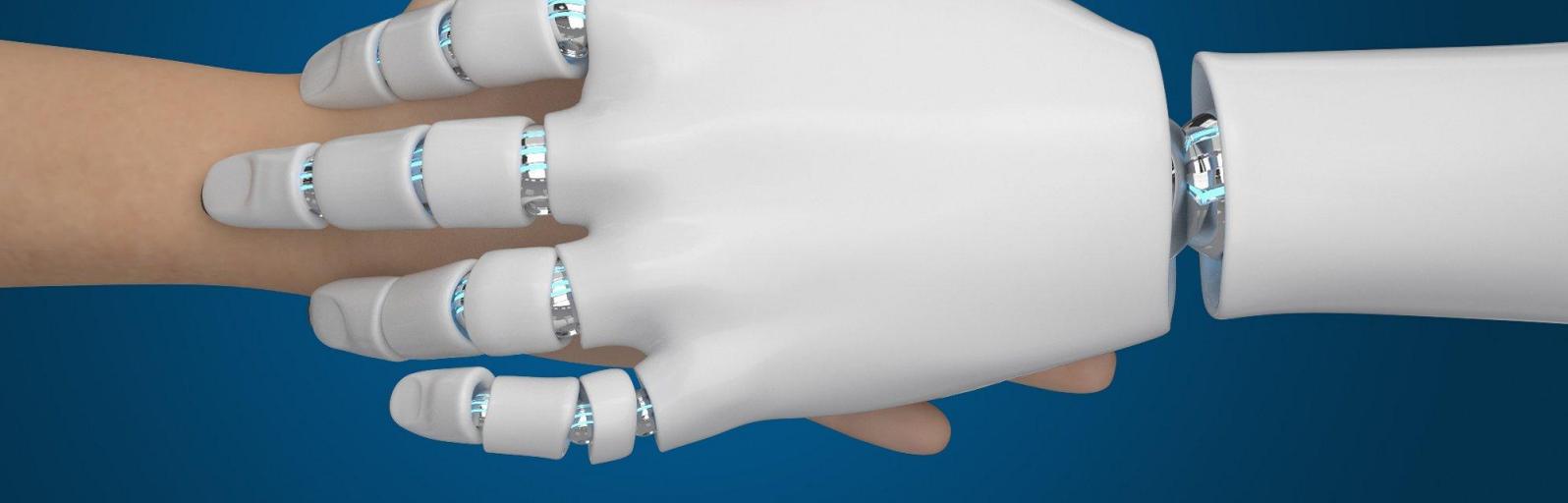
Environment



Rights, including Robot Rights

Repeat Fig. 2 – Challenges of SIS for Human Rights analysed in this Report

They are presented in the following pages in the order outlined above.



SIS, Dignity and Care for the Elderly

Overview

Dignity is a term that is widely used in legal instruments (Schroeder 2012) even though its meaning is highly contested (Schroeder 2010). For instance, in 2008, the Canadian Supreme Court decided that dignity was not to be used in anti-discrimination cases any longer as it was "confusing and difficult to apply".²⁴ It has also been argued that it is used in debates about new technologies as a slogan without substance (Macklin 2003). It is therefore most illuminative to look at one particular topic within the dignity debate rather than cover the subject generically. The topic chosen is care for the elderly and robots. In Japan, this topic is no longer futuristic (Foster 2018), which makes it particularly interesting for the European debate, which is still mostly hypothetical. The following table summarizes the overall challenge, two points of view in the SIS debate as well as the contributions from human rights instruments.

Challenge	SIS	Human Rights? Ethics?
<ul style="list-style-type: none"> • In 2050 over 36% of Europe's population is likely to be older than 65 years. • Care for the elderly in Europe still relies heavily on informal care provided by women. • In the UK alone, the formal care sector will be under-staffed by 400,000 by 2028. 	<ul style="list-style-type: none"> • Social robots could contribute to long-term care by reducing women's care load and the need for human staff. • Social robots could lead to a loss of privacy, be open to manipulation, reduce valuable human contact and create harm through malfunction. • Social robots might reduce loneliness and isolation. • 	<ul style="list-style-type: none"> • The European Pillar of Social Rights includes affordable and good quality long-term care (LTC) services as one of its 20 core principles. • Dignity is an important, often the most prominent, principle in professional codes about LTC. • The human rights and ethics challenges of robot use in LTC are not most usefully discussed using the concept of dignity.

Overview tables are provided only for the three broadly analysed challenges (challenges 1-3)

²⁴ R. v Kapp (2008) Supreme Court Canada 41 at §22: '[H]uman dignity is an abstract and subjective notion that... cannot only become confusing and difficult to apply; it has also proven to be an additional burden on equality claimants, rather than the philosophical enhancement it was intended to be.

What is the challenge?

An old lady sits alone in her sheltered accommodation stroking her pet robot seal. She has not had any human visitors for days. A humanoid robot enters the room, delivers a tray of food, and leaves after attempting some conversation about the weather, and encouraging her to eat it all up. The old lady sighs, and reluctantly complies with the robot's suggestions. When she finishes eating, she goes back to stroking the pet robot seal: "At least you give my life some meaning" she says (Sharkey 2014).

European societies are ageing. In 1950, only 12% of the European population was over age 65. Today the share has already doubled, and projections show that in 2050 over 36% of Europe's population will be 65-plus years (Pavlova 2017).

Old age brings specific challenges, which now affect higher numbers of people. In particular, social isolation and loneliness in older age are both increasing and have been identified as a health risk (Luo et al 2012).

This health risk could be reduced by good care. However, low pay and poor working conditions, caused by chronic underfunding of care and a 'race to the bottom' by private providers, has resulted in the sector struggling to recruit and retain the workers it needs to meet rising demand. In the UK alone, there will be a shortage of 350,000 workers in social care by 2028, rising to nearly 400,000 if freedom of movement ends after Brexit (Eichler 2018).

Care is not only provided professionally. In all 35 European countries long-term care (LTC) relies heavily on informal carers, mainly spouses and children of the care-dependent person. In most cases, they are women (Spasova et al 2018).

Taking all of these factors into account, one might argue that robots, in particular social robots, could resolve a major issue in care. "Loneliness and social isolation are problems for many seniors, but studies have shown that help could come from social robots – autonomous robots trained to interact and communicate with humans" (di Nuovo 2018).

Amanda Sharkey, whose vivid picture of an old lady was used at the outset of this section, entitles her contribution "Robots and human dignity: a consideration of the effects of robot care on the dignity of older people" (Sharkey 2014, emphasis added). Sharkey believes, contrary to di Nuovo (2018), that an old lady being cared for by robots is a depressing picture, and links this to dignity loss. Likewise, Sparrow and Sparrow (2006) emphasize "the importance of the social and emotional needs of older persons—which, we argue, robots are incapable of meeting—in almost any task involved in their care".

Why is this called a dignity problem? From a human rights perspective, dignity can never be lost, given that human rights frameworks usually use Kantian dignity as their reference point (Mahoney 2007: 33ff). According to Immanuel Kant (1724-1804), who is widely regarded as the greatest Western philosopher in post-medieval times (Roberts 1988: 9), all human beings have dignity or what he calls an absolute inner worth that nobody can take away from them (Kant 1990: 76). That all humans are equal in this dignity and therefore deserve to have human rights bestowed on them is something that Kant justified philosophically.²⁵

This Kantian approach on inviolable dignity contradicts much of the literature on dignity at the end of life, in particular positions from the assisted-dying movement. This movement often demands a peaceful death ahead of the indignities of old age, where other humans may see the patient as

²⁵ A short explanation of how "self-determination grounded within the authority of human reason" bestows human rights, according to Kant, is given in the Human Rights entry of the Internet Encyclopedia of Philosophy at: <https://www.iep.utm.edu/hum-rts/> To go into more detail here would be inappropriate for the purpose of this report.

incontinent and demented, a situation they claim creates significant indignities and embarrassment (Dworkin et al 1997).

Hence, on the one hand, we have the Kantian position, which is engrained in legal instruments, that dignity can never be lost. Hence, there cannot be any dignity problems in the care world at the end of life. On the other hand, we have two contradictory positions on the topic of elderlies and robot care, both assuming that dignity can be lost. The vignette at the start of this section by Sharkey (2014) is part of a longer article, which assumes that robot care can be an affront to human dignity.

Simultaneously, robot care could be a solution to dignity problems understood as resulting from perceived indignities. Older people are often too embarrassed to mention problems and request help with incontinence and memory lapses to carers or family (Robinson et al 2014). There is currently not enough research to indicate whether they would be more comfortable to raise such issues with robots, but Jean Paul Sartre might argue that this is likely. He indicated in much of his work that being looked upon by other humans in embarrassing situations is problematic because of the ensuing judgement (Sartre 1958: 222). Robots, at least in the foreseeable future, would not have this ability. Hence, they might be a suitable solution for care involving tasks that elderly people find damaging to their personal dignity. Can legal and ethical instruments shed some light on these contradictions?

Current legal and ethical instruments

Hard law

The term dignity was not part of the language of law or jurisprudence before the 20th century. It was first mentioned in the Constitution of the Weimar Republic in 1919, followed by the Portuguese Constitution in 1933 and the Irish Constitution in 1937 (Tiedemann 2006: 13). However, it was the concept's inclusion in international legal documents which marked its ascendancy. Table 1 lists some major legal instruments which make prominent reference to dignity, starting with the Universal Declaration of Human Rights in 1948.

Table 2 - Dignity in Legal Instruments and Guidelines

Origin	Quote
UN Universal Declaration of Human Rights. 1948. Preamble.	The recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world.
International Covenant on Civil and Political Rights. 1966. Preamble	Recognizing that these rights derive from the inherent dignity of the human person.
Treaty on European Union, Art.2 and Art. 21	The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. The Union's action on the international scene shall be guided by the principles which have inspired its own creation [...] respect for human dignity.
German Constitution. 1949. Article 1.	Human dignity is inviolable.



The above four entries in the table are indicative of a large number of legal instruments, in particular constitutions, which make use of dignity in their preambles or founding provisions (Schroeder and Bani-Sadr 2017: 22).

However, the dignity referred to in constitutions around the world does not address the kind of dignity issues that the old lady faces. They are usually reserved for a different type of much more severe violations (see Figure 1), in particular related to torture, slavery, extreme discrimination, reproductive manipulation or breaking of the will (Schroeder and Bani-Sadr 2017: 19ff).

Can the European Pillar of Social Rights (EPSR) (European Commission 2017) be helpful, where the dignity concept of constitutions is not? Principle 18 of the EPSR reads:

Everyone has the right to affordable long-term care services of good quality, in particular home-care and community-based services.

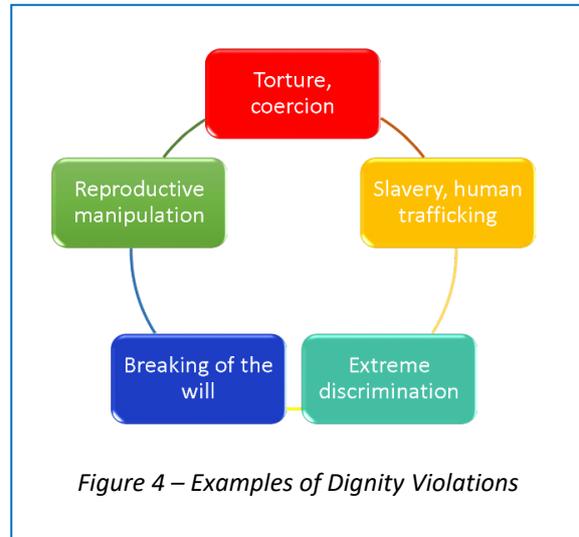


Figure 4 – Examples of Dignity Violations

How this right is promoted through the various European governments is different in each case. For instance, the German government supports an elaborate system to attract Eastern European, especially Polish, carers to Germany. But this has highly negative impact on the situation in Poland (von Wrangel 2017). World-wide, the only government dynamically promoting robot care for the elderly is the Japanese government, which hopes that such care can fill a projected shortfall of 380,000 specialized [care] workers by 2025” (Foster 2018). At this point, it is unclear how Principle 18 will be related to robot care for the elderly, as European governments have not yet developed specific policies. The British government’s policies might be the most interesting to observer in this regard, as their shortage of care workers for the elderly will resemble Japanese shortages due to Brexit (Eichler 2018).

There are therefore no hard law prescriptions for the types of dignity loss that the old lady faces, left without human contact, cared for by a robot. What about soft law?

Soft law

Broad ethics statements, such as the Convention for the Protection of Human Rights and Dignity of the Human Being (short: Oviedo Convention) (Council of Europe 1997) are not relevant. As in hard law, the Oviedo Convention only refers to dignity very generally at the start.

One would then next look in professional ethics code for those who directly work with elderly people, e.g. nurses or social workers. And, indeed, the first Article in the UK’s Nursing and Midwifery Council’s (2018) The Code - Professional standards of practice and behaviour for nurses, midwives and nursing associates reads:

1. Treat people as individuals and uphold their dignity To achieve this, you must:
 - 1.1 treat people with kindness, respect and compassion
 - 1.2 make sure you deliver the fundamentals of care effectively
 - 1.3 avoid making assumptions and recognise diversity and individual choice
 - 1.4 make sure that any treatment, assistance or care for which you are responsible is delivered without undue delay
 - 1.5 respect and uphold people’s human rights

In this professional code, dignity is equated with respecting and upholding human rights. But there are no human rights to human company or avoidance of observed indignities, neither in hard law, nor in soft law. Is dignity then perhaps not the best concept to discuss the needs, including for company, of the elderly?

Discussion

“It is difficult to write about dignity. No other term has been used in so many settings with so many contradictory meanings” (Schroeder and Bani-Sadr 2017, 1).

Some people are likely to say that being cared for by a robot in old age contributes to human dignity, for instance by removing some of the perceived indignities (e.g. incontinence) from human view. Others are likely to say that leading a life in isolation from others, with only social robots for company, is a life that lacks dignity (Sharkey 2014). Hence, dignity is used by proponents of opposing views to defend their position. One could therefore agree with the Canadian Supreme Court cited at the start, which decided (in anti-discrimination cases) that dignity was too confusing to apply in courts.

Recognising that dignity is only very generally protected in human rights law, it is important to ask whether other rights violations or unethical practices might be connected with robot care for elderly people before coming to any conclusions.

A literature review showed three main unresolved issues with regard to care for the elderly by robots (other than dignity losses), which are listed in Table 2.

Table 3 - Unresolved Issues in Robot Care for the Elderly

Issue	Description	Source
Loss of privacy	The user is under observation through robot technology and how it is linked to, for instance, support networks in the case of emergencies,	Sharkey and Sharkey 2012 Sorrell and Draper 2014
Harm through malfunction	Malfunctioning robots can create harm in a multitude of ways, for instance, by handing a person the wrong pills.	Stahl and Coeckelberg 2018
Deception and manipulation	Elderly people, especially those with cognitive impairments, might be unable to realise they are being cared for by robots, and mistakenly believe they are dealing with an empathic human.	Borenstein and Pearson, 2010 Sharkey and Sharkey 2012 Wachsmut 2018

The above three issues are a direct concern in robot care for the elderly. But the concept of dignity is not a useful vehicle to discuss potential human rights and ethical issues in this context, because the concept can support diametrically opposed positions, as shown earlier, given that there are so many interpretations of dignity.

In addition, individual human beings may vary considerably in their estimation of what robot care can do for them. A one-conclusion-fits-all-cases suggestion is therefore often not possible. For instance, many people may want to stay in their own home despite needing care and may welcome robot care to facilitate their wish. Research has shown that

“older people indicated that they would like a robot for detecting falls, controlling appliances, cleaning, medication alerts, making calls and monitoring location. Most of these tasks point towards maintaining independence and dignity” (Robinson et al 2014).

Others, who have a strong need for human contact, may prefer a care home with human nurses. The pros and cons of robot care for the elderly cannot therefore be resolved through arguments across all cases. It is more important that mechanisms are developed to reduce privacy loss, ensure safety against malfunctions, and examine in more detail the potential detrimental effects of deception and how they can be reduced.

A cautious position on the subject would be: “Care robots don't substitute for the human being— [says a geriatric nurse] they help when no one else is there to help” (Wachsmut 2018)

References

- Borenstein J, Pearson Y (2010) Robot caregivers: harbingers of expanded freedom for all? in: Ethics and Information Technology, 12(3)277-88.
- Council of Europe (1997) Oviedo Convention, <https://www.coe.int/en/web/bioethics/oviedo-convention>
- di Nuovo, A (2018) How robot carers could be the future for lonely elderly people, Independent 6 December 2018, <https://www.independent.co.uk/life-style/gadgets-and-tech/features/robot-carer-elderly-people-loneliness-ageing-population-care-homes-a8659801.html>
- Dworkin R, Nagel T, Nozick T, Rawls J, Scanlon T, Jarvis Thomson J (1997) Assisted Suicide, The Philosophers' Brief, New York Times Book Review, 27 March 1997.
- Eichler, W (2018) Care sector faces staff shortage of 400,000 over next decade, LocalGov, <https://www.localgov.co.uk/Care-sector-faces-staff-shortage-of-400000-over-next-decade-/46444>
- European Commission (2017) The European Pillar of Social Rights in 20 principles, https://ec.europa.eu/commission/priorities/deeper-and-fairer-economic-and-monetary-union/european-pillar-social-rights/european-pillar-social-rights-20-principles_en
- Foster, M (2018) Robots making inroads in Japan's elder care facilities, but costs still high, Japan Times, <https://www.japantimes.co.jp/news/2018/03/30/national/robots-making-inroads-japans-elder-care-facilities-costs-still-high/#.XLmZpfZul2w>
- Kant I (1990) *Metaphysische Anfangsgründe der Tugendlehre*, Hamburg: Felix Meiner Verlag.
- Luo Y, Hawkey LC, Waite LJ, Cacioppo JT (2012) Loneliness, health, and mortality in old age: a national longitudinal study, in: *Soc Sci Med* 74(6):907-14.
- Macklin R (2003) Dignity is a useless concept, *BMJ* 327: 586.
- Mahoney, J (2007) *The Challenge of Human Rights*, Blackwell: Oxford.
- Nursing & Midwifery Council (2018) *The Code - Professional standards of practice and behaviour for nurses, midwives and nursing associates*, <https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/nmc-code.pdf>
- Pavlova, M (2017) Europe is going grey: can EU countries work together to care for their elderly?, in: *The Conversation*, 22 August 2017, <https://theconversation.com/europe-is-going-grey-can-eu-countries-work-together-to-care-for-their-elderly-80416>
- Roberts J (1988) *German Philosophy - An Introduction*, Polity Press, Oxford.
- Robinson H, MacDonald B, Broadbent E (2014) The Role of Healthcare Robots for Older People at Home: A Review, *Int J of Soc Robotics*, 6:575–591.
- Sartre, JP (1958) *Sartre, Jean-Paul (1958) Being and Nothingness*, London: Methuen & Co.
- Schroeder D (2010) Dignity – One, two, three, four, five; still counting, *Cambridge Quarterly of Healthcare Ethics*, Vol. 19:1,118-125, 2010

- Schroeder D (2012) Human Rights and Human Dignity - An Appeal to Separate the Conjoined Twins, *Ethical Theory and Moral Practice*, Vol. 15(3):323-335.
- Schroeder D, Bani-Sadr AH (2017) *Dignity in the 21st Century – Middle East and West*, Springer: Berlin.
- Sharkey, A (2014) Robots and human dignity: a consideration of the effects of robot care on the dignity of older people, in: *Ethics Inf Technol* 16: 63. <https://doi.org/10.1007/s10676-014-9338-5>
- Sharkey, A and Sharkey N (2012) Granny and the robots: ethical issues in robot care for the elderly, in: *Ethics Inf Technol*, 14(1) 27–40.
- Sorell T, Draper H. (2014) Robot carers, ethics, and older people, in: *Ethics Inf Technol*, 16: 183
- Sparrow R, Sparrow L (2006) In the hands of machines? The future of aged care), in: *Minds and Machines*, 16 (2) 141–61.
- Spasova S, Baeten R, Coster S, Ghailani D, Peña-Casas R, Vanhercke B (2018) Challenges in long-term care in Europe - A study of national policies, European Commission, <https://ec.europa.eu/social/BlobServlet?docId=20225&langId=en>
- Stahl BC, Coeckelberg M (2018) Ethics of healthcare robotics: Towards responsible research and innovation, in: *Robotics and Autonomous Systems*, 86, 152-161.
- Tiedemann P (2006) *Was ist Menschenwürde?* Wissenschaftliche Buchgesellschaft, Darmstadt.
- von Wrangel (2017) *Polnische Pflegekräfte : Wickeln, kochen, aufpassen*, Frankfurter Allgemeine, 13.8.2017.
- Wachsmut I (2018) Robots Like Me: Challenges and Ethical Issues in Aged Care, in: *Front Psychol*. 9: 432.

SIS and the Digital Divide

Overview

The digital divide describes the disparities between those who have access to the Internet and its benefits and those who do not. This includes the divide between those who have access to SIS and those who do not (Jarrett 2017). The following table summarizes the overall challenge, the specific challenge or opportunities through SIS and the contributions from human rights instruments.

