Ethics Advisory Group

REPORT
2018

EDPS
EUROPEAN DATA PROTECTION SUPERVISOR

Towards a digital ethics

EDPS Ethics Advisory Group

Foreword

When I first espoused ethics three years ago, while the legislative procedure for the adoption of the EU's General Data Protection Regulation was still underway, it is fair to say my initiative raised a few eyebrows.

Today, ethics and data protection are intertwined like never before and I observe an ever closer convergence between the two. Many issues related to ethics involve personal data; data protection authorities now face ethical questions that legal analysis alone cannot address.

Ethics and the law each have an important role in our societies. Convergence allows us to put the human being, their experience and dignity at the centre of our deliberations.

This report by the members of the EDPS's Ethics Advisory Group engages thoughtfully with this question. The report presents the main shifts provoked by the digital revolution and the impact they have on the values we hold dear.

I am grateful to the group for helping to advance this still young debate on digital ethics. The EDPS will continue, over the coming months and through the 40th edition of the International Conference of Data Protection and Privacy Commissioners which we host in October, to consider more deeply and widely how we can make technology work in the interests of the dignity of the human being.

Giovanni Buttarelli
European Data Protection Supervisor

The Ethics Advisory Group (EAG) is composed of six Members:

J. Peter Burgess holds the chair in the Geopolitics of Risk at the Ecole Normale Supérieure, Paris, is Professor at the Centre for Advanced Security Theory (CAST) of the University of Copenhagen, and member of Interdisciplinary Research Group on Law, Science, Technology and Society Studies (LSTS) of the Vrije Universiteit Brussel. Trained in engineering, literary studies, political science and philosophy, his research and writing focus mainly on the theory and ethics of security and insecurity.

Luciano Floridi is Professor of Philosophy and Ethics of Information and Director of Research of the Digital Ethics Lab, Oxford Internet Institute, University of Oxford. He is also Turing Fellow and Chair of the Data Ethics Group of The Alan Turing Institute. The philosophy and ethics of information have been the focus of his research for a long time, and are the subject of his numerous publications, including The Fourth Revolution: How the Infosphere is Reshaping Human Reality (Oxford University Press, 2014), winner of the J. Ong Award.

Jaron Zepel Lanier is an American computer philosophy writer, computer scientist, visual artist, and composer of classical music. A pioneer in the field of virtual reality, Lanier and Thomas G. Zimmerman left Atari in 1985 to found VPL Research, Inc., the first company to sell VR goggles and gloves. In the late 1990s, Lanier worked on applications for Internet2, and in the 2000s, he was a visiting scholar at Silicon Graphics and various universities. From 2006 he began to work at Microsoft, an Interdisciplinary Scientist in Microsoft Research from 2009 to 2018, and currently working in the Office of the CTO, Prime Unifying Scientist (OCTOPUS).

Aurélie Pols is an economist/econometrist and statistician by education and has been involved in the analysis of data from the very beginning of this activity. She is an important actor in the field of "digital data". She runs her own consulting business in Spain after selling her own first start-up company a few years ago.

Antoinette Rouvroy is Doctor of Laws of the European Uni-versity Institute (Florence), she is permanent research associate at the Belgian National Fund for Sci-entific Research (FNRS), senior researcher at the Research Centre Information, Law and Society, Law Faculty, and Professor of "Questions of applied ethics after the digital turn» in the Department of Philosophy at the University of Namur (Belgium). In her writings, she has addressed, among other things, issues of privacy, data protection, non-discrimination, equality of opportunities, due process in the context of "data-rich" environments (the so-called genetic revolution, the so-called computational turn) with an ap¬proach combining legal and political philosophy. Her current interdi¬sciplinary research interests revolve around what she has called algorithmic governmentality. Under this foucauldian neologism, she explores the semiotic-epistemic, political, legal and philosophical im¬plications of the computational turn (Big Data, algorithmic profiling, industrial personalisation) and the impacts of automated algorithmic processes on human evaluations, decisions and judgments.

Jeroen van den Hoven is University Professor and Professor of Ethics and Technology at Delft University of Technology. He has written extensively on ethical aspects of information technology. He is Founding Editor in Chief of the Journal Ethics and Information Technology, since 1999. In 2009, he won the World Technology Award for Ethics as well as the IFIP prize for ICT and Society for his work in Ethics and ICT. Jeroen van den Hoven was founder, and until 2016 Programme Chair, of the Dutch Research Council on Responsible Innovation. He chaired the EU expert group on Responsible Research and Innovation (RRI) and he is member of the European Group on Ethics (EGE) of the European Commission.

Authors of this report

J. Peter Burgess, Chair

Luciano Floridi

Aurélie Pols

Jeroen van den Hoven

With thanks to
Jaron Lanier & Antoinette Rouvroy
for their valuable advice and contributions

Preface

The EDPS Ethics Advisory Group (EAG) has carried out its work against the backdrop of two significant social-political moments: a growing interest in ethical issues, both in the public and in the private spheres and the imminent entry into force of the General Data Protection Regulation (GDPR) in May 2018. For some, this may nourish a perception that the work of the EAG represents a challenge to data protection professionals, particularly to lawyers in the field, as well as to companies struggling to adapt their processes and routines to the requirements of the GDPR. What is the purpose of a report on digital ethics, if the GDPR already provides all regulatory requirements to protect European citizens with regard to the processing of their personal data? Does the existence of this EAG mean that a new normative ethics of data protection will be expected to fill regulatory gaps in data protection law with more flexible, and thus less easily enforceable ethical rules? Does the work of the EAG signal a weakening of the foundation of legal doctrine, such as the rule of law, the theory of justice, or the fundamental values supporting human rights, and a strengthening of a more cultural approach to data protection?

Not at all.

The reflections of the EAG contained in this report are not intended as the continuation of policy by other means. It neither supersedes nor supplements the law or the work of legal practitioners. Its aims and means are different. On the one hand, the report seeks to map and analyse current and future paradigm shifts which are characterised by a general shift from analogue experience of human life to a digital one. On the other hand, and in light of this shift, it seeks to re-evaluate our understanding of the fundamental values most crucial to the well-being of people, those taken for granted in a data-driven society and those most at risk.

The objective of this report is thus not to generate definitive answers, nor to articulate new norms for present and future digital societies but to identify and describe the most crucial questions for the urgent conversation to come. This requires a conversation between legislators and data protection experts, but also society at large - because the issues identified in this report concern us all, not only as citizens but also as individuals. They concern us in our daily lives, whether at home or at work and there isn't a place we could travel to where they would cease to concern us as members of the human species.

1. Introduction

The EDPS Opinion *Toward a new digital ethics* (2015) grounds the 'new digital ethics' in the fundamental right to privacy and the protection of personal data, understanding both as crucial for the protection of human dignity[1]. The Opinion cites dignity—the bedrock of the European Union Charter of Fundamentals Rights—as the signpost for the new digital ethics. It highlights the interdependence of technology and human values, stressing that, while technological evolution is informed by human values, those same values do not remain untouched by technologies.

The EDPS Opinion identifies several technological trends that require a rethinking of the relation between technology and human values, thus calling for the formulation of a 'new digital ethics': *big data* generated from a variety of sources, from public administrations and private companies, *social networks* and other *online platforms*, *the internet of things* and *networked sensors, cloud computing*, and *artificial intelligence*, in particular machine learning. These digital technologies require what the Opinion calls a 'big data protection ecosystem': an interactive and accountable assemblage of 'future-oriented regulation', 'accountable controllers', 'privacy-conscious engineering', and 'empowered individuals'.