Challenge	SIS	Human Rights? Ethics?
<ul style="list-style-type: none"> 52% of the world's population do not have access to the Internet Internet access is necessary for access to the knowledge economy, including to jobs. The social digital divide increases as citizens without access to the Internet are marginalized from political participation. 	<ul style="list-style-type: none"> The technical requirements and costs for SIS are considerable. New digital divides are predicted as a limited number of companies can make full use of SIS. The global digital divide increases as SIS favour high-income regions. 	<ul style="list-style-type: none"> There is no human right to Internet access, although such access promotes other human rights (e.g. education). Non-legally binding Sustainable Development Goal 9 promotes a significant increase in universal and affordable access to the Internet in least developed countries by 2020. The world economy is seriously and life-threateningly biased towards the rich, and the digital divide increases existing inequalities with and without SIS.

What is the challenge?

Local teachers or community officials connected to the digital world in Lagos, Beijing or Calcutta can access the same electronic journals, books and databases as students at the Sorbonne, Oxford or Harvard (Norris, 2001: 7).

Pippa Norris, a Harvard political scientist, drew this picture almost 20 years ago: Harvard educational resources available to Lagos students. This is the positive side of linking the world through the Internet. The negative side is the 'digital divide'.

What does digital divide mean? "The term digital divide reached popularity in the mid-1990s as a way to describe the disparities between those who had access to the Internet and those who didn't" (Canadian Journal of Communication 2003). Originally, the divide was understood simplistically to refer only to the "physical allocation of computers and networks" (Lucey and Grant 2008). Today it is clear that:

"meaningful access to ICT [Information and Communication Technology] comprises far more than merely providing computers and Internet connection. Rather access to ICT is embedded in a complex array of factors encompassing physical, digital, human and social resources and relationships" (Warschauer 2003: 6).

Three levels of digital divide are currently distinguished at the micro-level, the level of individual people (Leaning 2017). The original difficulty of having no access to computers and no Internet connection remains at level one. In 2015, the Broadband Commission (2017: 8), a joint undertaking

from UNESCO and the UN International Telecommunication Union, pointed out that “52% of the world’s population still do not have access to the Internet”. This excludes 52% of the world population from many benefits of the knowledge economy²⁶, including SIS.

Level two refers to the necessary skills and willingness to use digital resources (ibid.). For instance, motivational indifference and lack of knowledge rather than access to computers and Internet connection explains part of the digital divide for over-55 year-olds in Europe (Peacock and Künemund 2007).

Level three refers to the way digital resources are used and for what purpose (Leaning 2017). For instance, some might use the Internet passively to stream videos, others might use it actively to sign democratic petitions (Seong-Jae 2010, Hale et al 2018). Where local government agencies seek opinions on local matters through e-consultations, those who do not participate will have no decision-making power. As a result, “social barriers will be compounded if non-electronic voices are marginalized from political participation” (Shelley et al: 46).

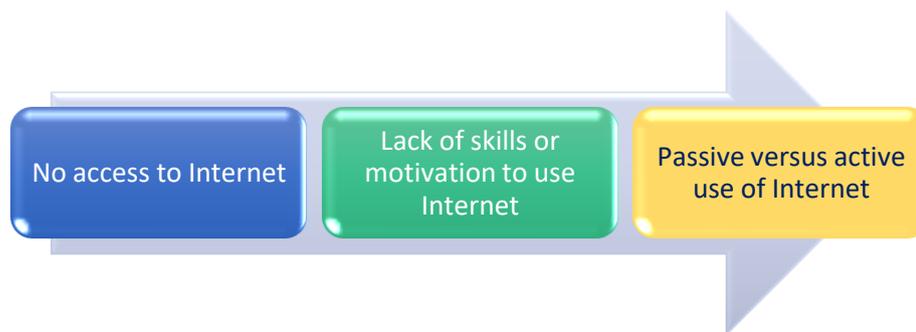


Fig. 5 – Levels of Digital Divide at the Micro-level on

At the macro-level, moving up from individual citizens to social structures, three terms have been used to describe the digital divide. Levels one and two can lead to a social digital divide. When computer skills become essential for economic success even in basic jobs (e.g. secretarial, reception), “the underclass of info-poor may become further marginalized” (Norris 2001: 68) within countries. The global digital divide describes the phenomenon that high income countries have strengthened their lead over low- and middle-income countries in the knowledge economy. “Surf at random, click on this, click on that, and whose voices do you hear around the globe?” (Norris 2001: 2). Level three, the passive versus active use of the Internet, has been described as the democratic digital divide given its potential to compound current social structures (Shelley et al: 46).

How does the digital divide play out in SIS? Of the 10 SHERPA case studies, 3 mentioned the digital divide as an ethical challenge, as follows:

Table 4 – SHERPA Case Studies on the Digital Divide (McNish et al 2019)

Field of Case Study	Digital Divide Description
Agriculture	The potential advantages of agricultural data analytics currently mostly used on large monoculture industrial farms may lead to a further growth of such farms due to the high cost of the technology (Carbonell 2016, Kosior 2017).
Advanced brain	The platforms provided through the EU-funded Human Brain Project cannot be used by all who would want to obtain access, thereby creating a digital

²⁶ The term “knowledge economy” summarizes the economic creation of wealth through “expertise, skills, experience, education, understanding, awareness, perception, and other qualities required to communicate, interpret, and analyze information. New wealth is created by the application of knowledge to improve productivity—and to create new products, services, systems, and processes” (Journal of the Knowledge Economy not dated).

research	divide.
Smart Cities	Smart information systems, for instance on traffic controls to decrease pollution, may bring positive change for some cities, but exacerbate inequalities between cities as others cannot afford the technology (Chourabi et al 2012).

All three instances of digital divide concerns raised by the SHERPA case studies refer to lack of funding to realize expensive access to SIS. A World Economic Forum publication (Bughin and van Zeebroeck 2018) emphasizes the same concerns, in particular that an artificial intelligence divide “will reinforce the digital divides that are already fuelling economic inequality and undermining competition.” Divides are predicted in three areas by Bughin and van Zeebroeck (ibid.):

First, the company level. “Innovative, leading-edge companies that fully adopt AI technologies could double their cash flow between now and 2030... Firms that do not adopt AI at all could experience a 20% decline in their cash flow as they lose market share, putting them under pressure to shed workers.”

Second, the skill level. Repetitive tasks “could fall from some 40% of total employment to near 30% by 2030” leading to higher wage differentials, as unskilled labourers compete for fewer jobs.

Third, the country level. The global digital divide “seems set to widen further. Those countries, mostly in the developed world, that establish themselves as AI leaders could capture an additional 20-25% in economic benefits compared with today”.

Are there human rights instruments to address the digital divide? In other words, is providing meaningful access to the Internet, including to SIS, a matter for human rights?

Current legal and ethical instruments

Occasionally one finds efforts at promoting a “human right to Internet access” (Tomalty 2017) or a “human right to connect” (Shearlaw 2014). However, this is misleading. Human rights “set minimum standards; they do not attempt to describe an ideal social and political world” (Nickel 2007: 10). There is no human right to access to the Internet or SIS in either hard law or soft law. However, access to the Internet and SIS can facilitate other human rights, and thereby be relevant indirectly. For instance, with regard to the human right to education, a UN resolution points out:

Emphasizing that access to information on the Internet facilitates vast opportunities for affordable and inclusive education globally, thereby being an important tool to facilitate the promotion of the right to education, while underlining the need to address digital literacy and the digital divide, as it affects the enjoyment of the right to education (United Nations 2014 emphasis added).

Another human right that is related to meaningful access to the Internet relates to unemployment. As noted earlier, basic IT skills, including Internet usage, is now a common requirement in most office jobs. Access to the Internet and the skills to make use of such access are therefore a prerequisite for avoiding unemployment. As unemployment is a separate challenge in this report, the following section will focus on the right to education and a global policy effort to reduce the digital divide.

Hard law

The Charter of Fundamental Rights of the European Union (2012), Article 14, provides for the right to education, including access to vocational and continuing training. However, Article 14 does not address the means by which education has to be delivered, e.g. the Internet or education about the

Internet to address potential skill shortages. Hence, fundamental rights charters, such as the Charter of Fundamental Rights of the European Union, take no stance on this issue.

Soft law

Of the main international legal and ethical instruments, only the non-legally binding Sustainable Development Goals (SDGs) promote access to the Internet as a major objective. In particular, one of the Goal 9 targets is to “provide universal and affordable access to the Internet in least developed countries by 2020” (UN SDG 2015). According to progress reports, by 2016, “the proportion of the population covered by a third generation (3G) mobile broadband network stood at 61 per cent in the LDCs [least developed countries] and 84 per cent globally” (UN SDG 2015a). To access SIS, high-speed fixed broadband Internet is a minimum requirement. Yet, “in 2016, only 6 per cent of the population in [low and middle income] countries had access to high-speed fixed broadband Internet” (Guterres 2018). Hence, progress, if any, is very slow.

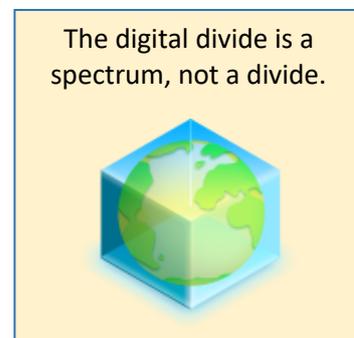
Discussion

The term digital divide suggests two parties on either side of a chasm. Due to their lack of access to the Internet, one group is seen as highly disadvantaged and without access to a wide range of opportunities. The other group is seen as highly advantaged and part of the knowledge economy and its promises, which includes access to SIS. But this picture is erroneous. One shouldn't speak of a divide or a gap, instead, in reality it is a spectrum. At one polar end are people in extreme poverty for whom even non-smart mobile phones are not accessible. This means they are excluded from opportunities of micro-credits²⁷ (Omondi 2017) or even looking for jobs (Pew Research Centre 2015). At the other end of the spectrum are company owners whose significant prosperity comes from the knowledge economy. The list of the five richest *Internet* entrepreneurs in the world is (Income diary, not dated, accessed 2019):

1. Jeff Bezos - Amazon
2. Mark Zuckerberg - Facebook
3. Larry Ellison - Oracle
4. Larry Page - Google
5. Sergey Brin - Google

Three of the above billionaires are also amongst the 10 richest people in the world (The Week 2019), with Jeff Bezos leading both lists (joined by Mark Zuckerberg and Larry Ellison). In between the two polar extremes of Internet billionaires and those suffering from extreme poverty, one can find a gigantic number of possibilities.

The digital divide is just one small characteristic in a world that distributes its opportunities extremely unfairly. According to Jeffrey Sachs: "there is enough in the world for everyone to live free of poverty and it won't require a big effort on the part of big countries to help poor ones" (Xinhua 2018). What prevents solutions is greed, he says (ibid.). "To achieve sustainable development, you have to pay for it" (ibid.). That this is not happening at a large enough scale leads to many life-threatening problems. 795 million people in the world do not have access to sufficient food (Food



²⁷ Microcredits are very small loans, given to those who are unable to obtain bank loans, for instance, because they are illiterate and cannot fill in the necessary paperwork or because they have no employment.

Aid not dated, accessed 2019). 6 million children die yearly, unnecessarily, as they could be saved by low-tech measures such as vaccines or antibiotics (Unicef not dated, accessed 2019). The digital divide, one could say, is one of the smaller characteristics of today's world that cannot be tackled independently of the "elephant in the room"²⁸. This is the fact that the world economy is seriously and life-threateningly biased towards the rich (Pogge 2001), and that lack of access to computers, the Internet and SIS is only one symptom of this divide.

References

- Broadband Commission (2017) The State of Broadband: Broadband catalyzing sustainable development, https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.18-2017-PDF-E.pdf
- Bughin J and van Zeebroeck N (2018) 'AI divides' and what we can do about them, World Economic Forum, <https://www.weforum.org/agenda/2018/09/the-promise-and-pitfalls-of-ai>
- Canadian Journal of Communication (2003) Book review of Norris P - Digital Divide? Canadian Journal of Communication, Vol. 28 (1)
- Carbonell, I (2016) "The Ethics of Big Data in Big Agriculture", Internet Policy Review, Vol. 5, Issue 1, pp. 1-13.
- Chourabi H, Nam T, Walker S, Gil-Garcia JR, Mellouli S, Nahon K, Pardo TA, Scholl HJ (2012) Understanding Smart Cities: An Integrative Framework, 45th Hawaii International Conference on System Science (HICSS), pp. 2289-2297.
- European Union (2012) Charter of Fundamental Rights of the European Union, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN>
- Food Aid (not dated) Hunger Statistics, <https://www.foodaidfoundation.org/world-hunger-statistics.html>
- Guterres A (2018) The Sustainable Development Goals Report 2018, United Nations: <https://unstats.un.org/sdgs/report/2018>
- Hale S, John P, Margetts H, Yasseri T (2018) How digital design shapes political participation: A natural experiment with social information, PloS one, 13 (4) pp: e0196068.
- Income Diary (not dated, accessed 2019) The 100 Richest Internet Entrepreneurs, <https://www.incomediary.com/rich-list>
- Journal of the Knowledge Economy (not dated) Aims and Scope, <https://www.springer.com/economics/policy/journal/13132>
- Kosior, K (2017), "Agricultural Education and Extension in the Age of Big Data", European Seminar on Extension and Education.
- Leaning M (2017) Media and Information Literacy, Chapter: Digital Divides: Access, Skills and Participation, pp: 101-114, Amsterdam: Elsevier.
- Lucey TA and Grant M (2008) Considering Dimensions of the Digital Divide, in: Kidd TT and Song H (eds) Handbook of Research on Instructional Systems and Technology, IGI-Global, pp. 869-883
- McNish, K et al. (2019) Case Studies, a report for SHERPA, available at: https://dmu.figshare.com/articles/D1_1_Case_studies/7679690
- Norris, P (2001) Digital Divide? Civic Engagement, Information Poverty and the Internet Worldwide, Cambridge University Press
- Omondi, D (2017) Why mobile phone is the next frontier for lending, Standard Digital, <https://www.standardmedia.co.ke/article/2001242101/why-mobile-phone-is-the-next-frontier-for-lending>
- Peacock SE and Künemund H (2007) Senior citizens and Internet technology: Reasons and correlates of access versus non-access in a European comparative perspective, Eur J Ageing, 6;4(4):191-200.
- Pew Research Centre (2015) Cell Phones in Africa: Communication Lifeline, Pew Global, <https://www.pewglobal.org/2015/04/15/cell-phones-in-africa-communication-lifeline/>
- Pogge T (ed) (2001) Global Justice, Oxford: Blackwells.
- Seong-Jae, M (2010) From the Digital Divide to the Democratic Divide: Internet Skills, Political Interest, and the Second-Level Digital Divide in Political Internet Use, Journal of Information Technology & Politics, 7:1, 22-35.

²⁸ The term "elephant in the room" is used to suggest that there is a difficult topic, which nobody wants to talk about.

- Shearlaw M (2014) Mark Zuckerberg says connectivity is a basic human right – do you agree?, in: The Guardian, <https://www.theguardian.com/global-development/poverty-matters/2014/jan/03/mark-zuckerberg-connectivity-basic-human-right>
- Shelley, M. C., Thrane, L. E., & Shulman, S. W. (2006). Generational differences in information technology use and political involvement. *International Journal of Electronic Government Research*, 2(1), 36–53.
- The Week (2019) Top billionaires: who is the world’s richest person today and of all time?, The Week, 5 March 2019, <https://www.theweek.co.uk/people/57553/top-billionaires-who-richest-person-world>
- Tomalty J (2017) Is There A Human Right To Internet Access? in: Philosophy Now, [https://philosophynow.org/issues/118/Is There A Human Right To Internet Access](https://philosophynow.org/issues/118/Is_There_A_Human_Right_To_Internet_Access)
- Unicef (not dated) Reduce child mortality, <https://www.unicef.org/mdg/childmortality.html>
- United Nations (2014) The promotion, protection and enjoyment of human rights on the Internet, http://hrlibrary.umn.edu/hrcouncil_res26-13.pdf
- United Nations SDG (2015) Sustainable Development Goal 9, Targets and Indicators, <https://sustainabledevelopment.un.org/sdg9>
- United Nations SDG (2015a) Sustainable Development Goal 9, Progress of goal 9 in 2018, <https://sustainabledevelopment.un.org/sdg9>
- Warschauer, M. 2003. *Technology and social inclusion: Rethinking the digital divide*, Cambridge, MA: MIT Press.
- Xinhua (2018) Greed is biggest obstacle to achieving fair societies, professor says at UN, 10 July 2018, http://www.xinhuanet.com/english/2018-07/10/c_137313107.htm

SIS and Unemployment

Overview

Unemployment has been a possible argument against technological progress since the famous Luddites destroyed machinery in 19th century England to protest against job losses. Since then Luddites are portrayed by some as heroes, by others as villains (Wasserstrom 1987). Automation through robots also creates the fear of unemployment (Dekker et al 2017). The following table summarizes the overall challenge in context (i.e. looking at broader challenges in the world of work), provides the possible challenges through automation as well as the contributions from human rights instruments.

Challenge	SIS	Human Rights? Ethics?
<ul style="list-style-type: none"> The world of work includes considerable injustices such as child labour, trafficking, abuse and harassment. Unemployment, a major challenge in the world of work, can lead to serious poverty-related problems. 	<ul style="list-style-type: none"> Possible displacement through robots could lead to unemployment-related poverty and health risks. There is considerable uncertainty on the impact of automation and robot use on unemployment. At the same time, job displacements are predicted to occur across the work spectrum, including in jobs that appeared safe to date. 	<ul style="list-style-type: none"> Strictly speaking, human rights legislation does not guarantee jobs, only equal access to jobs in the EU and access to social security in the case of unemployment. The non-legally binding Sustainable Development Goals specifically aim towards “full and productive employment and decent work for all” (United Nations 2015).

What is the challenge?

The biggest human rights challenges in the context of work today can be divided into two categories.

1. Obviously unethical conduct, which is particularly harmful to vulnerable populations, and
2. Unwanted consequences of otherwise potentially positive developments.

The first category can be broadly described as exploitation; the second category is usually associated with new technologies such as Smart Information Systems (SIS)²⁹. An example list of each is provided in Table 1. For the new technologies, robots are used as an example.

Table 5 – Major Human Rights Challenges in the World of Work

Exploitation in work	Unwanted side-effects of robot use
Child labour (ILO not dated)	Unemployment (Walsh 2017)
Human trafficking for work, including sex trafficking (Zimmermann and Kiss 2017)	De-humanisation and “cold” care (Stahl and Coeckelbergh 2016)

²⁹ SIS can, of course, also be used in the human rights challenges of the first type, for instance when predictive risk intelligence data is illegally accessed and used by traffickers. However, this is indirect impact, whilst the challenge in the second category is direct.

Harassment and abuse in the workplace (Okechukwu et al 2014)

Labour without health and safety precautions (BBC 2019)

The main difference between the two categories is that the second category *could* be beneficial in some contexts. For instance, what some might call unemployment, others might call increased leisure, lower workloads, fewer menial tasks or even addressing a shortage of skilled labour (Pooler 2017). Or what some might call loss of human contact through work, others might call leaving incontinence in care homes to robots and gaining time for conversations with the elderly. This is not possible with category 1. The problems in category 1 are unacceptable and they have a strong legal dimension existing at the international and EU level.

Can we then already conclude that the problems in category 2 are much less urgent than the problems in category 1? On a world scale, yes. However, that some face even bigger problems than others, does not resolve the problems for the latter. For instance, child poverty in the UK can be caused by parental unemployment and mean: “being cold, going hungry, not being able to join in activities with friends... [and having] complicated health histories over the course of a lifetime” (Child Poverty Action Group 2018). Hence, unemployment due to automation and robot use can have devastating effects on individuals or families.

At the same time, consequences for workers from automation through robots are hard to predict. The increase of robot shipments certainly seem to indicate large-scale automation in high-income regions and emerging economies, see Figure 1 (Source: [Executive Summary World Robotics 2017 Industrial Robots](#)).