This report aims to provide a preliminary account of the socio-cultural shifts that have taken place in concert with these technological trends, and to examine how European values may be understood as part of the new data protection ecosystem.

Mandate

It is this new ecosystem that is the object of reflection for the EAG, as described in the EDPS 2015-2019 strategy, with the mandate 'to explore the relationships between human rights, technology, markets and business models in the 21st century'[2]. This new data protection ecosystem stems from the strong roots of another kind of ecosystem: the European project itself, that of unifying the values drawn from a shared historical experience with a process of industrial, political, economic and social integration of States, in order to sustain peace, collaboration, social welfare and economic development. This project is sustained by the common destiny of all European citizens and by the principles and practices embodied in the European institutions, including the European Data Protection Supervisor.

With the digital age, European ambition has evolved rapidly. And yet, the fundamental freedoms and values set out in the EU treaties and accords of the last 60 years, and culminating in the Charter of Fundamental Rights of the European Union, ratified in 2000, remain the same. However, bridging the gap between traditional principles and a new digital world, with all its social, legal, and economic implications, is daunting. There is a distinct need to fundamentally revisit the way ethical values are understood and applied, how they are changing or being re-interpreted, and a need

[1] European Data Protection Supervisor (2015) Towards a new digital ethics: Data, dignity and technology. Opinion 4/2015.

[2] European Data Protection Supervisor (2015) Leading by Example: The EDPS Strategy 2015-2019, p. 18.

to take stock of their relevance to cope with the new digital challenges.

The right to data protection may have so far appeared to be the key to regulating a digitised society. However, in light of recent technological developments, such a right appears insufficient to understand and address all the ethical challenges brought about by digital technologies. Personal data protection regimes, like the GDPR, remain the privileged instruments for the governance of data flows and data processing. These remain valuable for the protection of personal data in line with classical data processing. And yet, they appear inadequate to address the unprecedented challenges raised by the digital turn. In particular, the tensions and frequent incompatibility of core concepts and principles of data protection with the epistemic paradigm of big data suggest limits to the GDPR even prior to its application.

For example, the principles of purpose limitation, data minimisation, and data retention may be at odds with some premises and applications of big data aiming at the almost limitless collection and retention of any information that exists in digital format and with the fact that the purpose data may not be known before an algorithmic analysis is carried out. Indeed, the purposes of algorithm-driven big data analysis is often to discover otherwise invisible patterns in the data, rather than to apply previous insights, test hypotheses, or develop explanations.

Moreover, the technical sophistication and complexity of data protection rules, together with that of emerging data processing systems (machine learning and deep learning algorithms, for example), can have the effect of distancing supervisory authorities and undertakings from the meaning and the spirit of the right to data protection. Ethics allows this return to the spirit of the law and offers other insights for conducting an analysis of digital society, such as its collective ethos, its claims to social justice, democracy and personal freedom.

The General Data Protection Regulation

The work of the Ethics Advisory Group has been carried out in anticipation of the General Data Protection Regulation (GDPR), which will become fully applicable on 25 May 2018[3]. The GDPR supersedes the 1995 Data Protection Directive, and strengthens and harmonises the protection of personal data within the European Union. It also expands the territorial scope of the EU data protection regime, by bringing a large number of overseas businesses and other organisations within its reach. The GDPR is itself a true product of globalisation, in that it considers not only the location of the data processing, as in the current Directive, but also whether personal data relating to individuals located in the EU are being processed, regard-

[3] 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), OJEU L119, 04/05/2016.

less of where the controller is established in the world.

While some of the EAG's deliberations concern some of the same issues addressed by the GDPR, its scope, focus, and purpose is different. Where the GDPR is concerned with regulating the processing of personal data, the EAG is interested in understanding the assumptions about both the ethical status or personhood of the individuals whose data is in question in the GDPR and the way these assumptions challenge and appeal to a reinterpretation for the digital age of the fundamental European values and principles that the GDPR seeks to protect. Ethical reflection developed by the EAG seeks to provide concepts and arguments for dealing with regulatory issues that were not and cannot be adequately foreseen. By providing some interpretive tools, arguments and a vocabulary for a digital ethics, the EAG seeks to help the data protection community to make relevant the core values that underpin its work and to ground the application of data protection principles in a way that is more relevant to the everyday experiences of European citizens.

In this sense, the EAG has sought to develop an understanding of human action—behaviour, decision-making, judgment, conduct, etc.—without taking for granted that these can be digitally captured, computed, calculated or optimised. The EAG has focused on understanding conduct that resists digitisation, conduct as contingent, fortuitous, unpredictable, even risky. It sees the ethical moment as the moment of engaging autonomy in the name of something that can neither be calculated nor computed.

By providing interpretive tools, arguments and a vocabulary of ethics for the digital age the EAG seeks to help the data protection community to reassert the core values that underpin its principles and to ground the application of data protection principles in a way that is relevant to the everyday experiences of European citizens.

Scope and aim of the report

This report seeks to propose terms and concepts that contribute to a constructive debate about the future of ethics in a full-fledged digital society. It identifies and clarifies some of the ethical questions that emerge in the application of data protection regulations to the new forms of data collection and processing and to the new economy that has rapidly formed around it.

The EAG expressly avoids an instrumental approach to ethics of a kind that would result in an ethical checklist or set of measures that, once accomplished, would essentially exhaust ethical reflection and release its practitioners from further discussion. The EAG wishes to discourage approaches to ethics governance that equate data protection with the application of do's and don'ts. On the contrary, it seeks to encourage proactive reflection about the future of human values, rights and liberties, including the right to data protection, in an environment where technological innovation will always challenge fundamental concepts and adaptive capabilities of the law. It seeks to inspire all relevant stakeholders to identify the areas where ethical problems not only emerge from the development and operation of today's digital technologies, but integrate in both their designs and business planning reflection about the impact that new technologies will have on society, generating their own guidelines for addressing them tomorrow while remaining vigilant to what their own guidelines had not foreseen, when by all accounts the premise, aims and impact will be astonishingly different from today. Ethical foresight, like technological foresight, will be the key to commercial success in the digital economy.

European data protection in an interconnected world

More than any other human enterprise, the wide-reaching circulation of data through worldwide networks, the global reach of its power to set standards across national borders and its trade and use in the business of everyday life, fulfil even the most audacious visions of globalisation, be they utopian or dystopian. And yet, just as there is a gap between personal knowledge and personal data, there is also a gap between immediate or local human experience and global or universally shared experience. Some kinds of concrete local experience, set free from space and time by the economy of global circulation, will wither and perish. Other kinds will flourish. Human culture does not adapt uniformly to globalisation.

Understanding the human limits to globalisation helps us to understand the limits of data protection regulation. We know that not all human experience lets itself be digitised with equal facility. There is significant variation in what segments of life and experience can be inserted into a digital framework, what information can be transformed or translated to a globally digestible form, what knowledge can produce added-value in the digital economy. Just as there is a limit to what can be globalised in the age of globalisation, there is an inherent limit to what can be digitised in the digital age. Indeed, the question of the limit of digitisation is at the very heart of social and political debate today. The starting point of any ethical reflection on the digital age is the simple observation that human beings are not identical to their data, despite the increasing precision with which human beings can be digitally modelled, their qualities and properties catalogued, their patterns systematised and their behaviour predicted. On the contrary, they may be understood in an infinite number of ways.

The work of the EAG is founded on the belief of the universality of human values. However, history teaches us that these values must be understood and implemented in the social, cultural, political, economic and not least, technological contexts in which the crucial link between personal data and personal experience is made. In other words, any digital ethics should also make us aware of the widely changing relationship between digital and human realities. Notwithstanding the great variety in which different countries around the globe respond to the challenges of digitisation, there are commonalities in how human beings experience the digital world and in how they may become vulnerable in light of their new technological condition.

While the work of the EAG is set in a European context, the concerns are global and can be observed beyond Europe (e.g. development of social scoring in China, biometric identification in India, the weakening in the USA of legal constraints on digital markets such as privacy, net neutrality). The EDPS strategy stipulates that the EU should lead the conversation on the ethical consequences of the digital transformation. Digital Ethics will therefore be the core topic of the 2018 international conference of Data Protection and Privacy Commissioners hosted by the EDPS in Brussels. The report of the EAG intends to contribute to the reflection to launch this global debate.

The EDPS Ethics Advisory Group work process

Since it began its work in March 2016, the EAG has met 9 times and convened two workshops aimed at collecting input and reactions from different communities.

The first workshop, held on 31 May 2016, was organised to interact with members of the data protection community. The workshop helped the EAG to understand the perceptions and concerns in relation to the GDPR. The discussions raised questions about the role of ethics in the relation between law and technological innovation. It led the EAG to consider the unique boundaries between ethics and law and the question of where the law ends and where ethics begins.

The second workshop, held on 18 May 2017, focused on the pragmatic challenges involved in squaring the radically new means and methods enabled by the digital revolution with the equally unique ethical issues generated by new digital technologies. To this end, the workshop was aimed at members of the data science community and data engineers.

Through these workshops, and subsequent discussions it became clear that the task of the EAG was not to define the rights and wrongs of navigating the digital ecosystem. It was rather about posing a broader and more primordial set of questions about what it means to do ethics in the digital age; about how to construe the object of ethical analysis about how to make explicit how the preconditions and aims of ethics have changed in the new digital age, and about where ethics will need to adapt in the future.

Digital ethics can be understood from a number of perspectives.

A basic distinction is commonly drawn in ethical reflection between normative (or prescriptive) ethics and metaethics. Normative ethics involves reflection leading to the formulation of moral standards intended to regulate conduct. Metaethics is concerned with discovering and formulating the cultural, social, political and value-based conditions formulating rules of moral conduct. In its deliberations the EAG took the consensus-based decision to focus primarily on metaethical questions of digital ethics. Its work thus consisted of considering more general and fundamental questions about what it means to make claims about ethics and human conduct in the digital age, when the baseline conditions of 'human-ness' are under the pressure of interconnectivity, algorithmic decision-making, machine-learning, digital surveillance and the enormous collection of personal data, about what can and should be retained and what can and should be adapted, from traditional normative ethics.

This led the EAG to confront a range of questions:

- how to link new data technologies to European values;
- the meaning and consequences of human interactions with machines;
- dignity in situations of declining autonomy;
- the market's power to define what it means to be human;
- the dilemma of the multitude of choices provided by a digital ecosystem that is controlled by new forms of automation;
- new challenges brought to traditional understandings of ownership and property rights applied to personal data; and
- responsible innovation in the digital ecosystem.

2. Socio-cultural shifts of the digital age

Below we highlight the seven 'shifts' that define the new landscape for digital ethics to emerge, to map problems, questions and concepts in each.

From the individual to the digital subject

Responding to a growing demand for personalised experiences, direct encounters between persons in the digital world are increasingly replaced by remote algorithmic profiling. As a consequence psychological, spiritual, cultural, social, moral and other qualities of persons tend to be more often detected through personal data, directly mined, or triangulated through multiple sources, as well as by asserting personal identity through traditional means of self-affirmation, individual or collective identity claims, group recognition, conventional social network, or conventional political categories. Today identity is often established through digital constructs and patterns. Yet in the new digital age, we must remember that data exhausts neither personal identity, nor the qualities of the communities to which individuals belong, that data protection is not only about the protection of data, but primarily about the protection of the persons behind the data.

The persuasiveness of algorithmic processes, which seek to optimise human interactions in a growing number of sectors, nurtures a perception that digitisation is only one among many possible ways of representing the world and its inhabitants and the digital transcription of behaviours and propensities is neither neutral nor exhaustive. The question is whether the digital representation of persons may expose them to new forms of vulnerability and harm. Data protection is not a technical or legalistic matter. It is a profoundly human one. The reflection of the EAG and the present report have consistently drawn upon the wide-reaching premise of an ontological shift in governance from an analogue logic to a digital one. Individuals, as well as public and private organisations, experience the world differently as a result of the socio-cultural shifts of the digital age. The traditional representations of identity and the self, morality, social relations, cultural belonging and political action are undergoing a number of socio-cultural shifts due to digitisation. As a consequence of these socio-cultural shifts, individuals, as well as public and private sector organisations experience the world differently.

From analogue to digital life

Human life may be understood by reference to the values that people hold and express through their social, cultural and political activities. Today the experience of persons as moral beings who think in moral terms, experience pleasure and pain in aesthetic and affective terms, participate in social relations with other individuals whom they consider worthy of recognition and who express and confront life in and through emotions, typically experienced and expressed through digital means as an aggregate of digital facts detached from the social, cultural, and historical conditions of life. As a consequence, digitisation puts pressure on our traditional understandings of the scope and limits of personhood, of its non-digital values and non-digital customs.

From governance by institutions to governmentality through data

Traditional expectations of governance in Western societies is based on an assumption that distinct institutions hold the power to govern and are held democratically accountable for their application of power. The governing and the governed are distinct, but nonetheless linked by mutually recognised principles of legal obligation and accountability.

Digital technologies have changed all this profoundly. The use of algorithms and large data sets can shape and direct the lives of individuals. Individuals may be increasingly governed on the basis of the data generated from their own behaviours and interactions. The distinction between the forces that govern everyday life and persons who are governed within it thus become more difficult to discern. In some contexts, algorithmic profiling – carried out by means of behavioural economics for purposes ranging from exploiting detected vulnerabilities in personalised marketing strategies to the influencing of human behaviours through environmental, contextual, informational stimuli – gradually transform how we may govern ourselves. Behaviour may be governed by 'nudging', that is by minute, barely noticeable suggestions, which can take a variety of forms and which may modify the scope of choices individuals have or believe they have. Because influences are minute and often unnoticed, while at the same time remaining within the bounds of democratic norms, nudging can be used together with forms of artificial intelligence and large quantities of data to promote particular interests or values. This shift represents a change in our premise about what it means to govern ourselves and be governed by others, to marshal political power and to influence perceptions, choices and behaviours of persons.

From a risk society to scored society

It has been common for institutions and organisations to collect and aggregate information in order to improve situational awareness for decision-making about the future. In the so-called risk society, risk assessment is carried out using techniques of probability calculation, allowing individuals to be pooled and situations with the same level of risks to be identified with each other for the purposes of understanding the value of loss and the cost of compensation. In the digital age, algorithms supported by big data can provide a far more detailed and granular understanding of individual behaviours and propensities, allowing for more individualised risk assessments and the apportioning of actual costs to each individual; such assessment of risk threatens contractual or general principles and widely shared ideas of solidarity.