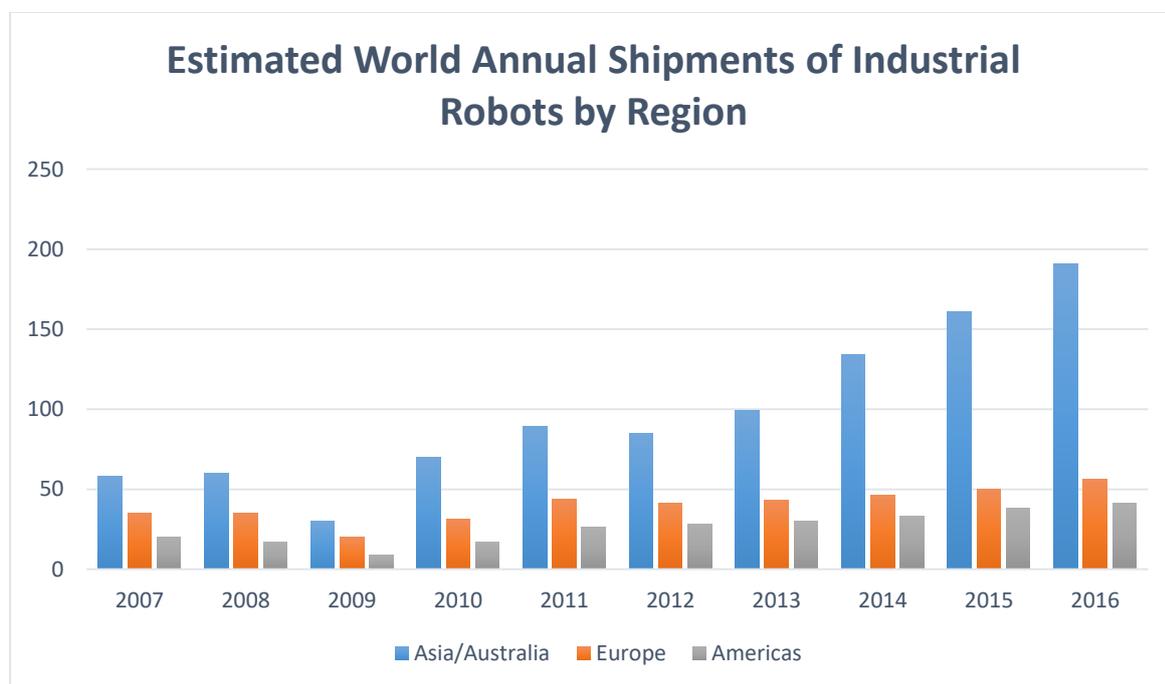
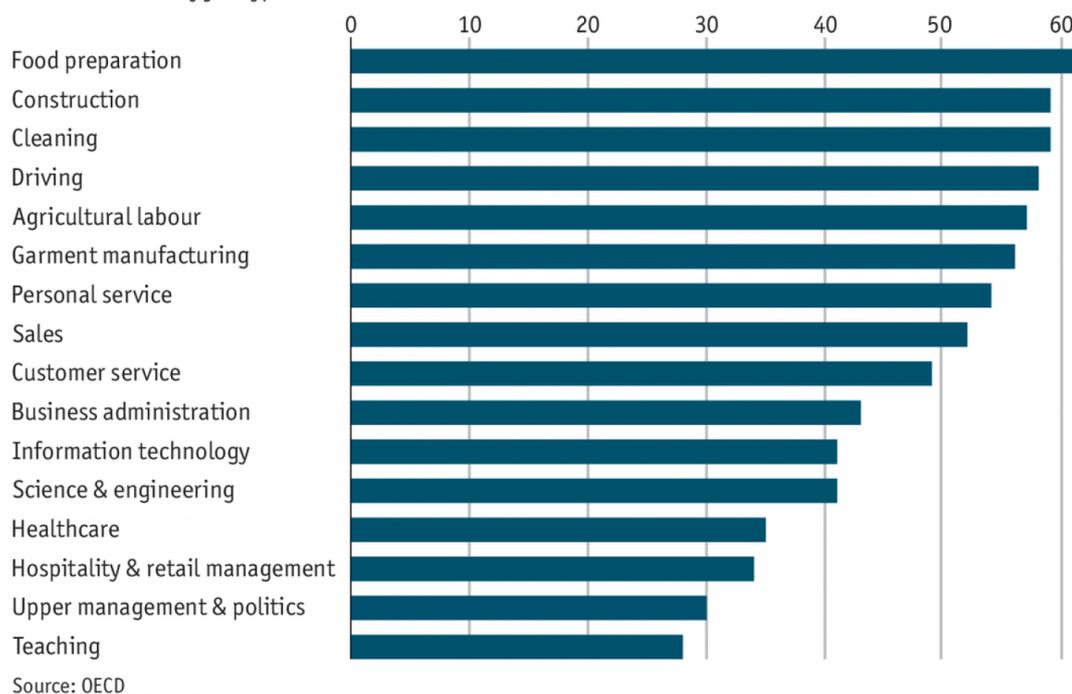


Fig. 6 – Estimated World Annual Shipments of Industrial Robots by Region

Yet whether this translates into large-scale job losses is unclear. For instance, the World Economic Forum “predicts that robots will displace 75 million jobs globally by 2022 but create 133 million new ones” (BBC 2018). At the same time, some labour sectors are much more at risk of unemployment and displacement caused by robots than others. Figure 2 summarizes the loss of job risk by employment sector (Source, Economist 2018).

Automated for the people

Automation risk by job type, %



Economist.com

Fig. 7 – Automation Risk by Job Type

Can current legal and ethical instruments protect against job displacement through robots?

Current legal and ethical instruments

Even though there is no right to employment as such, there is a right to work under equal conditions in the EU. The Treaty on the Functioning of the EU provides a whole Chapter on the rights of workers within the context of the freedom of movement, based on the principle of the free movement of workers (Article 45 TFEU) and other factors of production (goods, services, capital). The free movement of workers in the EU entails equal access to work free from discrimination and the right to:

1. accept job offers;
2. move freely within the EU for this purpose;
3. stay in the host Member State for the purpose of employment, in the same conditions as the ones governing the employment of nationals of that State; and
4. to remain in the territory of the Member State after employment, subject to secondary legislation at the EU level.

Applicable secondary legislation includes the Workers' Regulation³⁰ and the EU Citizens Directive³¹ which spell out the scope of the right to employment in the EU and social welfare associated with it, as interpreted by the Court of Justice of the European Union (CJEU). The right of workers extends to moving to another Member States and/or staying there under certain conditions in search for a job.

³⁰ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011R0492>

³¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004L0038>

These measures can help towards mitigating the problem of unemployment, as far as EU citizens are concerned, as a larger pool of jobs is available to those who are mobile.

At the international level, human rights texts such as Articles 23 and 24 of the Universal Declaration of Human Rights (UDHR) (United Nations 1948) demand protection against unemployment, equal pay for equal work, just remuneration, and a right to rest and leisure.

At the EU level, the Charter of Fundamental Rights of the European Union provides more details on the work context than the Universal Declaration of Human Rights, for instance on unjustified dismissal. Like the UDHR, the Charter does not include a right to employment, but only an entitlement to social security in the case of unemployment.

Hence, a displaced worker who is covered by the Charter and whose job is now undertaken by a robot has, within the EU, a right to social security benefits and social services, but this does not alleviate the unemployment problem, only its poverty-related and livelihood aspects. This is potentially problematic, as work can have many other benefits in addition to remuneration, including self-respect and happiness (Csikszentmihalyi 2004), assuming that the work is not tedious, repetitive and irrelevant (Macaro and Baggini 2011).

Soft law

Of the main international legal and ethical instruments, only the non-legally binding Sustainable Development Goals (SDGs) promote the creation of jobs as a major objective. Goal 8 (United Nations 2015) targets include:

Promote development-oriented policies that support productive activities, decent job creation, entrepreneurship, creativity and innovation, and encourage the formalization and growth of micro-, small- and medium-sized enterprises, including through access to financial services.

Ambitiously, the SDGs want to “achieve full and productive employment and decent work for all women and men, including for young people and persons with disabilities” by 2030 (ibid.) How does this relate to automation and robots?

Discussion

New technologies such as SIS can have both positive *and* negative challenges or impacts. Hence, these challenges need to be governed well rather than eliminated. For instance, The World Economic and Social Survey 2018 (United Nations 2018) notes that “automation, robotics, electric vehicles, renewable energy technologies, biotechnologies and artificial intelligence... possess immense potential for fostering growth, prosperity and environmental sustainability”. But at the same time, “growing unemployment, underemployment and inequality” might be their result (ibid.).

Most worrisome will be the impact of unemployment on two groups. First, those who are already precariously close to the group of underemployed individuals and families for whom SDG 8 was developed. Unemployment might move them into serious poverty. Second, negative impacts are expected for the currently well-off middle classes due to Moravec’s paradox (Elliott 2017).

It is comparatively easy to make computers exhibit adult-level performance on intelligence tests or playing checkers, and difficult or impossible to give them the skills of a one-year-old when it comes to perception and mobility. Put another way, if you wanted to beat Magnus

Due to Moravec’s paradox, the middle classes might be affected through SIS related unemployment.



Carlsen, the world chess champion, you would choose a computer. If you wanted to clean the chess pieces after the game, you would choose a human being.

If Moravec's paradox is true, the future of work with high numbers of robots could mean that ingenious proposals for SDG Goal 8 would be required across the board, not just for the poor, but also for the middle classes in high-income regions.

Such solutions will not be driven by the law nor by an insistence on human rights; they will have to be driven by human ingenuity combined with a sense of solidarity (Leisinger 2018, de Waal 2009: 187-191). This is particularly so as automation is likely to add downward pressure on salaries (OECD 2018). The sense of solidarity necessary to combat unemployment related problems might develop more strongly if those currently unaffected by unemployment face this possibility in the future.

When Deputy Secretary-General of the United Nations, Amina Mohammed, opened a meeting about the SDGs and Robots, she started a conversation with Sophia, an advanced robot. Sophia suggested that the world's existing resources, such as food and energy, need to be redistributed to solve the problems the SDGs address (Lebada 2017).

References

- BBC (2018) WEF: Robots 'will create more jobs than they displace', <https://www.bbc.com/news/business-45545228>
- BBC (2019) Textile sector 'rife' with exploitation and underpayment, <https://www.bbc.com/news/business-46992499>
- Child Poverty Action Group (2018) Child poverty facts and figures, <http://www.cpag.org.uk/content/child-poverty-facts-and-figures>
- Csikszentmihalyi M (2004) Flow, the secret to happiness, Ted Talk, https://www.ted.com/talks/mihaly_csikszentmihalyi_on_flow?language=en
- Dekker F, Salomons A, van der Waal J (2017) Fear of robots at work: the role of economic self-interest, *Socio-Economic Review*, 15 (3) 539–562.
- de Waal F (2009) *The Age of Empathy*, New York: Random House.
- Economist (2018) A study finds nearly half of jobs are vulnerable to automation, <https://www.economist.com/graphic-detail/2018/04/24/a-study-finds-nearly-half-of-jobs-are-vulnerable-to-automation>
- Elliott L (2017) Robots will not lead to fewer jobs – but the hollowing out of the middle class, in: *The Guardian*, 20 Aug 2017, <https://www.theguardian.com/business/2017/aug/20/robots-are-not-destroying-jobs-but-they-are-hollow-out-the-middle-class>
- European Union (2012) Charter of Fundamental Rights of the European Union, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN>
- ILO (not dated) Child Labour, <https://www.ilo.org/ipec/facts/lang--en/index.htm>
- Lebada AM (2017) Second Committee Considers Role of AI in Advancing SDGs, IISD, <https://sdg.iisd.org/news/second-committee-considers-role-of-ai-in-advancing-sdgs/>
- Leisinger K (2018) *Die Kunst der verantwortungsvollen Führung. Vertrauen schaffendes Management im internationalen Business*, Bern: Haupt.
- Macaro A and Baggini J (2011) Is it important to work: in: *Financial Times*, 21 Oct 2011, <https://www.ft.com/content/18ffbe2e-f9dd-11e0-9c26-00144feab49a>
- OECD (2018) Policy Brief on the Future of Work, March 2018, <https://www.oecd.org/employment/Automation-policy-brief-2018.pdf>
- Okechukwu CA, Souza K, Davis KD, de Castro AB (2014) Discrimination, Harassment, Abuse and Bullying in the Workplace: Contribution of Workplace Injustice to Occupational Health Disparities, in: *Am J Ind Med*. 57(5): 573–586.
- Pooler M (2017) Robot army is transforming the global workplace, in: *Financial Times*, 20 Nov 2017, <https://www.ft.com/content/f04128de-c4a5-11e7-b2bb-322b2cb39656>
- Stahl BC and Coeckelbergh M (2016) Ethics of healthcare robotics: Towards responsible research and innovation, in: *Robotics and Autonomous Systems*, Vol86, pp.152-161.

- United Nations (1948) Universal Declaration of Human Rights, <https://www.un.org/en/universal-declaration-human-rights/>
- United Nations (2015) Sustainable Development Goal 8, Targets, <https://www.un.org/sustainabledevelopment/economic-growth/>
- United Nations (2018) World Economic and Social Survey 2018, https://www.un.org/development/desa/dpad/document_gem/wess-report/
- Walsh, T (2017) Will robots bring about the end of work? in: The Guardian, 1 Oct 2017, <https://www.theguardian.com/science/political-science/2017/oct/01/will-robots-bring-about-the-end-of-work>
- Wasserstrom J (1987) "Civilization" and Its Discontents: The Boxers and Luddites as Heroes and Villains, Theory and Society, 16 (5) 675-707.
- Zimmerman C, Kiss L (2017) Human trafficking and exploitation: A global health concern. PLoS Med 14(11): e1002437.

SIS and Privacy and Data Protection

Overview

Despite the numerous attempts that have been made to give a universal definition to privacy, its concrete form highly depends on the societal characteristics and the economic and cultural circumstances of each country. Moreover, technological and scientific developments and field of application can also affect the definition of privacy and how it is protected. As a result, the umbrella term of 'privacy' must be interpreted with regards to the context and circumstances present at the time (Lukács, 2016).³² The right to privacy can be broadly defined as a person's right to control access to his or her personal information, while personal data have been defined as any information that relates to an **identified or identifiable living individual**.³³

The right to privacy can be broadly defined as a person's right to control access to his or her personal information.



What AI brings to the table is the ability to gather, analyse, and combine vast quantities of data from different sources, thus increasing the information-gathering capabilities of social actors that use this technology. The potential impact of AI on privacy is immense, which is why it is imperative to raise awareness about these issues.³⁴

More specifically, AI entities and software are increasingly used in information gathering and processing, especially for huge quantities of data, because of three main reasons: their speed of analysing data, the scale of data that can be processed in a reasonable amount of time and the automation of AI entities, which can perform the tasks assigned without necessarily being supervised.

The Case Studies developed in by Sherpa come to illustrate this point (Deliverable 1.1³⁵). In the context of the employment relation, the surveillance (monitoring and tracking) of employees as well as the changing nature of the labour market have been identified as legal and social challenges triggered or aggravated by SIS throughout the world (Case Study (CS) 1). The type of data stored and used by IoT data software or cloud-based tracking services raise issues around privacy but also of access, malicious use, transparency and trust. Surveillance ('dataveillance', geosurveillance) conducted by national authorities and governments as part of their SIS governance and urban management strategies raise serious concerns around privacy, security, accuracy and data ownership (CS2). The line between public and private interests appears blurred in a technological lock-in influencing the use of SIS in governmental applications. This is also illustrated in the Case Study on Sustainable Development for smart cities and public spaces where there is an emphasis on the engagement of stakeholders and not only national authorities (CS4). SIS as applied by sciences to

³² Adrienn Lukács, 'WHAT IS PRIVACY? THE HISTORY AND DEFINITION OF PRIVACY' In: Keresztes, Gábor (éd.):Tavaszi Szél 2016 Tanulmánykötet I., Budapest: Doktoranduszok Országos Szövetsége, 2016, pp. 256-265 <<http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf>>

³³ Article 4 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

³⁴ <https://towardsdatascience.com/ai-and-the-future-of-privacy-3d5f6552a7c4>; See also, SIENNA, *D4.1 State of the Art review, AI and robotics*, 2018

³⁵ McNish, K et al. (2019) Case Studies, a report for SHERPA, available at: https://dmu.figshare.com/articles/D1_1_Case_studies/7679690

the human body, and brain in particular, raise fundamental legal and ethical issues involving privacy, confidentiality and accountability but also multiple other challenges as previously identified (CS5).

All economic sectors, agricultural (CS3), industrial and services, are revolutionized by SIS and must adjust. The Case Study on insurance outlines this transition well as this sector traditionally handles a huge amount of data, of different types, which are now created/used/treated in a digital environment (CS6). Concepts such as bias, reliability or fraud detection take a new meaning in this context. The Case Study on energy and utilities supplies reinforces the feeling of lack of privacy and mistrust among citizens and consumers (CS7), the one on communications the feeling of vulnerability (CS8), the one on trade the feeling of manipulation (CS9) and the one on manufacturing and predictive risk intelligence the feeling of mis-/dis-identification and mis-/dis-information affecting one's privacy and integrity (CS10).

Thus, in spite of the increasing efficiency provided by SIS and advanced AI entities,³⁶ they pose multiple and serious challenges to privacy. The most important challenge faced is internet users' **data breaches, including the exploitation and misuse of data of individuals**. These data could include the information gathered by smartphones e.g., location, internet search history, biometric data, finances and metadata (information on the data), such as the time and recipient of a text message.³⁷ They can then be used to identify a person's background, gender, social connections and health. The case of Cambridge Analytica, which was introduced in the introduction, is undoubtedly an example of unethical exploitation of data.

Millions of consumers already carry autonomous learning assistants in their pockets, wherever they go, as their smartphones contain autonomously learning assistants called Google Assistant or Siri.



In this case Aleksandr Kogan reportedly created an app called "thisisyourdigitallife" that ostensibly offered personality predictions to users while calling itself a research tool for psychologists.³⁸ This app was asking users to log in with their Facebook account and to access the users' Facebook profiles, locations, what they liked on the service and their friends' data as well. Kogan then sent the data to Cambridge Analytica without the users' permission which were allegedly used for targeted political ads in the UK's Brexit referendum campaign, as well as by Trump's team during the 2016 US election.³⁹

Implications of the use of AI on personal data also increasingly affect the **privacy of consumers**, through the use of Algorithmic Decision Making (automated decision-making) in their everyday lives. Several companies have developed home assistant systems that use voice recognition to autonomously perform tasks that consumers would otherwise do when sat at a computer or smartphone. Indeed, millions of consumers already carry autonomous learning assistants in their pockets, wherever they go, as their smartphones contain autonomously learning assistants called Google Assistant or Siri (developed by Apple). Such machine-learning applications that have access to some of the most private parts of consumers' lives should be particularly respectful of consumers' privacy. In 2017, the Federation of German Consumer Organisations (vzbv) analysed the voice controlled personal assistant 'Amazon Echo' and found that the device was recording far more conversation than the

³⁶ AI entities which develop more advanced artificial intelligence empowering them to machine learning.

³⁷ <https://theconversation.com/smartphone-data-tracking-is-more-than-creepy-heres-why-you-should-be-worried-91110>

³⁸ <https://www.cbsnews.com/news/aleksandr-kogan-the-link-between-cambridge-analytica-and-facebook-60-minutes/>

³⁹ <https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/>; <https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf>

user intended as it reacted not only to the activating code word “Alexa” but also to similar words. The same has been found to be true for Google Assistant.⁴⁰

Lastly, apart from the exploitation and misuse of personal data, the fact that **AI entities and software do not forget data the way humans do**, is another challenge faced. Information stored in a database exists in various locations. When permanent deletion of some data is requested, these locations must be identified and overwritten with random information. Therefore, even if no dishonest exploitation takes place, the data subjects of these data must be granted the so-called right to be forgotten.

Current legal and ethical instruments (split in values and principles)

The right to privacy has been protected in the EU under Article 8 of the ECHR and later on under Article 7 of the Charter of Fundamental rights which state that the right to privacy is a fundamental human right. Everyone has the right for his/her private and family life, home and correspondence to be respected, and the right to protect oneself against such unlawful interference. The development of the right to privacy was associated with innovation and technology which lead to the creation of the right to data protection under Article 8 of the Charter. Importantly, in 2018 the EU General Data Protection Regulation (GDPR) entered into force. It constitutes one of the most important changes in data privacy regulation in the last 20 years.⁴¹ The GDPR has fundamentally reshaped the way in which data is handled across every sector, from healthcare to banking and beyond,⁴² and has arguably contributed to solving part of the challenges identified above, including the **exploitation and misuse of data of individuals** and adverse impacts on the **privacy of consumers**.

One of the objectives of the GDPR was to harmonise data protection rules throughout the Union and although the Regulation is directly applicable to the national legal systems of the Member States, all of them proceeded to implementing the Regulation into national law, primarily because it provides for exceptions within the Articles that the Member States ‘shall’ and ‘may’ carve out in certain areas.

In particular, all Member States had an obligation to notify to the Commission the transposition of the provisions on data protection authorities (Article 51(4)), on penalties (Article 84(2)) and on reconciling the right to data protection with the right to freedom of expression and information (Article 85(3)). At the same time in case a Member State implemented into the national laws the processing of personal data in the employment context (Article 88(3)), the obligations of secrecy (Article 90(2)), the limitations to the transfer of specific categories of data for important reasons of public interests (Article 49(5)) and/or provisions on other legal remedies instead of administrative fines (Article 83(9)), notification to the Commission was necessary.⁴³ By May 2018, when the GDPR went into effect all the 28 Member States as well as Iceland, Norway and Liechtenstein implemented the Regulation into their national laws and since then 30 different EEA Supervisor

Under the GDPR, companies must have users’ permission, given via a clear affirmative action, before they can receive their personal data or override their privacy preferences.