In this scored society, individuals can be hyper-indexed and hyper-quantified. Beliefs and judgments about them can be made through opaque credit or social scoring algorithms that must be open to negotiation or contestation. The tendency to replace aggregations of potential costs in terms of loss, damages or harms with 'real', 'individualised' costs, challenges conventional theories of justice or fairness, putting in doubt the role of solidarity in the face of uncertainty and challenges the premise of the social contract that makes us a society. Shifts of this kind suggest changes in the norms and methods available for describing, understanding and analysing social relations, replacing the interpretation of human intentions and conditions with the likelihood of numeric correlation between inputs to human action and their outputs.

From human autonomy to the convergence of humans and machines

An increasing number of technological artefacts, from prostheses like eyeglasses and hearing aids, to smartphones, GPS, augmented reality glasses and more, can be experienced in a symbiotic relationship with the human body. These artefacts are experienced less as objects of the environment than as a means through which the environment is experienced and acted upon. As such, they may tend toward a seamless framing of our perception of reality. They may shape our experience of the world in ways that can be difficult to assess critically. This phenomenon of incorporation or even embodiment of technologies is even more intense whenever the devices are implanted in the body.

A parallel frontier of convergence between human and machines is on the verge of being crossed by intelligent, or rather 'autonomous', machines that are able to adapt their behaviours and rather than merely executing human commands, collaborate with, or even replace human agents to help them identify problems to be solved, or to identify the optimal paths to finding solutions to given problems.

From individual responsibility to distributed responsibility

We are becoming familiar to problems of many hands and problems of collective action and collective inaction, which can lead to tragedies of the commons and problematic moral assessments of complex human endeavours, both low and high tech, where a number of people act jointly via distant causal chains, while being separated in time and space from each other and from the aggregated outcomes of their individual agency. The problems of allocation and attribution of responsibilities are exacerbated by the networked configuration of the digitised world. It seems that our conception of responsibility and control are hard to reconfigure in increasingly complex eco-systems of big data and advanced digital technology. Algorithmic transparency and accountability are among the most vividly debated themes of our time, yet, rendering algorithms more transparent and accountable can never decrease or alleviate the responsibility of human agents.

From criminal justice to pre-emptive justice

In legal practice, the detection and investigation of crime is no longer only a science of criminal acts, of identifying and adjudicating events authored by identifiable, accountable individual actors under precise conditions and in terms of moral and legal responsibility, but also a statistically supported calculation of the likelihood of future crime, a structuring of the governance of crime around the science of possible transgression and possible guilt, removing moral character from the equation. The aim of criminal justice remains the same: to provide security within society while at the same time adhering to high standards of human rights and the rule of law. However, the shift that marks one of the main backdrops of the digital age and calls for a new digital ethics is that of trying to predict criminal behaviour in advance, using the output of big data-driven analysis and smart algorithms to look into the future.

The shift is twofold. First, the object of legal regulation can become less interesting, as a phenomenon in the here-and-now and more an object for reasoned speculation about its future role, all based on the predictive powers of the big data and algorithmic processing. Second, while the analysis of legal issues is being pushed into the future, what is understood as existing in the future becomes drawn into the assessments of the present. Estimates of what the future will hold, generated through the patterns gathered in big data analysis, are continuously gaining in importance for the way criminal justice operates today and is purported to operate tomorrow.

3. Ethical reflection for the digital age

As a result of these shifts, it becomes clear that the key concepts that have supported our understanding of our lives, society and social and political order, no longer adequately relate to a world dramatically changed by the rise of digital technologies. An early warning of this misfit is the increasing number of traditional concepts that have had to be amended in order to mark their external transformation and extended scope, changing their semantics in yet unexplored ways. 'Privacy' becomes 'digital privacy', 'trust' becomes 'trust online', 'friendship' is 'Facebook friendship', a 'community' is a 'cyber-community', 'intelligence' becomes 'artificial', 'democracy' becomes 'tele-democracy', 'reality' becomes 'virtual', and so forth. These new terms indicate a novelty. The impact of these new concepts and the phenomena they describe places European data governance in uncharted territory.

The new digital age generates new ethical questions about what it means to be human in relation to data, about human knowledge and about the nature of human experience. It obliges us to re-examine how we live and work and how we socialise and participate in communities. It touches our relations with others and perhaps most importantly, with ourselves. If we accept the idea of a new digital reality, we also accept that it brings with it changing conditions of being human. It invites a new ethical evaluation, a new interpretation of some of the fundamental notions in ethics, such as dignity, freedom, autonomy, solidarity, equality, justice, and trust; and invites us to test the conditions of their validity for the new realities that present themselves in this new age.

In its deliberations, the EAG has regarded this kind of ethical reflection as a means to fill critical gaps in existing legal regulations and as a way of supporting those actors who work to adapt ethical principles to rapidly evolving issues, which often outpace the evolution of law. It is in this way that the EAG has understood the EDPS strategic call to assess 'the ethical dimension beyond data protection rules'. The EAG undertakes this work with a sense of urgency, based on the recognition that common sense and traditional notions of individual responsibility and ethics have come under pressure and risk becoming irrelevant.

Digital ethics does not refer to a radically new idea. From the moment the first computational devices and the first digital computers became available in the 1960's, ethical questions were raised, and a number of different approaches contributed to what can be called in hindsight digital ethics: social informatics, computer ethics, information ethics, Science and Technology Studies (STS), technology assessment, value sensitive design, democratic design, professional ethics for the IT field (IEEE, ACM, IFIP).

The purpose of digital ethics is not only to account for the present, but also to perform a foresight function. Such a function has many layers. Two of them are taken into consideration in this report. One is an anticipatory function, preparing technology users and policy-makers and providers for potential concerns lying on the horizon and requiring technologies to hold tools and concepts able to confront our evolving digital reality. The other is to develop means for empowering individuals and groups to confront anxieties linked to both the potential weakening of fundamental rights and to technological uncertainty itself.

Technological change has a significant societal impact that is nonetheless experienced across a range of individual experiences. In the consensus view of the EAG digital ethics will provide new terms for identifying, analysing and communicating new human realities, in order to displace traditional value-based questions and identify new challenges in view of values at stake and existing and foreseeable technological changes.

4. From foundational values to digital ethics

A re-assertion of the fundamental values at the heart of European data protection and other fundamental rights and liberties is needed in order to make way for a reflection and debate on the implications of the new digital technologies in relation to Fundamental and Human Rights and the basic principles at the heart of the European project. As we enter the coming era, new concepts of data protection will be called for. New kinds of digital opportunities, risks, benefits and harms will need to be conceptualised and addressed. In the new big data ecosystem, unprecedented commodification of data gathered from persons, behaviours and environments can be expected. This new ecosystem will directly challenge traditional European values of dignity, autonomy, freedom, solidarity, equality, democracy and trust.

Dignity

The notion of human dignity in the European intellectual tradition has its origins in the Kantian idea that human beings are to be understood as ends in themselves and never as a means alone. Since the end of World War II in particular, this concept has had a key impact on International Human Rights Law, in legal scholarship and in jurisprudence. It has also been acknowledged as a foundational value in most human rights instruments. The Universal Declaration of Human Rights of 1948 recognises that the inherent dignity and the equal and inalienable rights of all members of the human family are the foundation of freedom, justice and peace in the world. It appears in every iteration of the Treaty of European Union (or Community) beginning from the Treaty of Rome (1957) together with freedom, democracy, equality, rule of law, and respect for human rights, as one of the core values of the European project. The Charter of Fundamental Rights of the European Union explicitly acknowledges the foundational role of the value of human dignity.

Revisiting the concept of dignity will, for example, provide a foundation for the ethical assessment of a range of next generation algorithmic profiling techniques which are increasingly deployed in most sectors of activities and government. The aim of these techniques is the anticipation and where necessary or useful, the influencing of future paths, behaviours, preferences and performances of individuals. In the age of big data, this corresponds to the intensification of algorithmic profiling and 'personalisation'. When individuals are treated not as persons but as mere temporary aggregates of data processed at an industrial scale so as to optimise through algorithmic profiling, administrative, financial, educational, judicial, commercial and other interactions with them, they are arguably, not fully respected, neither in their dignity nor in their humanity.

Freedom

Like dignity, freedom is one of the foundational values of the European Union and a pillar of the common provisions of the Treaty of European Union. Since 1999, it has, in addition, been the core feature of the Schengen political program of offering all EU citizens an 'area of freedom, security and justice'. In its core European ethical and judicial formulations, freedom is understood as a determining, positive right. It determines in the sense that it is not regarded as unconditional, but rather made meaningful by its insertion into the European system of values, underpinning a specific system of laws, directives, communication and international obligations.

The digital age reposes the question of what freedom means, how and to what extent our common and individual sense of freedom is shaped and nourished by information and how new configurations of data and data flows contribute to the production of new kinds of freedom. Freedom will need to be increasingly considered as a product of the digital age. In some cases, citizens will find it increasingly difficult to understand their freedom and its value, independently of their digital experience.

Thus, the World Summit on the Information Society, convened under the auspices of the United Nations in 2003, declared that access to the internet is henceforth to be considered a requirement in order to exercise and enjoy one's rights to freedom of expression and opinion, stipulated in Article 19 of the Universal Declaration of Human Rights. At the same time, freedom to navigate the web is enabled by decisions about technological functions. These functions are part of the background assumptions of most users. These technological settings function like political assumptions about freedom in the internet. They are the tacit governing premise for online life, silently and invisibly allocating band-width, routing data and regulating speed. The suppression of 'net-neutrality' by the U.S. Federal Communications Commission will disrupt a range of premises of digital use that up until now have been taken for granted.

Autonomy

The concept of individual autonomy is also deeply rooted in the Kantian concept of the human person and its dignity. It is an individual capability and a collective potential, the implementation of which is always a matter of degree. Threats to autonomy in the digital age can be observed as circumstances or modes of government that prevent people from developing and/or effectively implementing their potential for autonomy. Such threats include the potential substitution of computational or algorithmic optimisation for human deliberation and decision-making over time, eroding rather than sustaining human potential for autonomy. They include the algorithmic or human spreading of fake news that weakens the capacity of individuals to discriminate between what is reliable information and what is not. Similarly, democratic processes risk being weakened through new practices of political marketing relying on micro-targeting and algorithmic psychographic profiling. This includes automated decisions taken by digital systems on the basis of continuous observation of the choices, behaviour and emotions of individuals, without the possibility for them to understand and communicate their own motivations, intentions, reasons, and explanations or to take autonomous decisions.

Solidarity

Solidarity refers to a relation to others, the unity of community values, aims, interests, objectives or standards, past, present and future. In its most elementary form, solidarity corresponds to something shared, something that holds a group together in an environment. Solidarity has played a key role in the geopolitical discourse of European construction from its very origin. It is a core concept of Title IV of the Charter of Fundamental Rights, which contains guiding provisions about societal security, health care, access to economic services and consumer protection, to name a few.

Threats to solidarity and empowerment in the digital age are a consequence of the shift to a scored society as outlined in chapter two. They take the form of hyper-individualisation and for a focus on 'real' costs through, for example, behavioural profiling in the context of insurance, the interconnectedness of databases and the use of medical data in the context of employment or in breaches of context-specific rules of confidentiality.

Equality

Like solidarity, equality is a concept with a strong political tradition in Europe and features heavily in the Charter of Fundamental Rights (Title III) in reference to equality before the law, non-discrimination, diversity, gender equality, the rights of children, the elderly and the disabled.

In the digital age, novel forms of algorithmic discrimination pose a risk to equality of opportunity and to the fundamental right to be protected against digital networks that offer a wealth of often free and accessible information.

Unlike traditional economic goods, which obey a law of scarcity, information is multipurpose. The use of digital information for one purpose does not deplete its availability for another. This opens up, on the one hand, a wide array of opportunities for creating and stabilising an economy of sharing based on equality and fairness in a digital society. Yet, on the other hand, the equality of opportunity that is facilitated by the consumption of informational goods by multiple consumers risks creating new inequalities resulting from the fact that some people may have the advantage by learning about content before others do and may extract value from it.

Democracy

Most of the core debates about the overall viability of the European Union, its institutions, the inclusion and in some cases the exclusion, of Member States, have revolved around the question of the democratic legitimacy of the European project.

In the digital age, both the deliberative model of democracy, grounded on citizenship and the notion of the common good are challenged as a basis for the European social contract. Algorithmically processed big data play an increasingly dominant role in informing and guiding individual and social action, in virtually all sectors of business and government. Data-driven governance is often presented as a 'revolutionary' mode of governance emancipated from the yokes of what is assumed to be biased human representation, ambiguous human language, or subjective points-of-view.

Personal or anonymous data are the new coordinates of social modelling. Big data rather than institutional or deliberative processes threaten to become the basis on which individuals are classified, evaluated, rewarded or punished. These same categories are used to evaluate the merits and needs of individuals or the opportunities or dangers underlying the lives they lead. In this view of 'data-driven governance', the question arises whether the individual human person as a legal subject has a future and how one can ensure that individuals are not viewed only as temporary data aggregates exploitable on an industrial scale rather than subjects in their own right.

Interactions based on algorithmic profiling may exacerbate information imbalances between decision-making governments and companies on the one hand and individuals on the other hand. As a result, 'data-rich' public and private organisations will have greater ethical responsibilities towards citizens and customers. Digital ethics must identify new perspectives, potential and boundaries for dealing with data ethically, by formulating the terms of a proactive approach to ethics, beyond mere legal avoidance measures. As such it will set out the terms of a social innovation that parallels the rapid technological innovation we are experiencing on a daily basis.

Justice

Like the concept of freedom, justice appears prominently as a core value in the European project. It features as a core principle of the Schengen area of freedom, security and justice. It also features in the Title IV provisions on justice and rule of law, the primary recourse to the guarantee of basic rights and freedoms proclaimed by European Union law, including the right to fair trial, presumption of innocence, legality and proportionality of punishment and against double-jeopardy.

The guarantee of justice in any institution is dependent upon a complex and interwoven systems of information management. Political rights are often deeply intertwined with the free flow of impartial information, transparency and accountability. Criminal justice depends critically on information collected and disseminated about the political context. Criminal investigations are linked to the processing of forensic data and questions of appropriateness and admissibility of data. In criminal justice systems, data-driven algorithmic solutions play a privileged role in the tendency towards performance-oriented management of justice systems. This tendency toward technical management of judicial systems impacts the ecosystem of justice in terms of the presumption of innocence, rules of evidence, processes of justification and the ability to contest judicial decisions, non-discrimination, and equal access to justice. The new horizon of predictive litigation may render law firms more selective in the cases and the individuals they are willing to represent, encouraging advocates to assess the value of sources of evidence by algorithm instead of by human judgment.