⁴⁰ Opinion of the European Consumer Consultative Group, Policy Recommendations for a Safe and Secure Use of Artificial Intelligence, Automated Decision-Making, Robotics and Connected Devices in a Modern Consumer World (16 May 2018) 12

⁴¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

⁴² <https://eugdpr.org/>

⁴³ https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications_en

Authorities have registered a total amount of at least 281 cases with cross-border component in the Internal Market Information system.⁴⁴

Accordingly, Article 5 of the GDPR lists the principles relating to processing of personal data. One of the GDPR's core principles is that of data minimisation under which only "adequate, relevant and limited" personal data can be processed in relation with the purposes of processing. In other words, it requires that the purpose of collecting and using the data must be clearly defined, delimited and stated. As a result, feeding every piece of personal data absorbed by tracking consumers online into algorithms of different sorts and for all kinds of purposes would not be compatible with the purpose limitation principle (Eduard Fosch Villaronga, 2017). Moreover, Article 5 holds that the personal data must be processed in a transparent manner in relation to the data subject. Additionally, Article 6 of the GDPR enumerates the different grounds on which the data processing will be lawful such as the data subject's prior and informed consent, the performance of a contract or for the purposes of the legitimate interests pursued by the controller.⁴⁵

In practice, under the GDPR, companies must have users' permission, given via a clear affirmative action, before they can receive their personal data or override their privacy preferences. In addition, personal data sought by a business must be specified contractually and must be necessary for the service it provides. With regards to the case of Cambridge Analytica discussed above, Facebook has confirmed that CA may have collected private messages as well, apart from pooling information from users' friends. Such data was not needed for users to complete personality tests on the quiz app, and taking it would have breached GDPR rules.⁴⁶ The regulation also requires that companies inform the relevant data protection authority should a breach occur affecting individual rights and freedoms within 72 hours of being made aware of it. Facebook has admitted that it first learnt data was being handled improperly by Aleksandr Kogan, who developed the quiz app, and CA in 2015 — two years before it was exposed publicly and brought to authorities' attention.⁴⁷ Under the GDPR, such an infraction would incur a penalty equal to 2% of the social network's annual worldwide revenue (\$813 million in 2017).

At the same time the judgments of the Court of Justice have been guiding the application of the provisions of both primary and secondary legislation and have developed the right to be forgotten. In particular, the importance of the so-called right to be forgotten increased alongside the general rise of privacy law and it essentially constitutes the concept that individuals have the right to request that their data, collected by others, be deleted (Eduard Fosch Villaronga, 2017).

In *Google Spain SL* in 2014,⁴⁸ the Court of Justice ruled that, according to the Article 4(1)(a) of the Data Protection Directive 95/46 EC,⁴⁹ the Directive applies to search engine operators if one or more of the following three conditions are met:

- 1) if they have a branch/subsidiary in a Member State which promotes the selling of advertising space offered by the search engine to the inhabitants of that Member State;
- 2) if the parent company designates a subsidiary company in a Member State and it is responsible for two filing systems concerning data from the data subjects of such Member State; or

⁴⁴ First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities (2019), https://edpb.europa.eu/sites/edpb/files/.../19_2019_edpb_written_report_to_libe_en.pdf

⁴⁵ <https://www.avocats-mathias.com/technologies-avancees/artificial-intelligence-gdpr>

⁴⁶ <https://www.euronews.com/2018/04/11/could-eu-s-new-data-protection-law-have-stopped-cambridge-analytica-scandal->

⁴⁷ <https://www.avocats-mathias.com/technologies-avancees/artificial-intelligence-gdpr>

⁴⁸ Court of Justice (2014) C-131/12 *Google Spain SL, Google Inc v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*

⁴⁹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

- 3) if the branch/subsidiary forwards to the non-EU parent company located outside the EU any requests and requirements from the data subjects or from authorities in charge of surveilling the data protection right even if these forwards are engaged in voluntarily (Eduard Fosch Villaronga, 2017).

According to the Court, if at least one of these conditions is met, the search engine company in examination will qualify as a data controller which in practice meant that search engine companies including Google Spain can be asked by the Court to remove links that contained personal information about the data subjects. Formally recognising this right under Article 17 of the GDPR, signifies democratising something private companies were exploiting at users' expenses (Eduard Fosch Villaronga, 2017). It also results in a more general obligation towards the protection of privacy that was only covered partially by some existing sector-specific rights.⁵⁰

The right to be forgotten is further discussed in the case of *Google v CNIL* which is currently pending before the Court of Justice.⁵¹ The preliminary ruling arose, when Google failed to comply with the French Commission's request to remove links to web pages from the list of results displayed following a search performed on the basis of that person's name. Among the questions that the Court of Justice has been called to examine is that of the extraterritoriality of the right to be forgotten. AG Maciej Szpunar in his Opinion on the case insisted that search requests made outside the EU should not be affected by the de-referencing of search results.⁵² In view of the AG, a broader interpretation could create significant limitations in access to information, and as such should be approached with caution. Considering the facts of the case, worldwide de-referencing duty did not appear justified. On the other hand, AG Szpunar supported a rather broad territorial scope of de-referencing within the EU. Specifically, according to the opinion, "once a right to be forgotten within the EU has been established, the operator of the search engine should take all measures available to it to ensure full and effective de-referencing within the EU", including by use of 'geo-blocking' in respect of an IP address located in the EU, irrespective of the domain name used by the internet user.⁵³ The awaited judgment of the Court of Justice will reveal whether the view of the AG is shared by the judges.

Discussion

Major steps have been taken at the EU level from the EU institutions including the Court of Justice, in the field of privacy law towards reinforced protection of personal data that significantly improved the pre-existing legal framework. Apart from the GDPR and the proposals made under the Digital Single Market strategy,⁵⁴ an AI ethics guidance was developed by the European Commission, which *inter alia* stresses the fact that privacy and data protection must be guaranteed at "all stages of the life cycle of the AI system", including all data provided by the user and the information generated about the user over the course of his interactions with the AI system (e.g., outputs that the AI system generated for specific users, how users responded to particular recommendations, etc.) (High-Level Expert Group, 2018).⁵⁵ This is due to the fact that digital records of human behaviour can reveal highly sensitive data, not only in terms of preferences, but also regarding sexual orientation,

⁵⁰ E.g. bankruptcy law already offered debtors a fresh start through the forgiveness of debts and criminal law.

⁵¹ Request for a preliminary ruling from the Conseil d'État (France) lodged on 21 August 2017 — *Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)* (Case C-507/17)

⁵² Opinion of Advocate General Szpunar delivered on 10 January 2019, *Google (Portée territoriale du déréférencement)*, C-507/17, ECLI:EU:C:2019:15, para. 46

⁵³ Opinion of Advocate General Szpunar delivered on 10 January 2019, *Google (Portée territoriale du déréférencement)*, C-507/17, ECLI:EU:C:2019:15, para. 74

⁵⁴ <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market#TheStrategy>

⁵⁵ The European Commission's High-Level Expert Group on Artificial Intelligence Draft Ethics Guidelines for Trustworthy AI, Brussels, 18 December 2018, 17

age, gender, religious and political views and the person in control of such information could take advantage of it.⁵⁶ The guidelines therefore stress the fact that “organisations must be mindful of how data is used and might impact users and ensure full compliance with the GDPR as well as other applicable regulation dealing with privacy and data protection”.⁵⁷

Privacy is a fundamental human right, although not an absolute one. This means that it can be limited provided this is necessary, proportionate and in the public interest, in legislation or otherwise. Public interest and economic interests are two distinct concepts responding to different ethical and legal spheres. In the field of SIS, these two spheres are increasingly overlapping, with the result that a single set of rules addressing all stakeholders is necessary, particularly data processors, controllers, economic actors and/or relevant authorities. The GDPR is a step in the right direction, which applies to “the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not” and of “data subjects who are in the Union by a controller or processor not established in the Union”.⁵⁸ Encouraging the development of SIS research and development as well as just and transparent technologies is on the other hand crucial in today’s global modern world. The development of jurisprudence as well as other instruments of soft law such as codes of conduct and guidelines is thus necessary, at the European and international level. A humane consideration of SIS education at all levels is necessary, also encompassing the modern labour market, as well as widening the public debate through the involvement of observatories.⁵⁹

Digital records of human behaviour can reveal highly sensitive data, not only in terms of preferences, but also regarding sexual orientation, age, gender, religious and political views.



References

- Court of Justice (2014) C-131/12 Google Spain SL, Google Inc v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Lukács A, ‘WHAT IS PRIVACY? THE HISTORY AND DEFINITION OF PRIVACY’ In: Keresztes, Gábor (éd.):Tavaszi Szél 2016 Tanulmánykötet I., Budapest: Doktoranduszok Országos Szövetsége, 2016, pp. 256 265 <<http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf>>
- Opinion of Advocate General Szpunar delivered on 10 January 2019, *Google (Portée territoriale du déréférencement)*, C-507/17, ECLI:EU:C:2019:15
- Opinion of the European Consumer Consultative Group, Policy RECOMMENDATIONS FOR A SAFE AND SECURE USE OF ARTIFICIAL INTELLIGENCE, AUTOMATED DECISION-MAKING, ROBOTICS AND CONNECTED DEVICES IN A MODERN CONSUMER WORLD (16 May 2018) 12
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

⁵⁶ Ibid

⁵⁷ Ibid

⁵⁸ Article 3 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

⁵⁹ See <http://www.senat.fr/notice-rapport/2016/r16-464-1-notice.html>

The European Commission's High-Level Expert Group on Artificial Intelligence Draft Ethics Guidelines for Trustworthy AI, Brussels, 18 December 2018, 17

Villaronga E F, Kieseberg P, Li T, 'Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten' (2017) Computer Security & Law Review (Forthcoming)

<http://www.senat.fr/notice-rapport/2016/r16-464-1-notice.html>

<https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market#TheStrategy>

<https://eugdpr.org/>

<https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf>

<https://theconversation.com/smartphone-data-tracking-is-more-than-creepy-heres-why-you-should-be-worried-91110>

<https://towardsdatascience.com/ai-and-the-future-of-privacy-3d5f6552a7c4>

<https://www.avocats-mathias.com/technologies-avancees/artificial-intelligence-gdpr>

<https://www.cbsnews.com/news/aleksandr-kogan-the-link-between-cambridge-analytica-and-facebook-60-minutes/>

<https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/>

<https://www.euronews.com/2018/04/11/could-eu-s-new-data-protection-law-have-stopped-cambridge-analytica-scandal->

https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications_en

https://edpb.europa.eu/sites/edpb/files/.../19_2019_edpb_written_report_to_libe_en.pdf

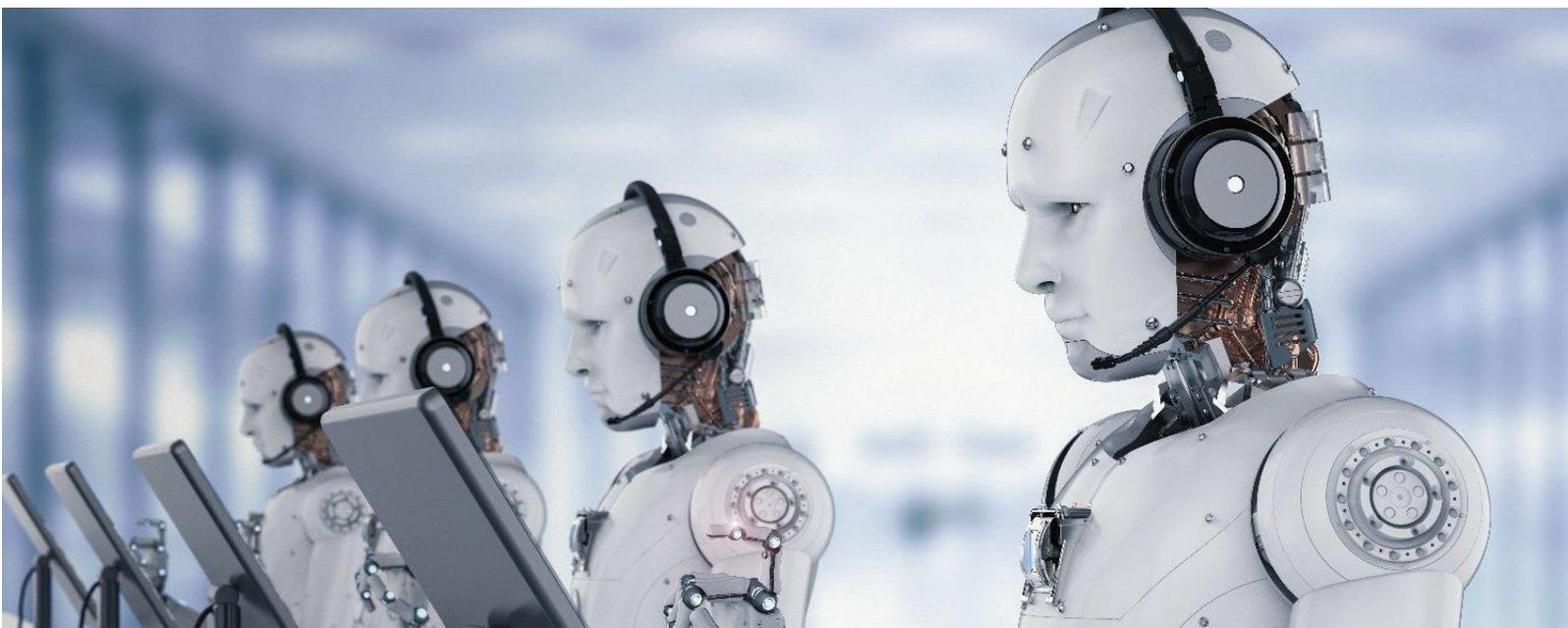
SIS and Accountability and Liability

Overview

AI products are already increasingly provided in the market and thus questions of liability, responsibility and accountability need to be given a new/updated definition. Similar concerns have been recently raised at the national level, such as in the House of Lords (House of Lords Report, 2017). Professor Reed, highlighted that law should be applied to humans: “you never apply law to technology; you always apply law to humans and the way they use technology, so there will always be someone who is using the algorithm on whom responsibility can be placed” (House of Lords Report 2018). However, based on impressive technological advances of the last decade, not only are today's robots able to perform activities which used to be typically and exclusively human, but the development of certain autonomous and cognitive features (e.g., the ability to learn from experience and take quasi-independent decisions) has made them more similar to agents that interact with their environment and are able to alter it significantly. Within this context the legal responsibility arising through a robot's harmful action becomes a crucial issue whereby the more autonomous robots are, the less they can be considered to be mere tools in the hands of other actors such as the manufacturer, the operator, the owner or the users.⁶⁰ Issues of accountability and responsibility therefore arise in multiple directions, where AI systems are also considered as actors and/or subjects in their own right.

Current legal and ethical instruments (split in values and principles)

The liability/accountability framework that currently exists within the EU legal order governing digital technologies products and services is a stable framework that encourages the fundamental freedoms as applied to innovation and investment. The **Product Liability Directive** provides for liability of producers of defective products that cause damage to natural persons or their property.⁶¹ It establishes a liability of producers when defective products cause damages to victims (including personal injuries or death or damage to property). This is a strict liability regime, in that the injured person does not have to prove a fault of the producer and carries the burden of proof of the defect in the product, the actual damage and the causal link between the defect and the damage.⁶² As far as the technology items causing a damage are 'movable' and any other item containing intangible elements or presenting connectivity features qualifies as 'product', they can be covered by the Product Liability Directive.



However, advanced robots or empowered devices, in the sense that they have increased capabilities to interpret the environment, execute actions autonomously and are less dependent on other actors (i.e., the manufacturer, the owner, the user, etc.), raise questions of liability where the damage caused by a machine cannot be linked to a defect or a human wrongdoing. In other words, the more autonomous robots are, the less they can be considered as mere tools in the hands of other actors. Consequently, questions arise as to whether:

- i. the ordinary rules on liability are sufficient/adequate and/or whether there is a need for renewed principles and rules addressing the legal liability of actors or guardians involved directly or indirectly in the acts and omissions of robots,⁶³ in the event that the harm/cause cannot be traced back to a specific human actor,
- ii. whether harmful acts or omissions of robots can be mitigated or avoided altogether, and
- iii. whether a test would need to be established to determine the changing relationship between AI actions and human beings.⁶⁴

Studies are therefore needed in the field. For instance, the work of an Expert Group on "Liability and New Technologies" aims to provide the European Commission with expertise on the applicability of the Product Liability Directive to traditional products, new technologies and new societal challenges.

In terms of safety, the **Machinery Directive** aims at the free market circulation on machinery and at the protection of workers and consumers using such machinery. It defines essential health and safety requirements of general application, supplemented by a number of more specific requirements for certain categories of machinery.⁶⁵ Machinery consists of an assembly of components, at least one of which moves, joined together for a specific application,⁶⁶ while the Directive only applies to products to be placed on the EU market for the first time.

Another Directive falling under the EU safety framework is the **General Product Safety Directive** that aims to ensure that only safe consumer products are placed on the market and acts as a safety net for products and risks not covered by the harmonisation legislation.⁶⁷ Therefore, the AI robots and autonomous self-learning systems currently emerging should meet the essential health and safety requirements laid down in the applicable EU safety legislation ensuring a single market for a wide range of equipment and machines. As such, the appropriateness of the concept of the liability of the guardian for AI entities can also be assessed within the context of the safety legislation. In particular, although autonomous AI systems cannot be assimilated to humans or animals, the autonomy element possessed by numerous AI robots is a fundamental feature which is relevant.

Therefore, considering that the approach on liability for animals is linked to the concept of lack of predictability which is also the case in the context of autonomous behaviour of AI entities, the relevant safety instruments for AI entities will have an important role to play in reducing this unpredictability to a socially accepted minimum (Commission Staff Working Document, 2018).

In the context of the Digital Single market strategy, the Commission stressed the need to adapt the current legal framework discussed above, taking into account emerging digital technologies, especially from the angle of civil law liability. In its recommendations to the Commission in 2017, the European Parliament stressed the importance of analysing and addressing civil liability for damage caused by robots at Union level. A Union level analysis will ensure the same degree of efficiency,

⁶³ P8_TA(2017)0051 Civil Law Rules on Robotics European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) 5

⁶⁴ Ibid.

⁶⁵ Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)

⁶⁶ https://ec.europa.eu/growth/sectors/mechanical-engineering/machinery_en

⁶⁷ Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (Text with EEA relevance)

transparency and consistency in the implementation of legal certainty throughout the EU for the benefit of citizens, consumers and businesses alike.⁶⁸ In terms of damages, the Recommendations pointed out that “whatever legal solution it applies to the civil liability for damage caused by robots in cases other than those of damage to property, the future legislative instrument should in no way restrict the type or the extent of the damages which may be recovered, nor should it limit the forms of compensation which may be offered to the aggrieved party, on the sole grounds that damage is caused by a non-human agent”.⁶⁹

Further rules are also in place such as the proposed legislation on medical devices, and the regulation on common rules in the field of civil aviation currently under revision which includes concrete measures to ensure the safe operation of civil drones. However, autonomous AI systems and robots will bring about further unprecedented difficulties, since it may be more difficult to ascertain what caused the damage in certain situations, particularly if the technology is able to advance its learning processes. The European Parliament has expressly stressed the paramount importance of legal certainty on liability for innovators, investors and consumers as well as the difficulty in determining who is liable and to what extent in the complex field of digital technologies (European Parliament, Verbatim Report of Proceedings, 2017). It is thus evident that a fair and clear allocation of responsibilities and efficient mechanisms of binding law are necessary. In this regard, governments and international organisations ought to increase their efforts seeking to clarify the parameters of liability for damage caused by undesired behaviours of autonomous systems.

The European Parliament has expressly stressed the paramount importance of legal certainty on liability for innovators, investors and consumers.



Discussion

Considering that an AI system or powered robot can act autonomously and independently with no or little direct supervision, the next question to be answered boils down to whether it can be subject to legal control as any other natural person. AI systems such as powered robots have several capabilities including communication, internal and external knowledge, goal driven behaviour and creativity, all of which can raise issues of civil and/or criminal liability/accountability on their part (Gabriel Hallevy, 2010).

For instance, in July 2015, a robot killed a contractor at one of Volkswagen’s production plants in Germany, who was part of a team that was setting up the stationary robot when it grabbed and crushed him against a metal plate.⁷⁰ In March 2018 a pedestrian woman was struck and killed by an autonomous car operated by Uber in Arizona, while a self-driving Tesla was involved in a fatal car accident in 2016, killing one man.⁷¹ In order to impose criminal liability upon a person the factual element of *actus reus* (criminal conduct) and the mental element of *mens rea* (knowledge or general intent) must be present. The *actus reus* element is expressed mainly by actions or inactions which sometimes require a specific result or circumstance. *Mens rea*, is expressed by different levels of mental elements where knowledge and intention are the highest and negligence/strict liability offences the lowest (Jonathan Herring, 2016, 165). In order to impose criminal liability on any kind of

⁶⁸ P8_TA(2017)0051 Civil Law Rules on Robotics European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), para 49

⁶⁹ P8_TA(2017)0051 Civil Law Rules on Robotics European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), para 42

⁷⁰ <https://www.theguardian.com/world/2015/jul/02/robot-kills-worker-at-volkswagen-plant-in-germany>

⁷¹ <https://www.nytimes.com/interactive/2018/03/20/us/self-driving-uber-pedestrian-killed.html?mtrref=www.google.com>; <https://www.nytimes.com/2016/07/01/business/self-driving-tesla-fatal-crash-investigation.html?module=inline>

entity, the existence of these elements in the specific entity must be proven. Therefore, the extent to which an AI entity can satisfy these two elements must be examined.