Trust

The development of human societies has also taken the form of institutionalising trust. As a concept, trust is related to the notions of risk and uncertainty. Trust has grown in importance in the evolution of information technologies as a bridge between technical and moral aspects of technically assisted communication systems. It does however appear prominently wherever the European Commission seeks to advance technological innovation against the apparent or proven resistance of public trust, such as in the Digital Agenda for Europe (2010), the Framework for Building Trust in the Digital Single Market (2011), the Cloud Computing Strategy (2012), the Cybersecurity Strategy (2013) or the much-heralded A Digital Single Market for Europe (2015).

Crucially, trust has a double-meaning in data protection. One is a technologically-oriented, functional or knowledge concept: trust in a technology refers to the confidence that it will not fail in its pure functionality, that its design and engineered properties will carry out their expected function. The second, trust is a moral concept referring to belief and reliance in a person or organisation that they will honour explicit or implicit promises and commitments.

Human society has arguably taken the course it has, because cultural, social, institutional and technical solutions have been found to create arrangements that can establish and reinforce trust: promises, contracts, witnesses, institutions, ethical norms, laws and associated compliance arrangements. Where trust is absent, social cooperation is weakened and costly informational transactions, governance structures and enforcement mechanisms need to be deployed, decreasing efficiency and increasing costs. Low-trust societies struggle to exit this suboptimal equilibrium.

Data protection faces three interrelated crises of trust:

i) individual trust: trust in people, institutions and organisations that deal with personal data is low;
ii) institutional trust: transparency and accountability as a condition for keeping track of the reputations of individuals and organisations and

trust-building in a society requires access to personal data; and

iii) social trust: trust in other members of social groups used to be anchored in personal proximity and physical interaction, which are being increasingly replaced by digital connections.

A range of technological fixes to this triple-crisis have appeared on the horizon, though the outcome of their implementation seems unclear: distributed ledger technologies (e.g. blockchain) and peer-to-peer technologies and possibly quantum cryptography could help to solve some of the problems with eroding trust in digital societies. However, blockchains and their functional equivalents give rise to a number of other problems that need to be identified and addressed in due course. In ethical terms, this costly crisis of trust can be addressed by revisiting the terms and qualities of digital communities.

Trust builds on shared assumptions about material and immaterial values, about what is important and what is expendable. It stems from shared social practice, shared habits, ways of life, common norms, convictions and attitudes. Trust is based on shared experiences, on a shared past, shared traditions and shared memories.

What are the necessary conditions for implementing foundational values?

In light of these values, what are the necessary conditions for people today and in future to be respected in their dignity, to develop their autonomy, to be able to count on solidarity, feel equal notwithstanding their individual differences and experience trust?

Protecting fundamental values is not the same as privileging an individualistic concept of fundamental rights. A digital ethics must be precise and rigorous in its regard for the relation between ethics and innovation.

Among the issues raised by digital ethics, the EAG has focused on the following conditions that it considers necessary for an ethically sustainable development of digital technologies in relation to the fundamental values of dignity, freedom, autonomy, solidarity, equality, democracy, justice and trust:

- material conditions e.g. fair distribution of infrastructure, supplies, affordances, environment, social welfare, health and economics;
- cultural conditions e.g. access to education, tradition, art, language, world views;
- personal conditions e.g. the freedom to develop and express one's identity without interference, the possibility to revise one's own preferences and choices, the possibility to control the image of oneself and one projects;
- political and social-structural conditions e.g. equal opportunities and non-discrimination, social rights, participation, transparency, accountability;
- legal conditions e.g. due process, effective prohibition, prevention and

prosecution of violations of dignity, freedom and fundamental rights .

5. Digital ethics of the innovation ecosystem

Innovation as ethics

The concept of responsible innovation which has developed over the last few years, can be fruitfully applied, with modifications deal with the new innovation challenges linked to digitisation. One of the most encouraging insights recently garnered from industrial practices is that innovation often finds ways to overcome ethical deadlocks and apparently insurmountable value-dilemmas, such as increasing transparency while observing confidentiality, strengthening accountability without breaches of security, or explaining the application of algorithms without reducing the functionality of IT systems.

Although there is no guarantee that such innovations are always possible, it is worthwhile exploring whether and under what conditions they can be. Innovation can and should be geared towards improving society and people's lives through the design of ethically robust socio-technical systems. In this sense, ethical questions emerging from discussions of digital technologies should become opportunities for ethical and technological evolution. In order to nourish critical debates, concrete forms of collaboration between engineers, applied scientists and ethicists and multiple stakeholders, resulting in responsible innovations, should be provided, allowing the co-shaping of ethical considerations and design solutions.

Designing for values

Digital ethics will need to accompany rapidly moving technological evolution and become part of the research and development processes as well as cycles of innovation and obsolescence or risk becoming irrelevant. The high speed of technological innovation challenges the traditional, low-velocity, sense-making of human beings.

Digital ethics that comes after the fact has wasted an opportunity to inform and shape the world. A design perspective in digital ethics would help to overcome this problem, because it would insert moral considerations at the point in which they can make a significant difference with lower costs and risks: at the initial stages of the design and development.

Value-sensitive design should highlight ethical values at play, allowing debates about their content, interpretation and application. These debates can be facilitated by studying the practical consequences of the way values of stakeholders and different parties have shaped engineering design for better or for worse.

A responsive digital ethics will need to provide solutions to unprecedented challenges. Therefore, digital ethics will foster well-informed debates to address rapidly changing conditions.

While the innovation of technical artefacts alone does not necessarily generate value-added for societies, minute changes may have global effects that are potentially irreversible yet not easily identifiable in advance. In short, it is at times impossible to know the impact of a new functionality in advance or whether the introduction of a technology is irreversible because of multiple path dependencies.

Approaches to the free circulation of data

Digital technologies recasts questions of autonomy and democracy, changing the nature of competition, introducing data flows into both individual everyday existence where they once might not have been meaningful; they facilitate transnational flows of information that challenge poorly harmonised national legal cultures of data protection, putting new pressures on the law and on the ethics of monopolies.

Analysis is needed of the new digital geopolitics created by differences in data protection rules applied across national borders that no longer represent the limits of data flows. The consequences for global governance can hardly be underestimated. The new digital geopolitics will impact national cultures to the extent that national sovereignty, increasingly squeezed between national pressures and the shifting norms of the international system, will need to be repurposed, with all the implications for democratic legitimacy that this implies.

Digital ethics will need to re-examine the foundation and application of private property law and property rights in the context of new digital commons and the new challenges to intellectual property rights. Current regimes of intellectual property rights do not exhaustively cover the opportunities and challenges created by rapid increases in data-sharing, in terms of both the sheer quantity of data being aggregated, re-combined, shared etc., and of the increasing number of types of data, protected by a variety of legal mechanisms and controlled by multiple technological systems involving multiple constraints. Digital innovation, while generating legal and ethical challenges also creates secondary vulnerabilities, both technological and human.