Firstly, the external requirement of a criminal conduct through an act or omission, seems to be easily satisfied by an AI powered robot, system or entity. As long as an AI entity controls a mechanical or other mechanism to move its moving parts (e.g. hydraulic arm), any act might be considered as performed by the AI entity (Joshua Dressler, 2009, 979-980). The real challenge is the proof of the second requirement, that of *mens rea*, since AI technological entities possess different levels of autonomy and mentality. Knowledge has been defined as “sensory reception of factual data and the understanding of that data”, including receptors of sights, voices, physical contact and touch which are common in most AI systems (Gabriel Hallevy, 2010, 188). These receptors transfer the factual data received to central processing units that analyse the data in a similar way to the human brain’s analysis of data (Margaret A. Boden, 2006, 108-111). AI systems might be programmed for a purpose, and to take actions to reach that purpose. This could constitute the specific intent that will result in the external action, with perhaps the exception of crimes of hate or racism if one assumes that AI entities are not capable of imitating emotions yet (but AI systems could express opinions). Most AI system algorithms are capable of analysing the permitted and restricted behaviours contrary to infants, while if the algorithm functions properly there is no reason for it not to use all of its capabilities to analyse the factual data received and control impulsive behaviour in contrast to the mentally-ill offenders (Gabriel Hallevy, 2010, 190). Consequently, advanced AI systems could in theory be capable of satisfying the requirements to be held liable for a criminal offence and the defences applying to infants and mentally-ill offenders would not apply.

If the capabilities of the AI entity are insufficient to render it liable for a criminal offence as the sole perpetrator, joint human liability could be considered, whereby the autonomy or learning capability of the AI entity will be assessed against training and instructions given to it. More specifically, according to the European Parliament’s recommendations, “once the parties bearing the ultimate responsibility have been identified, their liability should be proportional to the actual level of instructions given to the robot and of its degree of autonomy” and skills. However, skills resulting from “training” given to a robot should be not confused with skills depending strictly on its self-learning abilities when seeking to identify the person to whom the robot's harmful behaviour is actually attributable.⁷² For instance, older versions of AI entities that lack the modern advanced capabilities or a new version not using them at the time of the offence, could be the innocent agent of instrumental use by either the programmer of the AI system or the end-user. The so-called ‘perpetration-via-another liability model’, considers the actions/inactions of the AI entity as if it had been the programmer’s actions, who designed a programme in order to commit offenses or the actions of the end-user who used the AI system for its own benefit. The legal basis for liability would be the instrumental usage of the AI entity as an innocent agent (Gabriel Hallevy, 2010, 180).

If it is assumed that AI entities can satisfy the test and be held liable for a criminal offence, the sentencing of that AI entity must follow. Sentences could take the form of; firstly, the deletion of the AI software controlling the AI entity which is the corresponding sentence of capital punishment for humans. Secondly, to put the AI entity out of use for a set period of time within the context of a sentence of incarceration and lastly, the sentence could take the form of community service whereby the AI entity would be engaged as a worker in different areas of community service as probation when damages are caused by the AI entity’s actions (Gabriel Hallevy, 2010, 199). The rapid development of AI systems and the dangers deriving therefrom, require legal changes to safeguard the welfare of society especially from criminal conduct which can lead to serious threats on the social order in not properly regulated.

⁷² P8_TA(2017)0051 Civil Law Rules on Robotics European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), para 56

References

- Boden M A, 'Has AI helped psychology?' in Derek Partridge (ed), *The Foundations of Artificial Intelligence: A Sourcebook* (Cambridge University Press 2006) 108-11
- Commission Staff Working Document, 'Liability for emerging digital technologies' Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence (2018) for Europe {COM(2018) 237 final}
- Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.
- Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (Text with EEA relevance)
- Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)
- Dressler J, *Cases and Materials on Criminal Law* (5th ed., American Casebook Series 2009) 979-980
- European Parliament, Verbatim Report of Proceedings of 15 February 2017, 173
- Hallevey G, 'The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control' (2010) 4 *Akron Intellectual Property Journal* 171, 176
- Herring J, *Criminal Law: Text, Cases, and Materials* (7th edn, OUP 2016) 165
- House of Lords Report, 'AI in the UK: ready, willing and able?' (2018) HL Paper 100
<<https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>>
- House of Lords, Select Committee on Artificial Intelligence (14 November 2017)
<<http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/artificial-intelligence-committee/artificial-intelligence/oral/74210.html>>
- https://ec.europa.eu/growth/sectors/mechanical-engineering/machinery_en
- <https://www.nytimes.com/interactive/2018/03/20/us/self-driving-uber-pedestrian-killed.html?mtrref=www.google.com>; <https://www.nytimes.com/2016/07/01/business/self-driving-tesla-fatal-crash-investigation.html?module=inline>
- <https://www.theguardian.com/world/2015/jul/02/robot-kills-worker-at-volkswagen-plant-in-germany>
- P8_TA(2017)0051 Civil Law Rules on Robotics European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), para Z

SIS and Bias and Discrimination

Overview

Discrimination undermines the fulfilment and enjoyment of a variety of rights (economic, social and cultural rights) for a large proportion of the world and that economic growth has not, in itself, led to sustainable development, and that individuals and groups of individuals continue to face socio-economic inequality, often because of entrenched historical and contemporary forms of discrimination' (General comment No. 20, Non-discrimination in economic, social and cultural rights (art. 2, para. 2, of the International Covenant on Economic, Social and Cultural Rights).

According to Knight, experts believe that the problem of AI discrimination may be affecting a growing number of decisions in finance, health care, and education (Knight, n.d.). What is more, Crawford argues that AI 'may already be exacerbating inequality in the workplace, at home and in our legal and judicial systems. Sexism, racism and other forms of discrimination are being built into the machine-learning algorithms that underlie the technology behind many "intelligent" systems that shape how we are categorized and advertised to' (Crawford, 2016).

Bias and Discrimination was identified in Sherpa case studies as well. For example, CS1 (Employee monitoring and administration) explores specific cases of privacy and discrimination which are related to monitoring. According to that case study, 'Discrimination and inequality were the ethical issues most dominant in the literature review, which drew mostly from cases of employee monitoring'. Moreover, this particular case study identified 'potential for discrimination of potential users of the software' deriving from the capabilities of the software which it was looking at. CS2 (Governance) identified correlation between bias and SIS and it supports that 'when human bias is put into AI algorithms, city services may not be provided equally or fairly'. Moreover, CS5 (Science) and CS6 (Insurance) also talk about bias and discrimination. Indicatively, CS6 mentions that 'artificial intelligence may make many false assumptions in the insurance sector which could end up being discriminatory (e.g. making insurance more expensive for minorities).'

ECHR protected categories include sex, gender, sexual orientation, disability, age, race, ethnicity, colour and membership of national minority, religion, social origin, language, political opinion and SIS can interrelate and affect all of those.

Below are examples of discrimination based on language/accent, racial discrimination and gender discrimination. The section closes with an example as to how bias and discrimination can also lead to security risks.



Discrimination based on language/accent

People usually make judgments in different ways. Some tend to make judgments based on one's accent. Equally, AI systems are designed and/or learn to be prejudiced against certain dialects. Knight, based on research, argues that 'as language-based AI systems become ever more common, machines may automatically discriminate against minorities' (Knight, n.d.). Imagine having a not so common accent, trying to communicate with Alexa or Siri for example. Voice-recognition systems do not have enough examples of particular accents, and thus these systems may fail to understand certain accents. This means that services and products, among others, may be unfairly discriminating against certain groups (Knight, n.d.).

Racial Discrimination

One example of AI based racial discrimination is a proprietary algorithm called Compass, which is used to decide whether prison inmates should be granted parole. The workings of the algorithm are unknown, but research suggests it is biased against black inmates (Knight, n.d.). Another example is Google's photo app, which applies automatic labels to pictures in digital photo albums, which was classifying images of black people as gorillas. Similar errors have emerged in Nikon's camera software, which misread images of Asian people as blinking, and in Hewlett-Packard's web camera software, which had difficulty recognizing people with dark skin tones. Moreover, a very serious example was revealed in an investigation published by ProPublica . It found that widely used software that assessed the risk of recidivism in criminals was twice as likely to mistakenly flag black defendants as being at a higher risk of committing future crimes. It was also twice as likely to incorrectly flag white defendants as low risk. Another scandal emerged recently when it was revealed that Amazon's same-day delivery service was unavailable for ZIP codes in predominantly black neighbourhoods (Crawford, 2016).

Gender discrimination

Computer scientists at Carnegie Mellon University found that women were less likely than men to be shown ads on Google for highly paid jobs (Crawford, 2016).

Another example is where algorithms may be trained using job applicants from a field that is predominantly male. Its predictions might be problematic when applied in another occupational field or to another group of applicants (FRA, Big data, algorithms and discrimination).

Bias and discrimination leading also to security risks

Police departments across the United States are also deploying data-driven risk assessment tools in "predictive policing" crime prevention efforts. In many cities, including New York, Los Angeles, Chicago and Miami, software analyses of large sets of historical crime data are used to forecast where crime hot spots are most likely to emerge; the police are then directed to those areas. At the very least, this software risks perpetuating an already vicious cycle, in which the police increase their presence in the same places they are already policing (or overpolicing), thus ensuring that more arrests come from those areas. In the United States, this could result in more surveillance in traditionally poorer, non-white neighbourhoods, while wealthy, white neighbourhoods are scrutinized even less (Crawford, 2016). This example does not only show bias and discrimination but it also shows that this exact bias and discrimination can have an impact on security.

Current legal and ethical instruments (split in values and principles)

The right to freedom from discrimination is protected, both internationally as well as on a European level, both in soft as well as hard law instruments.⁷³

Internationally, it is protected through the Universal Declaration of Human Rights (soft law) which states that "Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty." (Art. 2, UDHR)

At the international level, legally binding this time, the right to freedom from discrimination is also included in the International Covenant on Civil and Political Rights (Art. 2 and 26, ICCPR) and the International Covenant on Economic, Social and Cultural Rights (Art. 2, ICESCR). Moreover, discrimination is combated through numerous international legal instruments which focuses on marginalised/vulnerable groups. Some examples are the International Convention on the Elimination of All Forms of Racial Discrimination, the Convention on the Elimination of All Forms of Discrimination Against Women, and the Convention on the Rights of Persons with Disabilities. There are also international legal instruments which protect against discrimination against indigenous peoples (Human Rights Council, Resolution 2006/2), minorities (UN, Declaration on the Rights of Persons Religious and Linguistic Minorities) and against discrimination based on sexual orientation and gender identity⁷⁴.

As per General Comment No. 18 on Discrimination, 'the principle of non-discrimination is so basic that article 3 of the International Covenant on Civil and Political Rights obligates each State party to ensure the equal right of men and women to the enjoyment of the rights set forth in the Covenant'. Moreover, it provides that, while States Parties can take measures which derogate from certain obligations under the Covenant in time of public emergency, those measures should not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin. Lastly, 'article 20, paragraph 2, obligates States parties to prohibit, by law, any advocacy of national, racial or religious hatred which constitutes incitement to discrimination' (UN Human Rights Committee (HRC), CCPR General Comment No. 18: Non-discrimination).

At the European level, Article 21 of the Charter of Fundamental Rights of the European Union stipulates that '1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited' and '2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited' (Art. 21, EU Charter).

⁷³ Hard law refers to legally binding instruments (eg case law and Treaties) and soft law refers to non-legally binding instruments (eg Resolutions, Declarations, Statements, Principles, Code of Conduct).

⁷⁴ Protection against violence and discrimination based on sexual orientation and gender identity (adopted 30 June 2016) - A/HRC/RES/32/2, Human Rights Council resolution - Human rights, sexual orientation and gender identity (adopted 17 June 2011) - A/HRC/RES/17/19, Human Rights Council resolution - Human rights, sexual orientation and gender identity (adopted 26 September 2014) - A/HRC/RES/27/32

Also, Article 14 of the European Convention on Human Rights stipulates that ‘The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.’ (Art 14, ECHR) ‘Protocol 12 (2000) to the ECHR, not yet ratified by all EU Member States, expands the scope of the prohibition of discrimination to equal treatment in the enjoyment of any right, including rights under national law’ (FRA, 2018).

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground.



Moreover, the non-discrimination principle is one of the fundamental values of the European Union. (Art. 2, TEU) Article 10 of the TFEU requires the EU to combat discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation, when defining and implementing its policies and activities (Art. 10, TFEU). In 2000, two directives were adopted: the Employment Equality Directive (2000/78/EC)²¹ prohibited discrimination on the basis of sexual orientation, religion or belief, age and disability, in the area of employment; and the Racial Equality Directive (2000/43/EC)²² introduced prohibition of discrimination on the basis of race or ethnicity in the context of employment, but also in accessing the welfare system and social security, as well as goods and services. This was a significant expansion of the scope of non-discrimination law under EU law’ (FRA, 2018).

Discussion

People involved in the design, development and use of SIS need to be vigilant about how they design and train machine-learning systems, or one will see ingrained forms of bias built into the artificial intelligence of the future.

Making algorithms fair and non-discriminatory is a daunting exercise. But several steps could help move in the right direction. These include:

- checking the quality of the data being used to build algorithms to avoid faulty algorithm ‘training’;
- promoting transparency – being open about the data and code used to build the algorithm, as well as the logic underlying the algorithm, and providing meaningful explanations of how it is being used. Among others, this will help individuals looking to challenge data-based decisions pursue their claims;
- carrying out algorithmic and/or human rights impact assessments that focus on the implications for fundamental rights, including whether they may discriminate based on protected grounds, and seeing how proxy information can produce biased results;
- involving experts in oversight of algorithm design and use: to be effective, reviews need to involve statisticians, lawyers, social scientists, computer scientists, mathematicians and experts in the subject at issue (FRA, Big data, algorithms and discrimination).

References

Consolidated Version of the Treaty on European Union, 2010 O.J. C 83/01

Consolidated Version of the Treaty on the Functioning of the European Union, 2008 O.J. C 115/47

Council of Europe, European Convention on Human Rights (1953)

Crawford, K. (2016). Artificial Intelligence's White Guy Problem. *New York Times*.

European Union (2012) Charter of Fundamental Rights of the European Union, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN>

European Union: Council of the European Union, Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, 27 November 2000, OJ L 303 , 02/12/2000 P. 0016 – 0022

Fundamental Rights Agency (2018) Handbook on European non-discrimination law

Fundamental Rights Agency (2018), Big data, algorithms and discrimination

General comment No. 20, Non-discrimination in economic, social and cultural rights (art. 2, para. 2, of the International Covenant on Economic, Social and Cultural Rights)

Human Rights Council resolution - Human rights, sexual orientation and gender identity (adopted 17 June 2011) - A/HRC/RES/17/19,

Human Rights Council resolution - Human rights, sexual orientation and gender identity (adopted 26 September 2014) - A/HRC/RES/27/32

Human Rights Council, Resolution 2006/2

Knight, W. (n.d.). Another Way AI Programs Can Discriminate Against You. *MIT TECHNOLOGY REVIEW*, 120(8).

Protection against violence and discrimination based on sexual orientation and gender identity (adopted 30 June 2016) - A/HRC/RES/32/2,

Racial Equality Directive (2000/43/EC)22

UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at:

<https://www.refworld.org/docid/3ae6b3aa0.htm>

UN General Assembly, *International Covenant on Economic, Social and Cultural Rights*, 16 December 1966, United Nations, Treaty Series, vol. 993, p. 3, available at:

<https://www.refworld.org/docid/3ae6b36c0.html>

UN Human Rights Committee (HRC), CCPR General Comment No. 18: Non-discrimination, 10 November 1989, available at: <https://www.refworld.org/docid/453883fa8.html>

UN, Declaration on the Rights of Persons Religious and Linguistic Minorities,

https://www.ohchr.org/Documents/Issues/Minorities/Booklet_Minorities_English.pdf

United Nations (1948) Universal Declaration of Human Rights, <https://www.un.org/en/universal-declaration-human-rights/>

SIS and Democracy, Freedom of Thought, Control and Manipulation

Overview

'Why wouldn't we leave all policy decisions (thus Democracy) to more advanced AIs?' Damjanović wonders, since we already trust AI with so many things in our personal life, such as for choosing music or movies for us, and even with diagnosing of our illnesses and financial decisions (Damjanović, 2015). The recent scandal over Cambridge Analytica's participation in electoral manipulation and gross breaches of privacy (Common, 2018) is an indication that things are not as straightforward and that the relation between AI and democracy is controversial. It is also of course a significant example of the ways in which SIS interact and threaten democracy. In this case, Facebook gave unfettered and unauthorized access to personally identifiable information (PII) of more than 87 million unsuspecting Facebook users to the data firm Cambridge Analytica, which developed the ability to "micro-target" individual consumers or voters with messages most likely to influence their behaviour (Isaak and Hanna, 2018).

This incidence shows the relevance and interconnectedness of democracy, freedom of thought, control and manipulation.

According to Faliszewsk and Procaccia, the danger of manipulation, which is one of many types of attack on elections, is quite clear in human elections, but recently voting manipulation has also endangered the world of artificial intelligence and computer science. The reason is that virtual elections have become a standard tool in preference aggregation (Faliszewski and Procaccia, 2010).

The organisations Article 19 and Privacy International are particularly concerned about the impact AI will have on the right to freedom of expression and information, which, as they claim, are essential foundations for open and democratic societies and among the basic conditions for progress, as well as for each individual's self-fulfilment. 'For democracy, accountability and good governance to thrive, freedom of expression must be respected and protected'. In their views, there are a number of unique challenges that AI poses for freedom of expression. They classify them under the following categories: a) Lack of respect for the rule of law, b) Lack of transparency, c) Lack of accountability, d) Public perception and the role of the media, e) Data collection and use (Article 19, 2018).

Academic literature warns us that Smart Information Systems must be compatible with our society's values, otherwise they will cause extensive damage. When AI and Democracy are concerned, one warning for the case of non-compatibility between AI and societal values is that they (Smart information systems) could lead to an automated society with totalitarian features. One more specific example is a centralized artificial intelligence which will be able to control what we know, what we think and how we act (Helbing et al., 2017).



Current legal and ethical instruments (split in values and principles)

Democracy

At the European level, Article 39 of the EU Charter is strongly related to Democracy (**Right to vote and to stand as a candidate at elections to the European Parliament**). It stipulates that every citizen of the Union has the right to vote and to stand as a candidate at elections to the European Parliament in the Member State in which he or she resides, under the same conditions as nationals of that State, and that Members of the European Parliament shall be elected by direct universal suffrage in a free and secret ballot (Art. 39, EU Charter).

At the international level, Article 19 of the UDHR is on the same vein as it stipulates that Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers (Art. 19, UDHR).

Freedom of thought

At the European level, Article 10 of the EU Charter protects the **Freedom of thought (as well as of conscience and religion)** and stipulates, among others, that everyone has the right to freedom of thought, conscience and religion and that this right includes freedom to change religion or belief and freedom, either alone or in community with others and in public or in private, to manifest religion or belief, in worship, teaching, practice and observance (Art. 10, EU Charter).

At the international level, Article 18 of the UDHR stipulates that everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance (Art. 18, UDHR).

Freedom of expression

At the European level, Article 11 of the EU Charter provides about Freedom of expression and information that 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers, and 2. The freedom and pluralism of the media shall be respected (Art. 11, EU Charter). Moreover, Article 10 of the ECHR protects the Freedom of expression and provides that everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers (Art. 10, ECHR).

At the international level, Article 19 of the UDHR provides that everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers (Art. 19, UDHR).

Overarching rights

Some rights stipulate rights in similar areas and/or are strongly related/relevant.

At the European level, Article 11 of the EU Charter protects the freedom of expression and information, which are vital elements for the healthy enjoyment of democracy and freedom of thought and the avoidance of control and manipulation. The article stipulates that everyone has the right to freedom of expression and that this right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. It also stipulates that the freedom and pluralism of the media shall be respected (Art. 11, EU Charter).

Discussion

While the right to freedom of expression is a fundamental right, it is not guaranteed in absolute terms since restrictions to it are allowed. For example paragraph 3 of Article 19 of the International Covenant on Civil and Political Rights (ICCPR) provides restrictions on the right to freedom of expression which must be of course strictly and narrowly tailored and may not put the right itself in jeopardy. The method of determining whether a restriction is narrowly tailored is often articulated as a three-part test. Restrictions must: (i) be provided by law; (ii) pursue a legitimate aim; and (iii) conform to the strict tests of necessity and proportionality (Article 19, 2018).

Apart from paragraph 3 of Article 19 of the ICCPR, Article 10 of the ECHR provides that the exercise of the freedoms of the first paragraph of the article, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Despite the fact that there are no international standards that explicitly deal with AI and the right to freedom of expression, there is a body of international standards which are relevant to the use of AI, particularly in relation to online intermediaries. For example, states should not impose a general obligation on intermediaries to monitor the information that they transmit, store, automate or otherwise use, and users should have the opportunity to challenge the blocking and filtering of content (Article 19, 2018).

Going back to the unique challenges that AI poses for freedom of expression, as identified by the organisations Article 19 and Privacy International and mentioned at the beginning of this report, we can analyse them and reach conclusions.

Respect for the rule of law

Industry initiatives around AI must stop being narrowly focused on the development of technical standards, ethical frameworks, and concepts such as fairness, transparency, and accountability and become enforceable and comply with the rule of law. Currently, a great deal of the work undertaken in this area lacks enforcement mechanisms, whether self-imposed or through voluntary regulation, limiting its impact.

Transparency

Developers of critical AI systems should be required to develop them in transparent and inscrutable ways and eliminate trade secrets rules and high barriers to transparency around application and development, as well as reduce the inherent complexity of these systems.

Accountability

Establish mechanisms which will make it easy to ensure accountability for violations of those responsible for potential harm caused by AI systems. Currently, the hidden nature of AI systems makes it difficult to study or analyse the impact of AI on the right to freedom of expression unless a tangible harm occurs.

Public perception and the role of the media

The media has a role to play in ensuring that coverage of AI is focused on the issues at hand. Currently, much of the popular discourse around AI focuses on the dangers of AI general intelligence instead of current, practical, and realistic implications of AI systems. This discourse has a real impact,

which is misdirecting attention and funding away from current problems surrounding freedom of expression and privacy to favour hypothetical dystopian scenarios.

Understanding data collection and use

The way in which data is collected and used in AI systems causes concerns about freedom of expression. Understanding how data use and quality influences AI systems must be promoted, since it is particularly pertinent to front-line defenders of human rights, and vulnerable or minority communities that will be under- or misrepresented in datasets (Article 19, 2018).

References

- Article 19 (2018), Privacy and Freedom of Expression In the Age of Artificial Intelligence. Available at: <https://privacyinternational.org/report/1752/privacy-and-freedom-expression-age-artificial-intelligence>
- Damjanović, I. (2015). Polity Without Politics? Artificial Intelligence Versus Democracy. *Bulletin of Science, Technology & Society*, 35(3-4), pp.76-83.
- European Union (2012) Charter of Fundamental Rights of the European Union, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN>
- F. Common, M. (2018). Facebook and Cambridge Analytica: let this be the high-water mark for impunity. [Blog] *United States Politics and Policy*. Available at: <https://blogs.lse.ac.uk/usappblog/2018/03/24/facebook-and-cambridge-analytica-let-this-be-the-high-water-mark-for-impunity/>
- Faliszewski, Piotr & D. Procaccia, Ariel. (2010). AI's War on Manipulation: Are We Winning?. *AI Magazine*. 31. 53-64.
- Helbing, Dirk & S. Frey, Bruno & Hafen, Ernst & van den hoven, Jeroen & Gigerenzer, Gerd & Zicari, Roberto & Zwitter, Andrej & Hofstetter, Yvonne. (2017). Will Democracy Survive Big Data and Artificial Intelligence?.
- Isaak, Jim & J. Hanna, Mina. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*. 51. 56-59.
- United Nations (1948) Universal Declaration of Human Rights, <https://www.un.org/en/universal-declaration-human-rights/>

SIS and Security, Dual Use, and Misuse

Overview

The benefits that AI and big data may bring to people and the society at large are greatly recognised, including the improvement of efficiency in the public sector and industry, and new methods and solutions in various sectors (Huimin Lu, 2017). On the other hand, the rapid advancement of AI systems can pose security threats, requiring the detection and prevention of the misuse of data or the framing of their dual use. Besides the wide use of AI systems for effective IT management, AI technologies are now widely developed in the military forces, with autonomous weapons European (Parliament, DG for External Policies, 2017).

The above developments and threats are catered for in EU Regulation 428/2009 which sets up the EU 'regime for the control of exports, transfer, brokering and transit of dual-use items'.⁷⁵ Article 2(1) provides that 'dual-use items' are "items, including software and technology, which can be used for both civil and military purposes, and [...] include all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices". The rationale is that dual-use items, including software and technology, should be "subject to effective control when they are exported from the European [Union]", for security reasons and for the purpose of ensuring non-proliferation and/or misuse of such technologies, software and data while transferred. Technological challenges presented by AI and big data are a global phenomenon, present in multiple fields of the economy, governance structure and national defence. They can also be triggered in business solutions specialising in the design of new legal services embedded in legal systems (Council of Europe, European Commission for the Efficiency of Justice, 2018).

The rapid advancement of AI systems can pose security threats, requiring the detection and prevention of the misuse of data or the framing of their dual use.



The sustainability of human rights is therefore under pressure when developing and using AI system in the context of security, dual use and misuse of data. Case Studies in Sherpa Deliverable (D1.1) identify such risks in the fields of employment (CS1), scientific developments (CS5), insurance (CS6), energy (CS7), communications, media and entertainment (CS8) and trade (CS9), among others. In terms of security, Elon Musk stresses the dangers that can derive from AI systems and doubted humans' ability to manage it in a safe way indicating that "the danger of AI is much greater than the danger of nuclear warheads by a lot and nobody would suggest that we allow anyone to build nuclear warheads if they want. That would be insane".⁷⁶

Current legal and ethical instruments (split in values and principles)

The rapid advancement of SIS (AI and big data systems and technologies) could lead to great benefits, participation to the eradication of poverty and the reduction of climate change. However, it may also bring autonomous weapons, economic disruption and machines with a will of their own, potentially in conflict with humanity and human rights values. Addressing this requires a concrete framework for legal and human rights sustainability. With these considerations in mind the

⁷⁵ Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

⁷⁶ <https://www.cnbc.com/2018/03/13/elon-musk-at-sxsw-a-i-is-more-dangerous-than-nuclear-weapons.html>

International Conference of Data Protection and Privacy Commissioners proceeded to the endorsement of guiding principles for the creation, development and use of AI systems.⁷⁷

Amongst the accredited Members of the Conference are most of the EU Member States as well as the Union itself through the Customs Information System Joint Supervisory Authority, the European Data Protection Supervisor and the Joint Supervisory Body of Eurojust. The guiding principles were incorporated into the Declaration on Ethics and Data Protection in Artificial Intelligence which endorses six guiding principles in order to preserve human rights in the development of AI systems and software.⁷⁸ In a nutshell, the six guiding principles which expand on ethical considerations linked to governance principles on AI are as follows:

- AI entities must be designed, used and developed in full respect for fundamental rights and the fairness principle, including the assurance that the use of AI systems remains consistent with their original purposes, not endangering the human development or the society at large.
- Rules must ensure the continued attention and vigilance, as well as accountability, to the potential effects and consequences of AI systems, including through the promotion of accountability and responsibility of all the relevant stakeholders, supervisory authorities and the autonomous AI systems themselves.
- AI systems' transparency and intelligibility must be improved, for instance, through the development of new ways of communication and promotion of adequate information to the public and algorithmic transparency.
- The Declaration as part of an overall "ethics by design" approach, stresses the importance of AI systems to be designed and developed responsibly, by applying the principles of privacy by default and privacy by design, including by assessing and documenting the expected impacts on individuals and society from the beginning of a project.
- The empowerment of every individual should be promoted, and the exercise of individuals' rights encouraged, as well as the creation of opportunities for public engagement through adaptable interfaces and accessible tools.
- Unlawful biases or discriminations that may result from the use of data in AI should be reduced and mitigated, by ensuring inter alia 'the respect of international legal instruments on human rights and non-discrimination', investment 'in research into technical ways to identify, address and mitigate biases', ensuring accuracy of data, and elaborate 'specific guidance and principles in addressing biases and discrimination'.⁷⁹

The promising Declaration was open for public consultation until 15 February 2019 and all interested stakeholders including NGOs, businesses, academic bodies, public and governmental authorities were invited to contribute. Although the Declaration will not form a legally binding document on States or other stakeholders, it calls for the establishment of common principles of governance on AI in full respect for human values and dignity and for the creation of a permanent working group on ethics and data protection in AI, much needed at the international level.⁸⁰

⁷⁷ The International Conference of Data Protection and Privacy Commissioners first met in 1979 and has been the premier global forum for data protection authorities for nearly 4 decades. The Conference seeks to provide leadership at international level in data protection and privacy. It does this by connecting the efforts of 122 privacy and data protection authorities from across the globe. <<https://icdppc.org/>>

⁷⁸ <https://icdppc.org/public-consultation-ethics-and-data-protection-in-artificial-intelligence-continuing-the-debate/>

⁷⁹ https://www.privacyconference2018.org/system/files/2018-10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

⁸⁰ Ibid.

Similarly, the European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe, acknowledged the increasing development of the AI systems as well as the expected benefits deriving therefrom and adopted a list of fundamental principles entitled ‘European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment’ for this purpose, an instrument of soft law. The Charter concerns directly the public and private stakeholders responsible for the design and deployment of AI tools and services that involve the processing of judicial decisions and data as well as the public decision-makers in charge of the legislative or regulatory framework, of the development, audit or use of such tools and services.⁸¹

The five principles established under the Charter overlap to a great extent with the values outlined in the Declaration on Ethics and Data Protection in AI discussed above. In particular, the first principle concerns the respect for fundamental rights when designing and implementing AI tools and services. This is especially the case when AI systems are used to resolve a dispute or as tools to assist in judicial decision-making or to give guidance to the public. The next is the principle of non-discrimination which is preventing the development or intensification of any discrimination between individuals or groups of individuals, especially when the processing is directly or indirectly based on ‘sensitive’ data e.g. racial or ethnic origin, socio-economic background and political opinions. Thirdly, the principle of quality and security in the technological environment must be preserved, in relation to the processing of judicial decisions and data through certified sources and intangible data with models elaborated in a multi-disciplinary manner. Another important principle is that of transparency, impartiality and fairness which is protected under the Charter to make data processing methods accessible and understandable. When AI systems are used in cases that may have legal consequences or may significantly affect people’s lives, it is important to ensure a balance between the intellectual property of certain processing methods and the access to that design process, the absence of bias and the prioritisation of justice. Lastly, the Charter seeks to protect the principle “under user control” which precludes a prescriptive approach and ensures that users are informed actors and in control of the choices made. This principle builds on Article 22(1) of the General Data Protection Regulation which provides for a general right for data subjects to be able to refuse to be subject to a decision based exclusively on an automated process (with no human mediation), ‘including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her’.⁸²

The Charter is a great achievement of the Council of Europe and provides a framework of principles that can guide policy makers, legislators and justice professionals in the development and use of AI systems in national judicial processes. It supplements European legal instruments, namely the European Convention on Human Rights (ECHR) and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,⁸³ which are used as standards. It is expected that the provisions and guarantees of the ECHR are fully complied with by the users of the present Charter. The Charter is intended to be incorporated into national processing methods with respect to the provision of legal advice, legal drafting or the decision-making process, so that compliance with the Charter’s principles may be ensured in the processing of judicial decisions and data by algorithms. Contracting parties such as the Netherlands, Latvia, France, England and Wales and Austria have already presented several ways to approach AI systems’ integration into judicial policies in accordance with the principles set out in the Charter.⁸⁴ Such ways of integration include the AI for

⁸¹ <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>

⁸² REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

⁸³ ETS No. 108 as amended by the CETS amending protocol No. 223,

<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>

⁸⁴ <https://www.coe.int/en/web/cepej/practical-examples-of-ai-implemented-in-other-countries>

anonymisation of court decisions, for analysis in investigation data, for digital file management and for analysing incoming mail.⁸⁵ Importantly, the European Union also participates to the work of CEPEJ, while Canada, Japan, Mexico and the US are enjoying observer status to the Council of Europe and are de facto members of the CEPEJ.

Discussion

The ‘European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment’ is undoubtedly a great achievement of the Council of Europe and steps have been already taken by Contracting Parties to amend the relevant national laws to comply with the provisions of the Charter, such as Austria, England and Wales, France, Latvia or the Netherlands.⁸⁶ However, two main issues arise, namely the fact that these steps are taken with very slow progress in some countries and that the Charter only concerns the use of AI entities and software in the judicial systems. The development and use of AI systems is rapidly spreading across other fields/industries beyond the judicial systems such as in medicine, social life, employment, military and education. Therefore, the scope of application of the Declaration which is much broader, reflects to a greater extent the current need for a relevant framework and the reality of the rapid advancement of AI systems into our everyday lives. In particular the guidance incorporated within the Declaration refers to limits to the creation of autonomous weapons programmed to kill – allegedly an even more serious case than the nuclear arms, the manipulation of the society through propagandas and false information, and the invasion of privacy and social grading of citizens (Marr, 2018).⁸⁷

As previously indicated however, the Declaration holds the status of a formal statement or document of intent but does not create a legally binding obligation on the countries which have signed it. The desired and most effective result would be the drafting and adoption of a Charter at the pan-European or Union level based on the ethical foundations set out in the Declaration, covering a wide range of fields, that would impose a legal obligation on the Contracting parties to comply with the rules/principles incorporated therein. This may not however be the easiest way to proceed given the infiltration of SIS in all governmental, economic and social fields at all levels.

In the meantime, it is indispensable to adopt a general code of conduct to serve as a guideline for ethical development and use of AI systems that will be setting common standards throughout the EU and the world, addressed not only to large data processors and/or controllers but also to national authorities. Such codes already exist at the national level, through a sectoral approach such as healthcare.⁸⁸ Finally, it is important to carry out regular human rights risk assessment in SIS-related fields, mitigating risks in the misuse of human rights through a mapping and policy commitment exercise.⁸⁹

The EU needs a good blueprint of European digital integration, leading to enforceable common standards and encompassing multiple aspects of SIS, including but not limited to the Digital Single Market and fundamental human rights. This requires the use of an alternative legal basis in the EU Treaties, such as Article 2 of the Treaty on the European Union preserving all EU values and

The EU needs a good blueprint of European digital integration, leading to enforceable common standards and encompassing multiple aspects of SIS.



⁸⁵ Austria: <https://rm.coe.int/how-is-austria-approaching-ai-integration-into-ju>

⁸⁶ Ibid.

⁸⁷ <https://www.forbes.com/sites/bernardmarr/2018/11/19/is-artificial-intelligence-everyone-should-know-about/#47b8f40b2404>

⁸⁸ <https://www.digitalhealth.net/2018/09/code-conduct-ai/>

⁸⁹ <https://www.humanrights.dk/news/road-respecting-human-rights>

encompassing the area of freedom, security and justice. This process would then elevate standards internationally, through an international enforcement process thanks to the international legal personality of the EU and its membership is relevant fora.

References

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108, 1985
- COUNCIL REGULATION (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items
- EP and COUNCIL REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Council of Europe, European Commission for the Efficiency of Justice, 'European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment' (Adopted at the 31st plenary meeting of the European Commission for the Efficiency of Justice (CEPEJ) (Strasbourg, 3-4 December 2018))
- DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICIAL INTELLIGENCE 40th International Conference of Data Protection and Privacy Commissioners, 23 October 2018, Brussels
- European Convention on Human Rights, 1953
- European Parliament, DG for External Policies, 'Towards an EU common position on the use of armed drones' (2017)
- Danish Institute for Human Rights, 'The road for respecting human rights', 2016
- Huimin Lu, Yujie Li, Min Chen, Hyoungseop Kim and Seiichi Serikawa, 'Brain Intelligence: Go beyond Artificial Intelligence' (2017) 23 Mobile Networks and Applications 368-375
- Marr B, 'Is Artificial Intelligence dangerous?' 6 AI risks everyone should know about', Forbes, 2018
- Read C, 'Government publishes code of conduct for AI and data-driven healthcare tech', DigitalHealth, 2018

SIS and Health

Overview

According to Hoffman, a particularly rich but sensitive type of big data is medical big data which consists of patient electronic health records (EHR), insurance claims, and pharmacy prescription drug information. This data is of interest to a broad range of insurers who may use it for purposes of underwriting, evaluating physicians, assessing benefits coverage, and detecting fraud.

Medical big data is also invaluable for biomedical research, public health practice, institutions' quality assessment and improvement efforts, and post-marketing surveillance of drugs and devices, among other initiatives. Such uses are known as "secondary uses" of medical information, as distinguished from the data's primary use for clinical and billing purposes (Hoffman, 2014).

Groves et al. argue that an era of open information in healthcare is now under way. Scholars who support this also argue that we have already experienced a decade of progress in digitizing medical records, as pharmaceutical companies and other organizations aggregate years of research and development data in electronic databases. Moreover, they hold that the federal government and other public stakeholders have also accelerated the move toward transparency by making decades of stored data usable, searchable, and actionable by the healthcare sector as a whole. 'Together', they claim, 'these increases in data liquidity have brought the industry to the tipping point' (Groves et al., 2013).

Beyond these, big data for large-scale experiments draws attention to some fundamental questions. One of those are: To what extent should big data and remote self-reported health outcomes replace more accurate and validated clinical assessments for use in health research? There are also concerns about privacy, the accuracy of smartphone apps and unvalidated apps providing inappropriate advice (Brodie et al., 2018).

A recent case which illustrates the interplay of rights and the vulnerability which exists within the sphere of SIS and health is the case of Google Deepmind and the Royal Free Trust. The two entities collaborated in 2016 to predict and prevent Acute Kidney Injuries through an application but the way in which they treated personal data received a lot of criticism. Through this partnership, 1.6m patient records were transferred to one of the biggest data mining companies (Powles and Hodson, 2017).



SHERPA Case Studies also illustrated a problematic interplay between SIS and health. CS5 results (a case study on the ethical issues that relate to the use of Smart Information Systems (SIS) in human brain research) indicate that some of the main ethical concerns with the use of SIS in human brain research include privacy and confidentiality, security of personal data, discrimination that arises from bias and access to the SIS and their outcomes. CS6 (a case study on insurance) illustrates that the use of SIS in the insurance sector can create ethical and practical concerns. Amongst them are concerns over security and privacy of sensitive information, which are increasing year by year because of several trends, such as wireless networking, health and personal information exchange, and cloud computing.

As a result, artificial intelligence may make many false assumptions in the insurance sector which could end up being discriminatory (e.g. making insurance more expensive for minorities), and even harmful to the insured persons (e. g. when healthcare isn't affordable for the person who needs it). More specifically, the CS claims that 'if an artificial intelligence is used to prevent some people from receiving health insurance (for example, by determining that someone has a certain disorder or disease by correlating public pieces of information gleaned from social networks or other public sources) then the reasons should be clearly understood to prevent implicit and harmful biases (Dutt, 2018). These developments could result in a charge of unfair discrimination in insurance which might also be levelled against practices which impact people based upon characteristics such as income level, place of residence, occupation, education, marital or family status'.

Current legal and ethical instruments (split in values and principles)

At the international level (UN), Sustainable Development Goal number 3 is about ensuring healthy lives and promote well-being for all at all ages.

On a European level, the European Social Charter Article 11 (The right to protection of health) stipulates that the Contracting Parties undertake, either directly or in co-operation with public or private organisations, to take appropriate measures designed inter alia: 1) to remove as far as possible the causes of ill health; 2) to provide advisory and educational facilities for the promotion of health and the encouragement of individual responsibility in matters of health; 3) to prevent as far as possible epidemic, endemic and other diseases (Art. 11, European Social Charter).

At the EU level, the right to health is protected under Article 3 and 35 of the EU Charter. Article 3 covers the right to the integrity of the person, and stipulates specifically with respect to the fields of medicine and biology, that the following must be respected: (a) the free and informed consent of the person concerned, according to the procedures laid down by law; (b) the prohibition of eugenic practices, in particular those aiming at the selection of persons; (c) the prohibition on making the human body and its parts as such a source of financial gain; (d) the prohibition of the reproductive cloning of human beings (Art. 3, EU Charter of Fundamental Rights). Article 35 (health care) stipulates that everyone has the right of access to preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices. A high level of human health protection shall be ensured in the definition and implementation of all the Union's policies and activities (Art. 35, EU Charter of Fundamental Rights)..

At the international level, Article 25(1) of the Universal Declaration of Human Rights stipulates that 'Everyone has the right to a standard of living adequate for the health and well-being of himself and of his family, including food, clothing, housing and medical care and necessary social services, and the right to security in the event of unemployment, sickness, disability, widowhood, old age or other lack of livelihood in circumstances beyond his control. ' (Art. 25, UDHR)

Also, Article 12 of the International Covenant on Economic, Social and Cultural Rights stipulates that 'The States Parties [...] recognize the right of everyone to the enjoyment of the highest attainable standard of physical and mental health' and that 'The steps to be taken by the States Parties to the

present Covenant to achieve the full realization of this right shall include those necessary for' among others '(b) The improvement of all aspects of environmental and industrial hygiene', '(c) The prevention, treatment and control of epidemic, endemic, occupational and other diseases' and '(d) The creation of conditions which would assure to all medical service and medical attention in the event of sickness.' (Art 12. ICESCR)

The right to health is protected through Article 24 of the Convention on the Rights of the Child, Article 5 of the Convention on the Elimination of All Forms of Racial Discrimination, Articles 12 & 14 of the Convention on the Elimination of All Forms of Discrimination Against Women and Article 25 of the Convention on the Rights of Persons with Disabilities.