The networked society is currently characterised by significant inequalities. Access to, and participation in, digital innovation is concentrated among a few digital giants. Barriers to entry into technology markets remain high, despite ambitions for lowering them. Questions about the democratic participation in markets may be raised if ambitions for lowering thresholds are not working, raising the stakes for the success of potential guidelines on data portability. Ethical approaches should be applied to determine how best to optimise financial cooperation.

There appears to be a fundamental conflict between the principle of data minimisation and the value of producing, storing and/or circulating data. An ethical consideration of the value of information, its determination and convertibility to other forms of data is needed. Clearly, the value of data fluctuates immensely as a function of its use. Can this change be calibrated with velocity of variation of ethical or economic value? The prospects of inter-governmental regulation, in many ways unlikely given the clashing architectures of digital networks and state-based regulatory authorities, particularly in the coordination of standards, will nonetheless need new discussion within the scope of digital ethics and sub-national, sectoral standards.

Data markets

Data markets are not new phenomena but they have achieved a new relevance in the digital age. In traditional direct marketing, the use of lists of prospective customers goes back to at least the early days of catalogue-selling, when improved information, together with innovative transportation solutions, were the recipe for growth supported by marginal gains. Today, marginal gains may be very small yet massive in scale.

Whereas in the past, data might have been used to better understand customer needs in order to better target product offerings, today the scale of data-driven marketing has grown exponentially. Competition also takes the form of refining customer profiles in order to better target them. An ethics for the digital market will need to understand and respond to the relation between small, marginal digital value and the human value that is the traditional basis for political economy.

Commercial enterprises that flourish in the scaled optimisation of value must also be attentive to the consequences of prioritising the creation of digital value compared to traditional analogue understandings of quality linked to more durable products.

Data commodification and digital property rights

Commodification refers to the process whereby something—for example a service or an artefact—which was not an object of trade with an economic value, becomes one. Data have been commodified in this sense, for example by attributing economic value to customer profiles by the advertising sector. But they have also been subject to 'commoditisation'. This is the process whereby something that is already an object of trade, with an economic value, becomes an undifferentiated good in the perception of customers. Fridges have been commoditised in this sense and so has journalistic information. Both data commodification and data commoditisation present ethical challenges. This is why the GDPR affirms 'the processing of personal data should be designed to serve mankind'.

It is often noted by advocates of data property that there is already a de facto freely operational market for personal data, which is at present not recognised as such. And yet a core value principle at the heart of the reflection behind this report is that the value of personal data stems not from its intrinsic character, its association with the individual and not from its potential to be aggregated with other data. The assumption of personal data as personal property, that the individual has the right to do whatever it wishes with its personal data, including selling them, has social-structural consequences, for example by forcing others to put their data on the market at the risk of suffering competitive disadvantages.

In short, the individualistic solution of property over personal data is not a good solution in the current environment, one in which data are not mere commodities but rather the new coordinates of digital society. 'My' in 'my data' is not the same as in 'my car' but rather the same as in 'my hands'. Personal data may constitute personal identities and should be protected accordingly, not merely commercialised and also be subject to a market mechanism.

6. Digital ethics at work

The following short analyses illustrate some of the challenges and issues that the EAG considers relevant for digital ethics and for our digital future.

Health care and research

Health care research and clinical care is today on the cusp of a new generation of digital innovation. This innovation will have far-reaching ethical consequences, in particular for the governance of personal data generated in and through health care research and medical practices. In traditional forms of data governance, biological data is collected, stored, accessed and analysed according to analogue means of identification, with biological data linked through prior authorisation, record-keeping and control linked to actual living subjects, who are endowed with certain rights to privacy and data protection.

In new digital contexts, research and treatment built around methods of big data collection and analysis increasingly detach the biological digital subjects from their biological data. The emphasis is moved away from the identifiable individual, endowed with individual rights and protections guaranteed under national and European law, towards the mass collection and analysis of biological data through the use of databases and data-mining practices. This is where a clash in data governance may emerge. The particularity of genetic science lies in the fact that genetic material, in its extraordinary specificity and reproducibility of its properties, gives a high level of granularity and thus specificity and identifiability of individuals.

However, the re-use and re-combination of multiple genetic data sets make the triangulation of multiple data points possible allowing access and active use of information initially covered by norms of privacy. Genetic data gathering is just one of many examples requiring a move away from a traditional governance model relying on prior authorisations to a monitoring governance model, relying on a co-stewardship between individuals and researchers/doctors. Indeed, minimal risk criteria and risk certification (authorisation) may be as required as the inclusion of some people in monitoring the governance model may become necessary.

The inclusion of actual individuals becomes more critical whenever anonymity may be challenged and as the informed consent of individuals becomes an inadequate safeguard. The practice of getting informed consent in clinical practice and research may potentially be supported by some form of tacit or broad agreement to participating in the digital health care ecosystem.

In some contexts, we are seeing a more basic transition from the material, connected, biological markers of identity and personhood, to personhood as digital matter. In a digital context, the tension between the ethics of care and the ethics of information monitoring becomes more acute.

The same process impacts the boundary between genetic data collected and adapted for therapy and those collected for research purposes.

Humanitarian work

Humanitarian agencies work in the space where fundamental values are in play as questions of life and death, indeed where humanity itself is in play. Humanitarian work today increasingly engages with data protection principles, in particular in questions involving the protection of third parties. Certain international organisations, for example, work to confirm the whereabouts of prisoners of war while contacting family or friends can put them at risk. Here the right to information clashes with the security of the person whose data is in question. For this reason, the risk management approaches to data processing are used, taking decisions on a pragmatic basis instead of in the name of the data protection principles. As technologies of identification improve through, for example, facial recognition, the challenge of protecting the identity of digital subjects from some, while sharing it with others, becomes exacerbated.

On a global level, humanitarian actors, like actors in other sectors, have become highly dependent on reliable data, though the risks involved in dealing with unreliable data are higher in this field than elsewhere. These dangers go beyond simple violation of the data protection rights of certain individuals. More often, it is a question of life and death. A type of dual use risk arises in many cases: data collected for the protection of victims can be used to further harm them. For example, organisations that use GIS-based maps in order to plan for refugee evacuation risk making open data available for use by belligerent actors for aggressive purposes.

Humanitarian activities have also led to new innovation in big data, the creation of 'digital humanitarian volunteers', the engagement of credit card and mobile phone companies. Yet this innovation also has its dark side. In Senegal, for example, mobile phone services provided data for a development project in order to be able to track mobile traffic as a measure of sustainable development. Yet this identification led to more exposure of vulnerable populations. For this reason, humanitarian organisations tend to be careful with sharing data, particularly with operators that would like to merge them in large multi-use data bases.

As a consequence, digital ethics in the humanitarian sector needs to be considered on a case-by-case basis. High standards are generally kept in order to protect the identity and the dignity of the vulnerable, at the frontiers of dignity, even in death. Because the humanitarian field involves vulnerable populations and because the humanitarian response often involves a management of populations, the margin of manoeuvre for people to make individual choices and take decisions is often limited.

Finance

The use of personal data in the financial sector is heavily regulated. Constraints and challenges range from legal compliance in globalised operations, to ethical alignment to avoid competitive erosion. Regulations have typically been based on observed data, actuarial exercises to organise solidarity, and financial support to assure sustainable business development. The use of data is moving from statistic-based observations towards machine learning, AI and predictive data uses. From the point of view of actors within the financial sector this reinforces challenges related to data quality and accuracy, where the frequency of updating training data as well as their biases need to be taken into consideration: the results should be open to evaluation, introducing ex-post testing. Ideally, this should build on globally recognised technical standards.