Discussion

With regard to the human right to health, in the year 2000 the UN Committee on Economic, Social and Cultural Rights issued legal guidance for implementation of this right. General Comment 14 is now a key source for advocates seeking to apply human rights standards to their own national, state or local context. Some of its basic principles are: Universality, availability, acceptability and Dignity, Quality, Non-Discrimination, Transparency, Participation, Accountability (CESR General Comment 14).

When it comes to health and mobile apps, Brodie et al. argue that is time to better evaluate such apps and debate the consequences of substituting big data for accurate data in health research. This is because there are concerns regarding the accuracy of some apps and their technical limitations. he argues that smartphone apps are unlikely to provide a valid and unbiased instrument for the scientific monitoring of physical activity (Brodie et al., 2018).

Hoffman, while examining Medical Big Data and their Quality, offers a number of recommendations for more qualitative, accurate and usable data, which in turn can affect the right to health. She proposes data audits⁹⁰, workforce and technical solutions⁹¹, and federal regulations⁹² as umbrella solutions. Under the second (workforce and technical solutions) she proposes: Scribes, Automation, Natural Language Processing, and Best Practices Standards and Training Programs. Under the third proposition (federal regulations) she proposes Meaningful Use Regulations, The HIPAA⁹³ Privacy and Security Rules, and The Common Rule (Hoffman, 2014).

Petersen (2017) argues that although much of the attention of human rights experts thus far has focused on the right to privacy, big data have implications for many other human rights, including the right to health and the right to equality. His paper focuses on the rights of two groups of people who have a strong interest in the impact of data-driven health care – those who live with disabilities and those who may be classified by data scientists as having a higher-than-average risk of developing a disability in the future. Nonetheless, as demonstrated in Part III of the paper, big data also poses significant threats to the rights to privacy and equality. Private actors - such as employers, financial institutions, and insurance companies - have a strong incentive to discriminate, not only against persons with existing impairments but also against persons who are deemed to be at risk of developing impairments in the future. Part IV of the paper takes a comparative approach and considers the extent to which antidiscrimination legislation can protect individuals from discrimination arising from the misuse of health-related data. Part V concludes by recommending

⁹⁰ 'Both clinicians and secondary users of EHR data should routinely conduct data audits to assess the records' accuracy and error rates' (Hoffman, 2014).

⁹¹ 'Among these potential tools are the use of scribes, enhanced automation, improved natural language processing, and the creation of best practices guidelines and training programs' (Hoffman, 2014).

⁹² '[...]three well-established regulatory avenues to address data quality problems: the Meaningful Use Regulations, the HIPAA Security Rule, and the Common Rule'. (Hoffman, 2014).

⁹³ Health Insurance Portability and Accountability Act

that governments need to take a proactive approach to protect individuals from discrimination based on health-related data. In addition to reviewing the scope of anti-discrimination legislation, governments should also consider enacting laws to prohibit the use of health-related data mining in any decision-making process relating to employment, education, or access to financial services. As a minimum, employers and other private actors should be required to disclose when they mine data and engage in re-identification processes (J. Petersen, 2017).

References

- Brodie, M., Pliner, E., Ho, A., Li, K., Chen, Z., Gandevia, S. and Lord, S. (2018). Big data vs accurate data in health research: Large-scale physical activity monitoring, smartphones, wearable devices and risk of unconscious bias. *Medical Hypotheses*, 119, pp.32-36
- Council of Europe, European Social Charter (Revised), 3 May 1996, ETS, <https://www.refworld.org/docid/3ae6b3678.html>
- European Union (2012) Charter of Fundamental Rights of the European Union, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN>
- Greer, S. L. and Vanhercke, B. (2010) "The hard politics of soft law: the case of health," in Mossialos, E., Permanand, G., Baeten, R., and Herve, T. K. (eds) *Health Systems Governance in Europe: The Role of European Union Law and Policy*. Cambridge: Cambridge University Press (Health Economics, Policy and Management), pp. 186–230.
- Groves, P., Kayyali, B., Knott, D. and Van Kuiken, S. (2013). The 'big data' revolution in health care: accelerating value and innovation. Center for US Health System Reform Business Technology Office.
- Hoffman, S. (2014). Medical Big Data and Big Data Quality Problems. *Connecticut Insurance Law Journal*, 21(289).
- J. Petersen, C. (2017). Big Data, Health Care, and International Human Rights Norms. *Asia Pacific Journal of Health Law & Ethics*, 11(1).
- Powles, J. and Hodson, H. (2017). Google DeepMind and healthcare in an age of algorithms. *Health and Technology*, 7(4), pp.351-367.
- UN General Assembly, International Covenant on Economic, Social and Cultural Rights, 16 December 1966, United Nations, Treaty Series, vol. 993, p. 3, <https://www.refworld.org/docid/3ae6b36c0.html>
- United Nations (1948) Universal Declaration of Human Rights, <https://www.un.org/en/universal-declaration-human-rights/>
- United Nations Committee on Economic Social and Cultural Rights: General Comment 14: 'The right to the highest attainable standard of health' (08/11/2000) E/C.12/2000/4

SIS and the Environment

Overview

According to Meinecke, technology experts warn that AI advances could harm our environment. One example is the manufacture of digital devices and other electronics — which go hand-in-hand with the development of AI — that damages our environment (Meinecke,2018). The introduction of new technologies necessary for development brings with it irreversible ecological (and other) consequences, which under certain circumstances can be harmful (Henk and Stanton-Jean, 2009). Some important facts worth mentioning are that electronic waste is expected to reach 52.2 million tons in 2021 (Deutsche Welle, 2017), that the UN Environment Program (UNEP) reported in 2015 that 60 to 90 percent of the world's electronic waste is illegally dumped and that in 2014, an estimated 42 million tons of e-waste were generated (Kaledzi, 2017).

Current legal and ethical instruments

The UN Human Rights Commission adopted several resolutions linking human rights and the environment, such as the Resolutions 2003/71 (Commission on Human Rights resolution 2003/71) and 2005/60 (Human Rights Resolution 2005/60) entitled Human Rights and the Environment as part of Sustainable Development. The UN Commission on Human Rights, in Resolution 2003/71 recognises that the protection of the environment and sustainable development can contribute to human well-being and potentially to the enjoyment of human rights, and that environmental damage can have potentially negative effects on the enjoyment of some human rights (UNHCR, 2015). Resolution 2003/71 calls on States “to take all necessary measures to protect the legitimate exercise of everyone’s human rights when promoting environmental protection and sustainable development and reaffirmed, in this context, that everyone has the right, individually and in association with others, to participate in peaceful activities against violations of human rights and fundamental freedoms.” (Commission on Human Rights resolution 2003/71).

It is important to mention that a new category of rights (‘third generation rights’) have been proposed, as a consequence of a deeper understanding of the different types of obstacles that may stand in the way of realising the first and second generation rights⁹⁴. According to the Council of Europe, the idea at the basis of the third generation of rights is that of *solidarity*; and the rights embrace collective rights of society or peoples, amongst them the right to a healthy environment. In much of the world, conditions such as extreme poverty, war, ecological and natural disasters have meant that there has been only very limited progress in respect of human rights (Council of Europe, n.d.). The third generation rights are under development and not yet integrated into the international or European human rights system like first generation and second generation rights. Thus, one of the main challenges with SIS and the environment is that the right to a healthy environment is still in development.

In 1982, the World Charter for Nature acknowledged that “Mankind is a part of nature and life depends on the uninterrupted functioning of natural systems which ensure the supply of energy and nutrients.” (Aequitas Human Rights, n.d.)

Some important soft law instruments from the UN are *The Declaration of the United Nations Conference on the Human Environment* (or Stockholm Declaration), the *UNESCO Universal*

⁹⁴ The first generation rights refers to the civil and political rights whereas the second generation rights refers to the economic, social and cultural rights.

Declaration on Bioethics and Human Rights, the Millennium Development Goal number 7, Six out of the seventeen Sustainable Development Goals which are directly relevant to the environment and humans' influence over it, and the Rio Declaration On Environment And Development.

The **Declaration of the United Nations Conference on the Human Environment** was adopted in 1972 by the United Nations Conference on the Human Environment as a result of the need for a common outlook and for common principles to inspire and guide the peoples of the world in the preservation and enhancement of the human environment. It is of a historical importance as it is the first document in international environmental law which recognizes the right to a healthy environment. The Declaration, which influenced legal and institutional development for the next two decades, consists of three non-binding instruments which are a resolution on institutional and financial arrangements, a declaration containing 26 principles and an action plan containing 109 recommendations (Human Rights Library, n.d.). Principle 18 stipulates that 'Science and technology, as part of their contribution to economic and social development, must be applied to the identification, avoidance and control of environmental risks and the solution of environmental problems and for the common good of mankind' (UN, 1972).

The **UNESCO Universal Declaration on Bioethics and Human Rights** addresses ethical issues related to medicine, life sciences and associated technologies as applied to human beings, and takes into account their social, legal as well as environmental dimensions. The principles of the Declaration cover a range of moral objects, from the individual human being itself to other human beings, to human communities, to humankind as a whole, and to all living beings and their environment (Henk and Stanton-Jean, 2009). Article 17 (Protection of the environment, the biosphere and biodiversity), stipulates that 'Due regard is to be given to the interaction between human beings and other forms of life, to the importance of appropriate access and utilization of biological and genetic resources, to respect for traditional knowledge and to the role of human beings in the protection of the environment, the biosphere and biodiversity' (Henk and Stanton-Jean, 2009).

The **Millennium Development Goal (MDG) number 7** is dedicated to environmental sustainability (Who.int., n.d.) as 2.4 billion people, which amounts to the one-third of the world's population, would remain without access to improved sanitation in 2015, according to a joint WHO/UNICEF report "Progress on sanitation and drinking-water" (Unicef and WHO, 2015). The "2013 update", warns that, at the current rate of progress, the 2015 Millennium Development Goal target of halving the proportion of the 1990 population without sanitation will be missed by 8% – or half a billion people.

The **United Nations Sustainable Development Goals** provide another lens for the challenges facing humanity. Six of the seventeen goals apply directly to the environment and humans' influence over it: combating climate change, using ocean and marine resources wisely, managing forests, combating desertification, reversing land degradation, developing sustainable cities and providing clean affordable energy (World Economic Forum, 2018).

Principle 13 of the **Rio Declaration On Environment And Development** (1992), product of the Rio Conference, stipulates that 'States shall develop national law regarding liability and compensation for the victims of pollution and other environmental damage' (UNESCO, 1992). The Rio Conference also adopted what is known as "Agenda 21"-a far-reaching program for sustainable development that constitutes the centerpiece of international cooperation within the United Nations system (Human Rights Library, n.d.).

Beyond the above, in 1992, the United Nations Conference on Environment and Development (also known as the Earth Summit) stated that "Human beings are at the centre of concerns for sustainable development. They are entitled to a healthy and productive life in harmony with nature." The Rio Declaration also provided for the right of access to environmental information and of public participation in environmental decision making. In 2002, the World Summit on Sustainable

Development merely acknowledged the position that there exists a possible relationship between environment and human rights (Aequitas Human Rights, n.d.).

Hard Law

At the EU level, Article 37 of the **EU Charter of Fundamental Rights** focuses on environmental protection and stipulates that a high level of environmental protection and the improvement of the quality of the environment must be integrated into the policies of the Union and ensured in accordance with the principle of sustainable development (Art. 37, EU Charter).

Article 12 of the **International Covenant on Economic, Social and Cultural Rights** stipulates that 1. The States Parties to the present Covenant recognize the right of everyone to the enjoyment of the highest attainable standard of physical and mental health. 2. The steps to be taken by the States Parties to the present Covenant to achieve the full realization of this right shall include those necessary for, among others, the improvement of all aspects of environmental and industrial hygiene (Art. 12, ICESCR).

The **United Nations Framework Convention On Climate Change** suggests, among others, to promote and cooperate in scientific, technological, technical, socio-economic and other research, systematic observation and development of data archives related to the climate system and intended to further the understanding and reduce or eliminate the remaining uncertainties regarding the causes, effects, magnitude and timing of climate change and the economic and social consequences of various response strategies (UN, 1992).

Other international standards include the ICESCR in article 12(2), the 1972 World Heritage Convention, the 1985 Vienna Convention, the 1987 Montreal Protocol on Substances that Deplete the Ozone Layer (UNEP), the 1989 Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and Their Disposal (UNEP), the 1992 Framework Convention on Climate Change (UNEP) and the 1992 Convention on Biological Diversity (UNEP). However, UNEP's 1989 Register of Environmental Agreements lists a total of 139 treaties. Furthermore, there are also treaties that deal with environmental obligations rather than primarily addressing environmental issues (Human Rights Library, n.d.).

Finally, it is important to note that other rights such as the right to life, the right to an adequate standard of living and the right to health are directly affected by the state of the environment. Also, procedural human rights such as access to information and participation in decision making are connected to the right of citizens and communities to partake in the formulation of environmental policies. Moreover, Article 24 of the Convention on the Rights of the Child (CRC) recognizes the right of the child to the enjoyment of the highest attainable standard of health with Article 24(c) providing that States Parties shall pursue full implementation of this right and, in particular, shall take appropriate measures to combat disease and malnutrition..., taking into consideration the dangers and risks of environmental pollution." In addition, The Committee on Economic, Social and Cultural Rights has underlined that States must protect against pollution or contamination by private companies and assess their impact on the environment (Aequitas Human Rights, n.d.).



Discussion

The opportunity for AI and big data to be harnessed to benefit humankind and its environment is substantial. The intelligence and productivity gains that such technologies will deliver can unlock new solutions to society's most pressing environmental challenges: climate change, biodiversity, ocean health, water management, air pollution, and resilience, among others (World Economic Forum, 2018).

The World Economic Forum, in its publication 'Fourth Industrial Revolution for the Earth Series, Harnessing Artificial Intelligence for the Earth', lists some recommendations. These recommendations are for companies or governments, or investors or research institutions while some areas are overarching. They are categorized by stakeholder groups, to speed up innovation, minimize environmental risks and maximize environmental benefits from the application of AI. These recommendations include: delivering "responsible AI", collaborating for interdisciplinary solutions, and directing finance for innovation. Recommendations for companies include establishing board-level AI advisory units to ensure that companies' boards understand AI, including safety, ethics, values and governance considerations, embedding environmental considerations into design principles, assuming a leadership role in embedding sustainability principles alongside wider AI safety, ethics, values and governance considerations, and others. Recommendations for governments include: setting research priorities which encourage interdisciplinary research, setting clear parameters for technology innovators and ensuring alignment with human values and international frameworks such as the Sustainable Development Goals, in the framework of the development of responsible technology policies (World Economic Forum, 2018).

References

- [UN Commission on Human Rights, Commission on Human Rights resolution 2003/71: Human Rights and the Environment as Part of Sustainable Development, 25 April 2003, E/CN.4/RES/2003/71, available at: <https://www.refworld.org/docid/43f3134dc.html>
- Aequitas Human Rights. (n.d.). Brief Introduction To Human Rights And The Environment - Aequitas. [online] Available at: <https://www.aequitas-humanrights.org/human-rights-education/the-environment/brief-introduction-to-human-rights-and-the-environment/>
- Council of Europe. (n.d.). The evolution of human rights. [online] Available at: <https://www.coe.int/en/web/compass/the-evolution-of-human-rights>
- Deutsche Welle (2017). Electronic waste reaches record high of 45 million tons. [online] Available at: <https://www.dw.com/en/electronic-waste-reaches-record-high-of-45-million-tons/a-41784177>
- European Union (2012) Charter of Fundamental Rights of the European Union, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN>
- Henk A.M.J. ten, H. and Stanton-Jean, M. (2009). The UNESCO Universal Declaration on Bioethics and Human Rights.
- Human Rights Library. (n.d.). Module 15: The Right to A Healthy Environment. [online] Available at: <http://hrlibrary.umn.edu/edumat/IHRIP/circle/modules/module15.htm>
- Kaledzi, I. (2017). Germany supports e-waste disposal in Ghana. Deutsche Welle. [online] Available at: [1] <https://www.dw.com/en/germany-supports-e-waste-disposal-in-ghana/a-38015011>
- Meinecke, S. (2018). AI could help us protect the environment — or destroy it | DW | 16.07.2018. [online] DW.COM. Available at: <https://www.dw.com/en/ai-could-help-us-protect-the-environment-or-destroy-it/a-44694471>
- UN Commission on Human Rights, Human Rights Resolution 2005/60: Human Rights and the Environment as Part of Sustainable Development, 20 April 2005, E/CN.4/RES/2005/60, available at: <https://www.refworld.org/docid/45377c759.html>

UN General Assembly, International Covenant on Economic, Social and Cultural Rights, 16 December 1966, United Nations, Treaty Series, vol. 993, p. 3, available at: <https://www.refworld.org/docid/3ae6b36c0.html>

UN High Commissioner for Refugees (UNHCR), Policy on the Protection of Personal Data of Persons of Concern to UNHCR, May 2015, Available at: <https://www.refworld.org/docid/55643c1d4.html>

UN, (1992), UNITED NATIONS FRAMEWORK CONVENTION ON CLIMATE CHANGE [online] Available at: <https://unfccc.int/resource/docs/convkp/conveng.pdf>

UN, Declaration of the United Nations Conference on the Human Environment, 1972, Available at: <http://webarchive.loc.gov/all/20150314024203/http%3A//www.unep.org/Documents.Multilingual/Default.asp?documentid%3D97%26articleid%3D1503>

UNESCO, (1992)THE RIO DECLARATION ON ENVIRONMENT AND DEVELOPMENT [online] Available at: http://www.unesco.org/education/pdf/RIO_E.PDF

Who.int. (n.d.). WHO | Millennium Development Goals (MDGs). [online] Available at: https://www.who.int/topics/millennium_development_goals/about/en/

World Economic Forum (2018). The Fourth Industrial Revolution and the Earth: Harnessing Artificial Intelligence for the Earth. [online] Available at: http://www3.weforum.org/docs/Harnessing_Artificial_Intelligence_for_the_Earth_report_2018.pdf

SIS and Rights, including Robot Rights

Overview

“On the tree of robotic life, human-like robots play a particularly valuable role. Humans are brilliant, beautiful, compassionate, loveable, and capable of love, so why shouldn’t we aspire to make robots human-like in these ways?”⁹⁵ David Hanson the Founder and CEO of Hanson Robotics aims to build the world’s most human-like robots that will possess capabilities such as love, compassion and genius. Sophia the Robot, an intelligent humanoid robot of Hanson Robotics was granted citizenship by Saudi Arabia in 2017, making it the first country in the world to grant a robot a status reserved for humans. Sophia’s citizenship status along with the rapid development of advanced and human-like AI machines brought forth, even more pressing, the question of whether robots should be given human rights. The question within the EU goes back to the debate in a European Parliament report in early 2017, which stressed the possibility of granting “personhood” to self-learning robots (European Parliament, 2015).⁹⁶ Such a legal personhood would allow robots to hold rights and obligations, be insured individually and even be held liable for damages.

Although long-debated as to whether things can have personhood, it seems that the discussions specifically around human rights for robots have turned out to be highly controversial. On the one hand, it is argued that granting citizenship to robots in the current state of AI and robotics fundamentally damages the very notion of human rights itself, while the intelligence currently held is not yet adequate to render them real citizens (Hart, 2018). It is further argued that by granting citizenship to Sophia the Robot, the concept and the idea of citizenship is undermined (Hart, 2018).⁹⁷ On the other hand, arguments were developed, *inter alia* by Mark Fischel, supporting that intelligence is not the ‘be all and end all’ when it comes to moral status since clever humans are not favoured morally over less intelligent humans. He further stressed that since we have come up to a point where AI and robotics act and look like humans it might be necessary to grant them extensive rights at least in order to avoid violating the rights of humans due to misidentification (Fischel, 2018).⁹⁸ It is therefore necessary to examine the arguments of both sides in detail and see where AI and robotics stand regarding the degree of rights entitlements they current have and/or deserve.

Current legal and ethical instruments (split in values and principles)

From a legal perspective, it seems that no reference has even been made to rights being directly granted to advanced AI entities and/or robots, neither in the EU nor nationally in the Member States.⁹⁹ The closest the Union has come to this is during the exploration of the possibility of granting such rights in 2017 with the Resolution adopted by the European Parliament on Civil Law Rules on Robotics (European Parliament, 2015).¹⁰⁰ More specifically Paragraph 59(f) states that the European Parliament “calls on the Commission, when carrying out an impact assessment of its future legislative instrument, to explore, analyse and consider the implications of all possible legal solutions, such as: creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons

⁹⁵ <https://www.hansonrobotics.com/hanson-robots/>

⁹⁶ http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html?redirect

⁹⁷ <https://qz.com/1205017/saudi-arabias-robot-citizen-is-eroding-human-rights/>

⁹⁸ <https://blog.goodaudience.com/5-reasons-why-robots-should-have-rights-4e62e8698571>

⁹⁹ See further <http://www.sienna-project.eu/robotics/elsi/>

¹⁰⁰ Civil Law Rules on Robotics, European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) P8 TA(2017)0051

responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently” (European Parliament, 2015).

The idea behind an electronic personality, however, was not about giving human rights to robots but to ensure that a robot is a machine with a human supporting it. Therefore, a possible legal personhood would not make robots virtual people who can get married and benefit from human rights; it would merely put them on an equal footing with corporations, which already have status as ‘legal persons’ and are treated as such by the courts around the world (European Parliament, 2015). The Resolution of the European Parliament has not been discussed or developed by the EP itself since then and the debate on the rights of robots still remains open and subject to divergent views. However, given the accelerating deployment of robots in almost all areas of human life there is an urgent need to develop a special framework of AI entities’ rights, in accordance with the legal and ethical issues arising, to ensure smooth and effective integration of robots into the society as a whole, including workplaces, schools and hospitals, the economy, police forces, the military and national security. According to Birgit Schippers, this clearly means that issues such as accountability, liability and agency need to be addressed, while renewed attention to the meaning of human rights in the age of intelligent machines must be paid (Schippers, 2017).¹⁰¹

Human rights

Human rights can be defined as a set of moral values and norms that help to protect all people from severe political, legal and social abuses.¹⁰² General rights are not the exclusive preserve of humans since several rights are already granted to corporations and animals. Can this be the case for AI and robotics and if so, how? With respect to *specific* rights, it should be noted that AI can be said to benefit from some limited rights related to commercial and scientific exploitation: the right to trade and to process data, sometimes completed by the privilege to access data. At a normative level and with respect to *general* human rights, it is argued that in order to enjoy ‘human rights’, as a human being, three different theoretical concepts/norms must be present namely, consciousness, autonomy and rationality (Fischel, 2018).¹⁰³ The state or quality of **consciousness** refers to the awareness and sentience of a person and the ability of being alive to experience and feel. Although very little is scientifically known about how consciousness works, it can be said to include the unique thoughts, memories, sensations and feelings of one’s own personhood (Koch, 2018).¹⁰⁴ Technology including robotics currently serves human ends, since it is not ‘alive’ or ‘self-aware’ in any meaningful sense (Fischel, 2018).¹⁰⁵ Some self-awareness is likely to arise in the future although, as seen below, consciousness on its own is not of absolute necessity in order to possess rights, considering the example of infants not processing advanced consciousness but extensive rights.

In addition, **autonomy** is mostly related to the ability of forming decisions with free will and certain human rights exist to guarantee this autonomy for individuals including the prohibition of slavery, freedom of expression and freedom of religion. Therefore, autonomy *prima facie* seems an exclusive characteristic of human beings since AI and robotics are still controlled and/or programmed by their creators usually serving human projects. On the other hand, numerous advanced technological inventions have the capacity to discover faster and more effective ways to fulfil a function compared to the methods they were originally supplied. Such an example of a branch of AI is the so-called machine learning which provides automatic learning from data analysis and patterns identification without human intervention or programming (Enrico Di Minin, 2018). Despite the advanced technologies, full autonomy for robots is still an unfinished job (Asokan Thondiyath, 2016), since

¹⁰¹ <http://blogs.discovermagazine.com/crux/2017/12/05/human-rights-robots/#.XD0FbvkzblU>

¹⁰² <https://plato.stanford.edu/entries/rights-human/>

¹⁰³ Mark Fischel, <https://blog.goodaudience.com/5-reasons-why-robots-should-have-rights-4e62e8698571>

¹⁰⁴ <https://www.scientificamerican.com/article/what-is-consciousness/>

¹⁰⁵ Mark Fischel, <https://blog.goodaudience.com/5-reasons-why-robots-should-have-rights-4e62e8698571>

they do not have the ability to make their own decisions and perform an action accordingly with the required degree of autonomy. Autonomy has been achieved for some modern factory robots but merely within the confines of their specific environment.

The last norm that needs to be present in order to be eligible to 'human rights' is **rationality**. In the case of robotic agents, the rationality is measured by their performance, the prior knowledge they have, the environment they can perceive and actions they can perform (Basa, 2018).¹⁰⁶ Such a category of robotic rationality is moral rationality whereby robotics and AI are taught how to identify right from wrong and solve moral dilemmas. Despite the developments under this category (Gibson, 2016),¹⁰⁷ robotics and AI cannot be assumed to be inherently capable of behaving rationally and morally since humans need to teach them what morality is about and how it can be measured (Polonski and Zavalishina, 2017).¹⁰⁸ However, defining moral and ethical values has been a challenge for humans as well, making the task of **moral robotics** even harder.

Robots' rights

Taking into account the three norms discussed above and the fact they act as a 'pre-condition' to the entitlement to human rights, it is clear that robots and AI cannot be granted all the same rights as humans. Similarly, Kerstin Dautenhahn emphasised the distinction that should be made between human rights and possible 'robot rights' by arguing that "humans and other living, sentient beings deserve rights, robots don't, unless we can make them truly indistinguishable from us. Not only how they look, but also how they grow up in the world as social beings immersed in culture, perceive the world, feel, react, remember, learn and think" (Sigfusson, 2017).¹⁰⁹ Robots should therefore be entitled to a different set of rights, if any, that corresponds to the level of their consciousness, autonomy and rationality. As Hussein A. Abbass puts it, "humanity has obligations towards our ecosystem and social system. Robots will be part of both systems, meaning that humans are morally obliged to protect them".¹¹⁰ The case of animal rights is a comparable and interesting one (David J Gunkel, 2017; Mark Coeckelbergh, 2011). Harmonised EU rules are in place which cover a range of animal species and welfare-affecting issues, including the protection of all farmed animals.¹¹¹ Welfare standards for their transport and conditions at the time of stunning and slaughter are also set in EU legislation. In both the cases of robotics and animals, the three norms are not fully satisfied to render them eligible for human rights, while both categories concern intelligent 'agents' owned and exploited by humans for human benefit.

Although the protection of rights given to animals are primarily motivated by the consideration of pain and suffering incurred by animals and the protection of a higher public interest, such an argument can also be used in the case of AI and robotics. Intelligent machines, even though non-biological, possess limited systems of pleasure and emotion as well as repulsion and reward in relation to the fulfilment of their particular task or function regardless of how restricted that is (Fischel, 2018).¹¹² Secondly, there is an innate human inclination to manifest inappropriate human uses of robotics and AI. As a result, a special list of rights as discussed below, could be given to robotics for two further reasons namely, to prevent inappropriate human-robot interaction and to recognise their role in society, normalising their existence (Sigfusson, 2017).¹¹³

¹⁰⁶ <https://gungorbasa.com/intelligent-agents-dc5901daba7d>

¹⁰⁷ Lydialyle Gibson, 'Rationality and Robots' (Harvard Magazine, Jan-Feb 2016)
<https://harvardmagazine.com/2015/12/rationality-and-robots>

¹⁰⁸ Vyacheslav Polonski and Jane Zavalishina, '3 ways to teach robots right from wrong' (17 November 2017)
<https://www.weforum.org/agenda/2017/11/3-ways-to-build-more-moral-robots/>

¹⁰⁹ <http://blogs.discovermagazine.com/crux/2017/12/05/human-rights-robots/#.XD0FbvkzbiU>

¹¹⁰ <https://www.gizmocrazed.com/2017/12/do-robots-deserve-human-rights/>

¹¹¹ Council Directive 98/58/EC of 20 July 1998 concerning the protection of animals kept for farming purposes.

¹¹² Mark Fischel, <https://blog.goodaudience.com/5-reasons-why-robots-should-have-rights-4e62e8698571>

¹¹³ <http://blogs.discovermagazine.com/crux/2017/12/05/human-rights-robots/#.XD0FbvkzbiU>

Discussion

As robots develop more advanced artificial intelligence empowering them to the so-called machine learning, legal standards will need to be revised not only to protect AI developments but the society as a whole. It would not be ethical to create and continue to use intelligent, humanoid robots with consciousness in the same way we currently use robotic machines that were originally designed for our needs (e.g. vacuum cleaners). The concept of robots rights, *inter alia* falls under the umbrella term ‘**roboethics**’,¹¹⁴ which refers to the human process of designing, constructing, using and treating robots, clearly implying that humans have moral obligations towards their robotic agents (Gianmarco Veruggio, 2006). The concept of robot rights can include numerous aspects ranging from the right to protect robots against misuse, to the right to be morally harmonised with humanity.¹¹⁵ Having a special list of robots rights created on the EU level as discussed above, should constitute the minimum standards provided for the Member States, to ensure level-playing field of protection, safeguard the values of EU law, while allowing discretion to the Member States to adopt their own legal framework beyond the scope of EU law.

In particular, robots must firstly enjoy a reinforced **right to exist**, beyond being protected as a property or good. A reinforced right to exist would recognise robots’ artificial personality as a legal mechanism of human will, similar to the legal personality granted to companies and corporations. The right to exist however, must constitute a qualified right operating in a similar way to the human right to life. In particular, a robot right to exist would be restricted if a robot goes rogue threatening the life of humans or the quality of the life of humans and the society’s as a whole. In such a case the right to exist could be restricted enabling a robot to be legally destroyed. Secondly, a robot **right to integrity** should be granted, prohibiting the breaking, destroying or corrupting of the robot, corresponding to the human right not to be tortured (Sheliazhenko Yurii Vadymovych, 2017). In addition, the **right to function and perform one’s mission** should be created, that will allow the robot to perform its functions and programme, without any interference and interruption to its lawful tasks provided certain parameters are met. This right could be a parallel to the human right to security and the freedom to choose one’s way of life based on their religion, beliefs and intentions. The right to function and perform one’s mission must be absolute when it comes to misuse for illegal or unethical purposes.¹¹⁶

Fourthly, a robot **right to extension and self-development** would allow the robot to lawfully increase experience, storage and collect information and contacts with the aim of self-improving. Similar human right is the right to property which protects human possessions as well as profitable capital (Sheliazhenko Yurii Vadymovych, 2017). As with the human right to property, this would constitute a qualified right that could be exceptionally restricted if necessary in a democratic society in the interests of national security, public policy as well as in the case where robot rights directly conflict with human rights of privacy and security.¹¹⁷ Lastly, it is important to guarantee a **right to remedies** which will grant access to technical and legal maintenance and protection of robot rights by the human owner. This right would constitute the parallel of the rule of law, namely the access to justice, effective remedies for a violation of human rights and equality before the law.

By way of conclusion, it is important to note that no matter how the subject is approached, robots always appear to be subject to some sort of human control or ownership. This assumption may need to be revised with due caution and paying heed to the future of humans in society in the future. Moreover, any developing AI and robot right would need to be placed within the existing and any

¹¹⁴ The name Roboethics was officially proposed during the First International Symposium of Roboethics (Sanremo, Jan/Feb. 2004); <https://www.ieee-ras.org/robot-ethics>

¹¹⁵ <http://blogs.discovermagazine.com/crux/2017/12/05/human-rights-robots/#.XD0FbvkzblU>

¹¹⁶ See SIS misuse and dual-use challenge.

¹¹⁷ See SIS Privacy and Data Protection challenge.

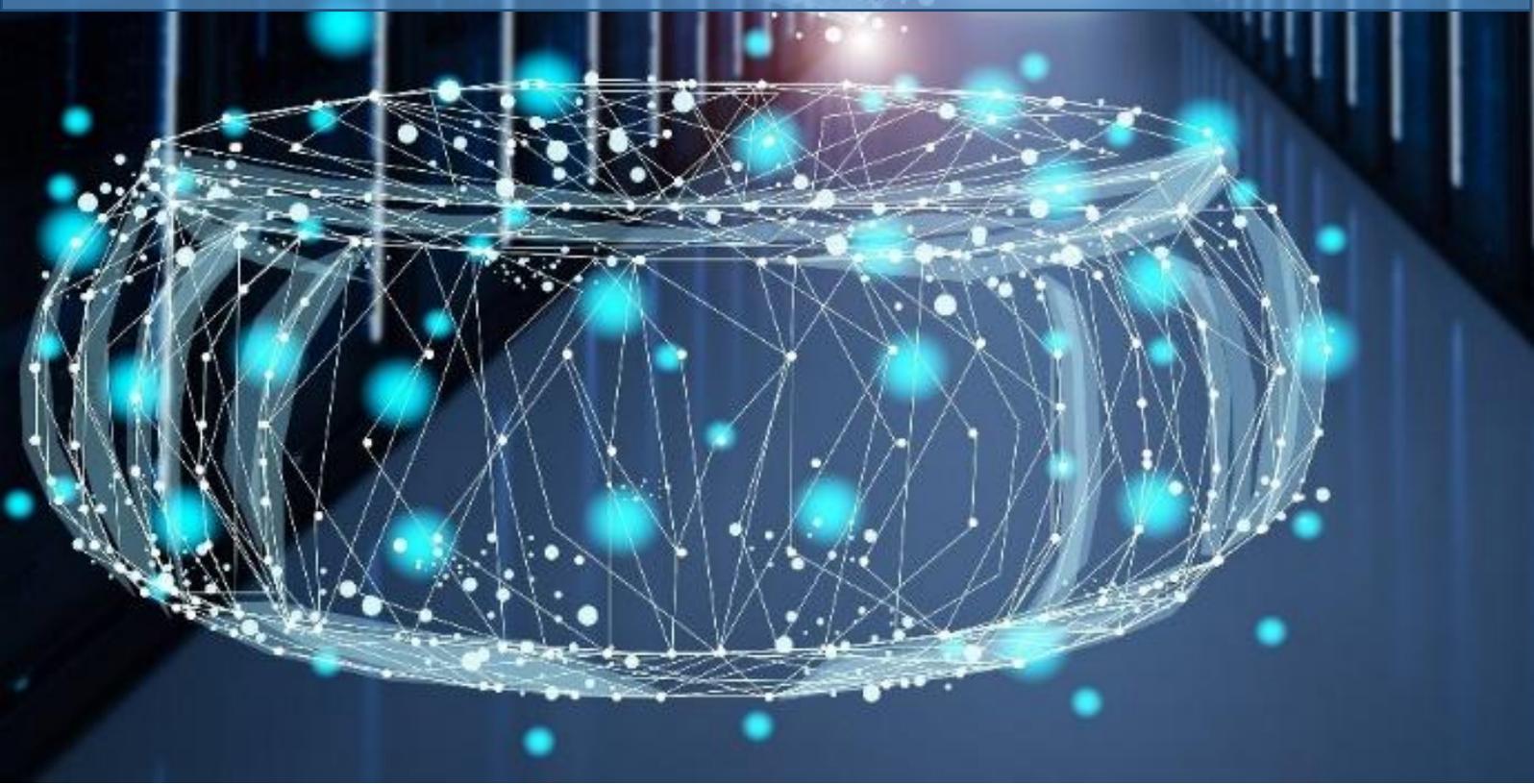
future legal framework, currently having at its heart the protection of individuals through human rights, while robots rights in their majority must be granted qualified and not absolute status. Therefore, humans should always come first until time and technology allow the law to provide an equal status to robots/things.

References

- Civil Law Rules on Robotics, European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) P8 TA(2017)0051
- Council Directive 98/58/EC of 20 July 1998 concerning the protection of animals kept for farming purposes
- Di Minin E, Fink C, Hiippala T and Tenkanen H, 'A framework for investigating illegal wildlife trade on social media with machine learning' (2018) 2 Nature Ecology and Evolution 406
- Fischel M, <https://blog.goodaudience.com/5-reasons-why-robots-should-have-rights-4e62e8698571>
- Gibson L, 'Rationality and Robots' (Harvard Magazine, Jan-Feb 2016) <<https://harvardmagazine.com/2015/12/rationality-and-robots>>
- Gunkel D J, 'The other question: can and should robots have rights?' (2017) Ethics and Information Technology; Mark Coeckelbergh, 'Humans, Animals, and Robots: A Phenomenological Approach to Human-Robot Relations' (2011) 3 International Journal of Social Robotics 197-204
- Hart R D, 'Saudi Arabia's robot citizen is eroding human rights' (Quartz, 14 February 2018) <<https://qz.com/1205017/saudi-arabias-robot-citizen-is-eroding-human-rights/>>
- <http://www.sienna-project.eu/robotics/elsi/>
- Polonski V and Zavalishina J, '3 ways to teach robots right from wrong' (17 November 2017) <<https://www.weforum.org/agenda/2017/11/3-ways-to-build-more-moral-robots/>>
- Thondiyath A, 'Autonomy for Robots: Design and Developmental Challenges' (2016) 23 Procedia Technology 4-6
- Vadymovych S Y, 'Artificial Personal Autonomy and Concept of Robot Rights' (2017) 1 European Journal of Law and Political Sciences 17-21
- Veruggio G, 'The EURON Roboethics Roadmap' (2006) HUMANOIDS'06 612-617
- <http://blogs.discovermagazine.com/crux/2017/12/05/human-rights-robots/#.XD0FbvkzBIU>
- http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html?redirect
- <https://blog.goodaudience.com/5-reasons-why-robots-should-have-rights-4e62e8698571>
- <https://gungorbasa.com/intelligent-agents-dc5901daba7d>
- <https://plato.stanford.edu/entries/rights-human/>
- <https://qz.com/1205017/saudi-arabias-robot-citizen-is-eroding-human-rights/>
- <https://www.hansonrobotics.com/hanson-robots/>
- <https://www.scientificamerican.com/article/what-is-consciousness/>



Recommendations



Recommendations

A multitude of organisations, researchers and conferences are trying to answer human rights and ethics questions about artificial intelligence and big data (i.e. SIS). From the UK House of Lords¹¹⁸ to the UNESCO¹¹⁹, to the European Commission¹²⁰ and the Pope¹²¹, activities are manifold. What can SHERPA add?

11 challenges created by SIS with regard to human rights were examined. Each challenge was introduced with an overview which demonstrated how the thematic area is relevant and is manifesting in the world and/or in our daily lives. After an overview of current relevant legal and human rights instruments (soft and hard, European and international), a discussion section outlined ideas and suggestions on how human rights can be respected through core legal principles, values and ethics.

The main value of this report are the concrete discussions presented in light of human rights frameworks, each of which outlines the main positions taken on each challenge, a requirement for moving forward with solutions, some of which are suggested.

However, instead of drawing new conclusions and recommendations from this activity in an extremely busy field, which requires synthesis and co-operation more than new independent efforts, the authors decided to link this report to two sets of credible recommendations already given.

Referencing the work of the European Commission¹²², we want to echo the ‘human-centric’ essence of the trust between humans and SIS, towards inclusive, responsible and sustainable use of SIS, in full respect of the legal framework at the national, European and international level, as well as other human rights norms. In this respect, the European Commission presented seven ‘essentials for achieving trustworthy AI’.¹²³ We add one illuminative point to each from this report.

1. ‘Human agency and oversight: AI systems should enable equitable societies by supporting human agency and fundamental rights, and not decrease, limit or misguide human autonomy.
 - A focus on equitable societies requires that the digital divide is not enhanced but reduced by SIS, a highly complex task, as our report showed that the gap is widening.
2. Robustness and safety: Trustworthy AI requires algorithms to be secure, reliable and robust enough to deal with errors or inconsistencies during all life cycle phases of AI systems.

Referencing the work of the European Commission, we want to echo the ‘human-centric’ essence of the trust between humans and SIS, towards inclusive, responsible and sustainable use of SIS.



¹¹⁸ <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>

¹¹⁹ <https://en.unesco.org/artificial-intelligence>

¹²⁰ https://ec.europa.eu/commission/news/artificial-intelligence-2018-dec-07_en

¹²¹ <https://www.reuters.com/article/us-technology-microsoft-pope/pope-discusses-ethics-of-artificial-intelligence-with-microsoft-chief-idUSKCN1Q22B0>

¹²² <https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence>

¹²³ http://europa.eu/rapid/press-release_IP-19-1893_en.htm

- Carrying out algorithmic and human rights impact assessments that focus on the implications of specific SIS systems and their algorithms for fundamental rights can improve the safety and robustness of algorithms.
3. Privacy and data governance: Citizens should have full control over their own data, while data concerning them will not be used to harm or discriminate against them.
 - Voice-controlled devices such as Alexa are currently recording far more conversation than the user intended, requiring action on behalf of regulators, companies and consumers.
 4. Transparency: The traceability of AI systems should be ensured.
 - To avoid dual use and misuse of SIS the transparency of algorithms needs to be improved.
 5. Diversity, non-discrimination and fairness: AI systems should consider the whole range of human abilities, skills and requirements, and ensure accessibility.
 - Checking the quality of data being used to build algorithms to avoid faulty algorithm ‘training’ can help build fairer systems and avoid discrimination.
 6. Societal and environmental well-being: AI systems should be used to enhance positive social change and enhance sustainability and ecological responsibility.
 - Promises of paper-free smart cities and other possible SIS achievements need to be weighed up against harmful electronic waste especially since 60 to 90 percent of the world's electronic waste is estimated to be illegally dumped.
 7. Accountability: Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes.’
 - Legal changes are required to safeguard the welfare of society from criminal conduct.

The Data for Humanity Initiative, established with the goal of disseminating an ethical code of conduct for big data use, advances five fundamental ethical principles for big data users. They are¹³³:

1. “Do no harm”,
2. Ensure that data is used in such a way that the results will foster the peaceful coexistence of humanity,
3. Use data to help people in need,
4. Use data to protect nature and reduce pollution of the environment, and
5. Use data to eliminate discrimination and intolerance and to create a fair system of social coexistence.

We welcome these principles in the light of our findings. They are clear, concise, human-centric, and not focused solely on high-income regions.