Prediction capabilities also give rise to the paradox where actors shape the future by advancing knowledge while at the same time rendering future events less likely because of that knowledge. Empowerment through transparency with the aim of promoting responsible use of money, better investments or 'preferred' behaviours have the secondary effect of allowing individuals to take responsibility for their choices, thus enabling a more ethically balanced equilibrium of resources.

Understanding and appropriately applying regulations will require a continuous dialogue between data science and legal teams. Ethically sound practices will require continuous learning from data scientists and the monitoring of deviation controls as we move from static to dynamic models of investment in which bias is no longer a given, but rather an object of ethical reflection and scrutiny. In the future, ethical frameworks and algorithmic oversight will be required to assure redressing of outcomes. The transition should be managed to support fairness but also competitiveness.

Democratic governance

Computing power fueled by masses of data and activated through micro-targeting capabilities has made nudging of electoral outcomes a fact. While such practices highlight their own set of challenges related to the demands of consumers as beneficiaries of a specific version of the social contract, outcomes related to political demands should not be considered a purely legal or compliance exercise.

Issues related to lack of transparency, loss of traceability and accountability have emerged through recent election cycles, as well as an awareness of considerable global misalignment related to classification of data types such as political affiliations or trade union memberships, to name just a few.

Misalignment in legal obligations related to clashes of belonging, loyalty and rights are also increasingly circumvented through extra-territorial shifts of data to assure immunity. While geographical targeting is not something new, micro-targeting of electoral canvassing changes the rules of public speech, reducing the space for debate and interchange of ideas. Consensus around political debates needs to be driven by group belonging, solidarity, empathy and not only fictional or virtual persons generated by processing big data needs alone.

Bias is often embedded into the learning data used to influence elections as well as upcoming policy making. The potential servitude to a 'wisdom of the crowds' type of societal decision making, contrary to European values, urgently requires a democratic debate on the use and exploitation of data for political campaign and decision-making.

Smart cities

Smart cities will be the greenfield of the Internet of Things (IoT), combined with regular internet, and massive reconfigurable sensor networks. In the course of the 21st Century, close to 75% of the world population will live in large urban areas, which will have the characteristics of ubiquitous computing environments where smart technology will dominate all sectors, transport and mobility, waste treatment, health, built environment, telecom, food chains, energy, administration, management. It is not unreasonable to claim that these large urban conglomerates, with often tens of millions of inhabitants, and featuring still unimagined challenges in terms of sustainability, safety, security, energy, health and quality of life, will only be viable through a well-ordered processing of the personal data generated through the interaction of citizens and their environments.

Large modern cities increasingly take the shape of complex organisms consisting of interrelated systems and subsystems, dependent and independent components. By the same token, as these components become normalised as modules in digitally related systems, a new range of opportunities and risks emerges. The mapping and interconnection of individuals and activities, makes understanding links and nodes of networked life immediately tactile. More than in other digital environments, however, cities cannot be simply controlled from a central node. They are decentralised. It is less a question of what the individual nodes in a smart cities are doing than of the way they interrelate with each other.

The logic and design of smart cities puts into question the traditional principles of ethics in general, and of privacy and data protection in particular. As a consequence there is considerable space for re-thinking the scope and object of digital ethics. The smart city is the meeting-place of social and cultural norms, on the one hand, and the technological horizon of connectivity, on the other. This may become a model of a techno-ethical ecosystem, in which trust between individuals and their data is respectful and oriented toward the collective good. Personal data is circulated with respect to individual rights. In essence, the smart city may be a living democracy, a democracy in real time.

A range of ethical issues emerges in these environments. The design of urban infrastructures will need to be informed by shared values distributed and applied in ways that have not yet been imagined or put into place. In order to form sustainable human community, such shared values will need to be internalised and institutionalised, and made instrumental to the shaping of the 'smart environments', which will be their technological platforms. Therefore ethical and democratic governance and design will be of utmost importance.

Predictive policing

Policing is evolving under the pressure of new forms of criminality, which has become multifaceted, decentralised and technology-savvy. Until recently, policing methods were mostly directed toward reaction to crimes (investigation-led policing), where police operations are triggered by reasonable suspicions, i.e. the existence of facts or information, which would satisfy an objective observer that the person concerned may have committed the offence or of specific, observable actions of unknown suspects. In the future, methods will move further towards a precautionary logic under which police operations are triggered by forecasts and predictions. Police may make use of early intervention techniques in order to act upon the risk, even before it has expressed itself or become acknowledged.

It is reasonable to assume an increasing use of risk management techniques and a focus on threat anticipation and prevention to optimise the allocation of police resources and the fight against crime. The target becomes not just the crime but also the 'future and potential' crime. Big data analytics are used to leverage existing crime forecasting techniques. They offer law enforcement the possibility to forecast places and times with an increased risk of crime ('heat maps'), to identify high risk individuals, individuals at risk of offending in the future, to identify groups or, in some cases, individuals who are likely to become victims of a crime ('heat lists').

This new form of policing, also called 'predictive policing', comes with a new set of challenges. The first impacts the predictability of law enforcement decision-making process, which becomes more opaque and prone to decisions, the legitimacy of which may be difficult to challenge. This stems from the risks of implicit or confirmative bias in the datasets. Police may risk becoming more interested in the patterns than in the substance, more concerned with the prediction than in observable facts.

7. New directions: Thinking ethically in the digital age

This report is issued at a time when the data protection community is preparing for the application of the long-awaited GDPR. It cannot and does not seek to override the GDPR, to regulate present data protection practices by proposing additional rules. This is adequately and appropriately accomplished by the new regulation. This report proposes concepts and arguments to support and advance data protection as a project of European values. It describes the way traditional concepts of value may be rethought, re-articulated and re-purposed in order to assure the continuity of legitimate practices and anticipate an unseen future. This task can, by way of conclusion, be condensed into five significant 'directions' of thought and innovation.

1. **The dignity of the person remains inviolable in the digital age**
   Life in the digital age is close to a confrontation with the basic principle of personhood: dignity. Digital experience reshapes our understanding of personal identity, human experience and social interactions. Digital life will need to be compatible with the inviolable nature of human dignity.

2. **Personhood and personal data are inseparable from one another**
   Personhood—understanding oneself as a person endowed with moral qualities, rights and responsibilities—is inseparable from the information produced by, and pertaining to that person.

3. **Digital technologies risk weakening the foundation of democratic governance**
   The freedom of choice of each person is a fundamental principle of democratic self-governance. Automated, big data-based interaction with political decision-making may be incompatible with democratic processes.

4. **Digitised data processing risks fostering new forms of discrimination**
   Profiling is part of everyday cognition and judgment. Digitally generated profiles based on very large quantities of data are powerful and increasingly unaccountable.

5. **Data commoditisation risks shifting value from persons to personal data**
   The market value of personal data is not intrinsic but stems from its relationship to the person or persons who give rise to it. Ethical tensions can arise where human value and market value intersect.

Contents

PSD00871 I Conception & Design: IDEA Unit I DGITEC, EDIT Directorate

Report by the Ethics Advisory Group established by
the European Data Protection Supervisor, the EU’s independent data protection authority

www.edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor