1 INTRODUCTION: EXPLORING THE BOUNDARIES OF BIG DATA

Bart van der Sloot, Dennis Broeders & Erik Schrijvers

This book deals with issues involved in Big Data from a technological, economic, empirical, legal, and regulatory perspective. Big Data is a buzzword used frequently in both the private and the public sector, the press, and online media. Large amounts of money are being invested to make companies Big Data-proof, and governmental institutions are eager to experiment with Big Data applications in the fields of crime prevention, intelligence, and fraud, to name but a few areas. Still, an exact and uniform definition of Big Data is hard to come by. Most definitions roughly regard three states of processing: data collection, as Big Data concerns collecting large amounts of data, from varied and often unstructured sources; data analyses, as Big Data revolves around the speed of the analyses and the use of certain instruments such as algorithms, machine learning, and statistic correlations; and use of data, as the results are often predictive in nature and are formulated at a general or group level.

Though the exact nature and delineation of Big Data is still unclear, it seems likely that Big Data will have an enormous impact on our daily lives. Many businesses are applying Big Data analytics to find patterns and statistical correlations in order to optimize their services, to target their customers, and to personalize their content. Governments are applying new data technologies to predict and prevent crime, to develop profiles of potential terrorists, and to make better informed policy choices in the social and economic domains, the legal and the healthcare sectors, and the fields of mobility and infrastructure. What everyone appears to agree on is that Big Data may have a huge positive effect on the world we live in, by promoting efficiency, justice, customer service, and security, but that it might also result in discrimination, privacy violations, and chilling effects. The hope is that an adequate framework will ensure that the beneficial uses of Big Data are promoted and facilitated, while the negative effects are prevented or sanctioned. This book provides building blocks for developing such a framework.

1.1 BACKGROUND OF THIS BOOK

On behalf of the Dutch government, the Minister for Security and Justice has asked the Netherlands Scientific Council for Government Policy (WRR) to write a report on the use of Big Data, especially in relation to national security, including its effect on the right to privacy. The Netherlands Scientific Council for Government Policy is an independent advisory body with the role of informing and advising the government and parliament on issues of significant importance for

society. The opinions of the WRR are cross-sectoral, cross-departmental, and multi-disciplinary. They concern the course of government policy in the longer term.

In his request, the Minister formulated four main questions. The first main question was whether a stronger distinction should be made between access to and use of information in Big Data processes, a question that was partly inspired by the transnational nature of many data processing activities. In particular, the Minister asked whether the mere collection and storage of personal data, without the data being analysed or used, should be limited by data protection legislation, pointing to the fact that it cannot be ruled out in Big Data processes that non-identifying data may become personal data at a later stage. In connection with this, the question was how big the role of the state should be, in the Big Data era, in ensuring that the use of Big Data for the promotion of security meets the standards of purpose limitation and data minimization, amongst other things. The Minister also wanted to know whether these principles can be maintained, and if so how.

The second key question concerned the use of Big Data processes and of techniques such as profiling and data mining. In particular, the Minister wished to be informed about how these techniques can be used in a transparent manner and how adequate checks and balances can be formulated to allow these techniques to be used safely and proportionately.

Thirdly, the Minister referred to the emergence of quantum computing and asked whether encryption and anonymity can still be guaranteed in the future.
Finally, the Minister wanted to know how the autonomy of citizens can be ensured in Big Data processes. This relates to the question of whether a focus on informed consent is still tenable, what possibilities citizens have for effective control over their data, what responsibility citizens have to contribute to the quality of data in databases, and more in general, how maintaining quality of information can be guaranteed.

Because Big Data processes are relatively new and could be studied from many different perspectives and scientific disciplines, the WRR decided, in preparation of its advice to the government, to invite several scholars to write a contribution to this book. These studies and insights gained from them were used by the WRR as background materials in writing its advice to the government. Because the book serves as preparatory work for the WRR's advice to the government, the intention of this study is to present a wide range of different perspectives on, approaches to, and applications of Big Data.

Rather than going to the core of Big Data, it explores the boundaries of Big Data. What should be called Big Data in a technical sense, and how should it be distinguished from other techniques and applications? How are Big Data processes used in practice, by whom, and to what purposes? What positive and negative effects may follow from Big Data analytics? What legal principles apply to Big Data techniques, and on which points does the current regulatory framework need an overhaul? These are but a few of the questions this book undertakes to answer. The fact that the book explores the boundaries of Big Data is also necessitated by the fact that it is still largely unclear what Big Data precisely is. It is a notion that is still in transition, and its nature and potential implications are still evolving. Consequently, it is still too early to define Big Data with great precision but an opportune moment to outline what new questions and challenges follow from this phenomenon.

1.2 CONTENTS OF THIS BOOK

This book is divided into five parts, each part engaging with a different perspective on Big Data: the technical, empirical, legal, regulatory, and international perspective. It is important to stress that the chapters contained in this volume were mostly written in early 2015, when the exact content of the General Data Protection Regulation was still under discussion, and the Schrems case had not been delivered by the European Court of Justice. The General Data Protection Regulation will replace the current European data protection framework, the Data Protection Directive from 1995. Leaving the core principles mostly intact, the Regulation invests heavily in the compliance and enforcement of those rules, with broader powers for DPAs, wider obligations for data controllers, and higher penalties violators. The (non-)enforcement of the data protection principles is currently considered the biggest problem of data protection instruments. Moreover, a Regulation, as opposed to a Directive, has direct effect at EU level, smoothing out the differences that currently exist between different EU-countries in their interpretation and application of the data protection principles in their respective countries.

The Schrems case was about the protection of personal data of European citizens. The Data Protection Directive holds that personal data may only be transferred to a third country if that country ensures an adequate level of protection. The European Commission had issued a decision, in which it held that the United States had an adequate level of protection. In the Schrems case, however, the European Court of Justice invalidated this decision. Although there are now transatlantic negotiations going on to design an ameliorated agreement that provides more protection to European citizens, it is still unsure at the moment of finalizing this introduction what rules this agreement will contain and whether they will hold

before the European Court of Justice. Some of the contributions anticipate these two developments, while others have tried to take a step back and signal general trends and focus on the underlying principles of the regulatory framework.

Part I of this book centres on the technological perspective on Big Data and contains chapter 2, entitled 'Sustainable Harvesting of the Big Data Potential', by Sander Klous and chapter 3, named 'Cryptology and Privacy in the Context of Big Data', by Seda Gürses and Bart Preneel. Part II engages with empirical perspectives on Big Data. It contains Gemma Galdon Clavell's chapter entitled 'Policing, Big Data and the Commodification of Security' and Rosamunde van Brakel's chapter 'Pre-emptive Big Data Surveillance and its (Dis)Empowering Consequences: the Case of Predictive Policing'. Part III investigates specific legal doctrines, as opposed to the general regulatory framework (whether legal or not) analysed in part IV. Chapter 6, entitled 'Predictive Profiling and its Legal Limits: Effectiveness Gone Forever?', is written by Paul De Hert and Hans Lammerant and is the only chapter in this section. Part IV contains regulatory perspectives on Big Data, asking how this new phenomenon should be regulated in the future. It contains two chapters, namely chapter 7 entitled 'The Individual in the Big Data Era: Moving towards an Agent-Based Privacy Paradigm' by Bart van der Sloot and 'Privacy Protection in the Era of 'Big Data': Regulatory Challenges and Social Assessments', chapter 8, written by Colin Bennet and Robin Bayley. Finally, for Part V, the WRR invited two contributions providing the reader with international and comparative research on Big Data. Because Big Data processes are almost by definition transnational, the lessons learned in other jurisdictions may have an important value for the European and Dutch regulator. The contributors to this section are Joris van Hoboken, 'From Collection to Use in Privacy Regulation? A Forward-Looking Comparison of European and US Frameworks for Personal Data Processing', and Alexander Roßnagel and Philipp Richter, 'Big Data and Informational Self-Determination. Regulative Approaches in Germany: the Case of Police and Intelligence Agencies'.

From the chapter by Sander Klous, we may conclude that Big Data is hard to define. Klous first provides the standard definition of Big Data, using the three Vs of Volume, Variety, and Velocity, with Volume referring to the vast amounts of data that are being generated, Variety referring to the different types of data and data sources, and Velocity referring to both the increasing rate of data collection and the increasing demand to get real-time insights and responses. Klous adds one more technical 'V', namely Veracity. Veracity refers to the correctness and accuracy of information. Most importantly, however, Klous argues, these four Vs only symbolize the technical side of Big Data, while one of the most distinguishing features of Big Data compared to other data-related subjects is that it is a topic primarily driven by business, not by technology. Hence, he argues that the most interesting V is a fifth one, namely Value. Moreover, there are several subtleties that need to be

addressed to get a better understanding of what Big Data is supposed to mean. First of all, the word 'big' in Big Data can be slightly misleading because these processes are often simply about the smart combination of limited amounts of data for personalization. Second, there are several developments closely related to Big Data, such as cloud computing and the Internet of Things, that act as enablers.

Sometimes these developments are confused with Big Data: cloud computing, for example, aims at transforming the IT architecture, whereas Big Data aims at transforming the decision-making process. Third and finally, Big Data plays an essential role in recent developments that may not immediately spring to mind when considering Big Data, such as the renewed interest in 'technological singularity', i.e. the moment in time when intelligent systems will exceed human intellectual capacity, or the block chain, the mechanism behind bitcoins, allowing trusted transactions without a third party.

Seda Gürses and Bart Preneel signal a number of challenges that Big Data poses to cryptology and privacy. First, services are organized to do computations on the server side, meaning that all data generated in using the services flows to the service providers. This could lead to an erosion of confidentiality. Furthermore, providers often require user authentication as a prerequisite to service use, and user tracking is central to their business models. In addition, the number of entities with access to user data is increasing while transparency is decreasing, and service providers increasingly limit users' ability to view or control what services are actually doing on their devices or their servers. Because data analytics is still a nascent field, finally, its application to daily matters in order to optimize organizational interests amplifies concerns about discrimination, unfair treatment, social sorting, and human experimentation. In relation to these challenges, they suggest that cryptographic techniques can be helpful in protecting data from unintended use and unauthorized access, that they can help to increase the accountability of cloud services and data analytics algorithms, and that applying privacy enhancing technologies is minimum but not sufficient requirement for protecting privacy.

Gemma Galdon Clavell signals several fundamental trends, the most important one being the hybridization of domains by blurring the lines between defence policy, crime prevention, and intelligence, especially in urban environments. Equally important is the move towards prevention, in which the idea of anticipatory action is embraced. While focusing on maintaining order, looking after the physical environment, and caring about some people's 'quality of life' spells care and proximity and can be seen as an attempt to build more democratic and representative police forces, this same rhetoric is underpinning harsh 'zero-tolerance' and 'three-strikes' sentencing approaches. Then there is informationalization: the trend to focus more and more on gathering and processing data. Similarly,

reference can be made to the increased interconnectivity between offline and online sources, ensuring that sources can be combined to enhance investigation results. For instance, fingerprints obtained at a crime scene may lead to an official name and date of birth; this name can be linked to numerous additional records, such as credit card utilization, telecommunications, travelling routines, or online social network activities. As a final example of an important trend currently taking place, reference can be made to privatization. According to Galdon Clavell, the global recession intensified pressures on budgets, increasing the need for security agencies to 'do more with less'. The shift to private-supported security often comes with the development of new consumption trends and social phenomena: new residential and shopping areas, or entertainment complexes, for example, which provide the illusion of being public spaces while being subject to private regulations and private security.

Rosamunde van Brakel has studied the use of Big Data in relation to predictive policing. She signals both potentially disempowering and empowering effects that the use of Big Data may have on citizens. With regard to the disempowering effects, she suggests that it is possible that in the future, it will no longer be a human who makes the assessments and decisions, but a computer, or rather the technology, which has serious consequences for questions of accountability.

Moreover, these types of algorithms and computer programs are often not transparent, which may have a disempowering effect on the position of citizens. The use of algorithms may also lead to algorithmic discrimination if the algorithms or the data on which they are based are biased. Furthermore, there is also the danger of both false positives and false negatives, which may lead to stigmatization and may have serious consequences for citizens' well-being and life chances.

The cumulative surveillance effect signals that predictive policing and Big Data may have a cumulative disadvantage effect, and groups such as Amish, Roma, and Luddites may be socially excluded. Van Brakel concludes by suggesting that Big Data may also have an empowering effect on citizens, but that Big Data is rarely applied in such a way at present. Still, Big Data could potentially be used to give more and more detailed information to citizens, about crime rates, for example, so they are in a better position to protect themselves against crime, or to use profiling to provide more protection to the weak.

Paul De Hert and Hans Lammerant investigate the use of profiling in relation to Big Data. They have analysed the standard literature on Knowledge Discovery in Databases, pattern discovery, group profiling, and predictive profiling. They argue that three groups of people may be affected by the use of profiling: the people whose data are used to create the profile, the people to whom the profiles refer, and the people who are subjected to decision-making based on the profile.

They also see three risks following from the use of profiling. Firstly, there is a heightened risk of more intrusive privacy interferences due to heightened surveillance. Secondly, there is the risk associated with social sorting – or sorting people into categories assigning worth or risk – and stereotyping. Thirdly, there are the risks related to opaque decision-making, which plays at two distinct levels: the application of a profile and the decision based on its results. They suggest that there are three general guarantees against the dangers of profiling that can be distilled from the current legal framework. A first safeguard can be found in the legality principle, which substantiates the idea of the rule of law and the need to limit state powers by linking them to competences and purposes. A second safeguard is the proportionality principle, which provides that decisions may not negatively affect people disproportionally in relation to the purpose of the decision and that supervisory and investigative competences may only be used if needed. A third category of safeguards concerns procedural safeguards given to the individual involved in state procedures, obliging the administration to establish and review all the relevant factual and legal elements of a case with due care. The authors conclude, however, that, although these are valuable safeguards, the legal regime needs an overhaul to adequately protect citizens' interests in the age of Big Data.

Bart van der Sloot suggests that privacy and data protection regulation did originally not focus on individual rights and individual interests, or only to a limited extent. The current regime, however, almost exclusively focuses on individuals, their rights, and their interests. He argues that this focus is untenable in the age of Big Data because Big Data processes do not specifically concern individuals but rather large groups of unidentified subjects. The individual interest in these types of processes is often difficult to demonstrate, and they rather they affect group or societal interests.

Likewise, it is increasingly difficult for individuals to invoke their subjective rights because they are often unaware of their personal data being gathered: data processing is so widespread in the Big Data era that it will be undoable for an individual to keep track of every data processing activity that includes (or might include) his or her data, to assess whether the data controller abides by the legal standards applicable, and if not, to file a legal complaint. And if an individual does go to court to defend his or her rights, he or she has to demonstrate a personal interest, i.e., personal harm, which is a particularly problematic notion in Big Data processes: what concrete harm, for example, has the NSA data gathering done to an ordinary American or European citizen? This also shows the fundamental tension between the traditional legal and philosophical discourse and the new technological reality; whereas the traditional discourse focuses on individual rights and individual interests, data processing often affects a structural and societal interest and, in many ways, transcends the individual. This is why Van der Sloot suggests

complementing the current regulatory framework, focusing on legal principles, black letter law, and individual rights, with a model that focuses on the agent of the privacy violations, either a state, a company, or an individual.

The core of the framework's attention, then, should not be on the potential harm a particular act may do to a specific individual, but the on the question whether power is used in a good and adequate manner. That means that there must be not only safeguards against abuse of power, but also positive obligations to use power for the good of all.

Colin Bennett and Robin Bayley also signal that many of the current Big Data practices affect not only individuals, but also a set of more general interests. They discuss three types of assessments that may help to ameliorate the current privacy paradigm. First, there are the Privacy Impact Assessments (PIAs) that are proposed in the upcoming General Data Protection Regulation. PIAs can be used to assess the impact a certain project or technique might have on the privacy of individuals before such a programme or technique is applied in practice. Furthermore, the concept of 'Surveillance Impact Assessments' (SIAs) has been introduced to respond to the critique that PIAs are too narrowly focused on individual privacy. A fairly broad definition of surveillance is adopted to include the systematic capture of personal data beyond that collected through visual means. Four nested concentric circles have been proposed to make up an SIA: in the innermost circle is the conventional PIA, focusing on individual privacy. The second layer adds other impacts on an individual's relationships, positions, and freedoms, with the third layer adding the impact on groups and categories. The fourth and outermost ring of the circle adds the broader impacts on society and the political system. The model is intended to be cumulative. Finally, Bennett and Bayley analyse Ethical Impact Assessments (EIAs). Unlike PIAs and SIAs, these assessments are explicitly motivated by the question how Big Data processes should be analysed ethically. Four integrated steps have been conceived: a Unified Ethical Frame, an Interrogation Framework, an Enforcement Discussion, and Industry Interrogation Models, with only drafts of the first two steps being currently available for comment. The idea is that the implementation of such EIAs will begin with an analysis of the larger ethical considerations and progressively drill down to more practical guidance for industry.

Joris van Hoboken has compared EU and US regulation, paying specific attention to the question whether the current focus on regulating the collection of personal data is still tenable in the Big Data era or whether it should be replaced by a focus on the use of data. He signals that the classic self-determination rationale for information privacy regulation entails that the collection of personal data enables the exercise of power and may have chilling effects on individual freedom and

behaviour, effects that should be assessed not only in terms of their impact on specific individuals, but also in view of the values of pluralism and democratic self-governance.

According to Van Hoboken, this rationale is widely accepted in European data privacy jurisprudence and affirmed in fundamental rights case law. The data protection principles as engrained in the Data Protection Directive are connected to this rationale and place many restrictions on the gathering of personal data, the most important one being the data minimization principle, which entails that data may only be gathered, stored, and used for data processing activities if this is necessary for achieving the goal of the data processing activity. In the US, the focus lies on the notion of notice and choice, which limits the gathering and use of data to the goal originally communicated to the individuals consenting to the collection of their data. American law also provides a number of rules regarding the use of data, which Europe mostly lacks. These differences notwithstanding, the article concludes that there are significant hurdles to overcome to refocus data privacy law towards use-based regulation on both sides of the Atlantic. In Europe, the existing fundamental rights framework is one of these hurdles as well as the omnibus approach to data privacy regulation.

In the US, the ideological attachment to notice and choice, a weak form of consent, as well as the third party doctrine, stand in the way of the radical reorientation use-based regulation advocates are proposing. In addition, existing experiences with use-based regulation in the US context can hardly be described as a resounding success.

Alexander Roßnagel and Philipp Richter, finally, have examined the German notion of 'Informational Self-Determination'. The right to Informational Self-Determination was concretized by the German Federal Constitutional Court in 1983 from the basic liberties in Art. 2 I and 1 I GG as adequate protection against the risks of modern data processing. According to this right, data subjects themselves may generally decide about the extent of disclosure and processing of their personal information. Along with Freedom of Information and Secrecy of Telecommunications, Informational Self-determination is the central basic right of the information society. Informational Self-Determination covers the protection of the individual as well as the objective protection of a democratic society.

On the one hand, it enables freedom of decisions, including the possibility to actually act upon these decisions, while, on the other, it makes possible the self-determined development of the individual. Informational Self-Determination is not only an individual right of the data subject, however. It is also the foundation of a free and democratic society. Roßnagel and Richter argue that the classic principles as entailed in the Data Protection Directive, among other things, follow from

the principle of Informational Self-Determination, such the required legitimate ground for processing, purpose limitation, data minimization, transparency, rules regarding profiling, etc.

They signal that each of these principles are put under pressure by Big Data and mass surveillance developments. They specify three risks to this basic right, namely individualized surveillance, pattern recognition, and behaviour prediction. With regard to the first, they argue that the new basic rights challenge is that recent principles for the protection of Informational Self-Determination and Secrecy of Telecommunications, such as purpose binding, necessity, and data reduction lose their effect. With regard to the second, they observe that Informational Self-Determination in its recent shape will not suffice as protection against this normative effect of Big Data. Recognition of suspect behaviour patterns can be conducted using anonymous data, to which data protection law does not apply. With regard to the third, they argue that if police and intelligence agencies used Big Data Analytics to predict future individual behaviour, this would raise fundamental rule of law issues, as when investigation is initiated, for example, prior to reasonable suspicion, which would aggravate the focus on preventive security. This may put fundamental principles such as individual guilt, the presumption of innocence, and reasonable suspicion under threat.

1.3 CONCLUSIONS OF THIS BOOK

As we have observed above, this book serves as preparatory work for the Netherlands Scientific Council for Government Policy's advice to the Dutch government, which has asked the Council to address four specific questions regarding Big Data, security, and privacy. This book should provide the Council with the building blocks for its advice and for developing a regulatory approach to Big Data.

Four general points

First of all, the reality of Big Data is constantly evolving, which makes it difficult to define, to delineate, and to approach it from a regulatory point of view. In addition, Big Data is a node, and many different aspects play an important role in studying this phenomenon: not only technical, but also organizational, societal, and legal aspects come into play. From a technological point of view, as pointed out by Klous, technological developments and new applications are intertwined and sometimes confused with Big Data, such as the Internet of Things, cloud computing, profiling, the use of algorithms, machine learning, etc. From a societal perspective, as Galdon Clavell has observed, developments such as securitization, commodification, informationalization, privatization, and an increased focus on prevention are taking place. The legal chapters show that many scholars and regulators are aware of the new threats to the underlying foundations of the current

legal regime and the need for new regulations, such as those provided by the General Data Protection Regulation of the European Union. Consequently, Big Data is not an isolated phenomenon, but in a sense is the umbrella term for all these different developments that are taking place at different levels.

Second, to the question what Big Data really is, no exact answer has been found. Rather, this book has explored the boundaries of this new phenomenon; it has mapped the outskirts of a new-found island, but its inland areas have remained largely unexplored. What has become clear is that it is difficult, perhaps even impossible, to point to one or a few criteria that are the intrinsic elements of this phenomenon. As Klous has pointed out, the relevance of each of the three classic Vs can be disputed, and he suggests that two other Vs should be added. Other authors embrace a host of definitions, thus showing that it is still too early to map out the new territory with any accuracy. Still, all authors feel that it is important to address this new trend, as all believe that it will bring fundamental changes to their field of expertise.

Third, the government is rightly interested in Big Data, for two reasons: Big Data's potentially positive effects, but also its potentially negative effects. The positive effects are pointed out by Klous, who has hinted at Big Data's economic potential and its use in the private sector. De Hert and Lammerant and Van Brakel also refer to the use of Big Data techniques for predictive profiling purposes by the police. This might not only have a beneficial effect on the distribution of resources and the effectiveness of policing activities, but Big Data may also have an empowering effect on citizens, as Van Brakel suggests. Many authors, however, also emphasize the potentially negative effects of Big Data. Roßnagel and Richter point out that almost every classic data protection principle is put under pressure in Big Data processes. The same has been observed with regard to the Fair Information Practices (FIPs) by Bennett and Bayley and with respect to the fundamental right to privacy by Van der Sloot. De Hert and Lammerant and Van Brakel also signal potential problems regarding discrimination and stigmatization, especially when Big Data is used in relation to predictive policing and group profiling. Authors have also pointed to the Kronos effect, the Matthew effect, and other potentially negative effects. In conclusion, Big Data might have added value when used correctly and appropriately, but it might also have negative effects when applied inadequately. New policies and regulations, therefore, may help to guide the use of Big Data in the right direction.

Fourth, most authors signal a duality with respect to the current regulatory framework in the age of Big Data. On the one hand, they feel that the core principles of privacy law, data protection legislation, discrimination law, and the human rights framework are valuable and should be maintained in the Big Data era. On the other, these principles are often fundamentally at odds with the core of Big Data

processes. It is suggested, consequently, that the current principles and frameworks should not only be maintained, but that new laws and regulations should also be introduced to tackle the new challenges posed by Big Data, in order to protect the fundamental values of the democratic rule of law.

Building blocks for answering the four questions of the government

The first main question from the Minister to the Netherlands Scientific Council for Government Policy was whether a stronger distinction should be made between access to and use of information in Big Data processes. Joris van Hoboken has analysed the current regulatory framework in both the EU and the US and their underlying foundations. It appears that both EU and US law entail principles that limit the collection and storage of personal data and contain rules on the use of personal data for specific purposes, even though the EU is more prone to regulating the collection of data and the US has several additional rules limiting the use of personal data compared to the EU. Van Hoboken sees the limitations on the gathering of personal data as intrinsically intertwined with the underlying fundamentals of data protection principles, with the notion of informational self-determination in the EU and with the idea of notion and choice, linked to the value of individual autonomy, in the US. It would appear to be unrealistic, therefore, to abandon regulating the gathering of personal data; rather, European law could supplement the current rules on gathering personal data with more and stricter rules on the use of personal data, inspiration for which might be found across the ocean.

The second key question concerned the use of Big Data processes and of techniques such as profiling and data mining. In particular, the Minister wished to ascertain how these techniques can be used in a transparent manner and how adequate checks and balances can be formulated to allow these techniques to be used safely and carefully. The studies by De Hert and Lammerant and Van Brakel show that this will be one of the key challenges for the next decade. Profiling has been used for a long time but will gain new momentum with the rise of Big Data. Not only the risks of discrimination and stigmatization are pointed out, but also potentially Kafkaesque or 'computer-says-no' situations. The fear is that computer programs and algorithms will increasingly lead their own lives and replace human-led decision-making processes. Both contributions suggest that transparency is key here, but that legal obligations curtailing the use of profiling should also be developed. Although such principles are currently already in place in anti-discrimination law, data protection law, human rights law, administrative law, and penal law, De Hert and Lammerant suggest that, in order to properly protect citizens' interests in the Big Data era, they need an overhaul.

Thirdly, the Minister referred to the emergence of quantum computing and asked whether encryption and anonymity can still be guaranteed in the future. Especially Gürses and Preneel have dealt with this point. They suggest that, for the past

two decades, researchers have been working on novel cryptographic algorithms that would resist quantum computers. The focus has been on public-key algorithms, but it cannot be excluded that novel quantum algorithms will be discovered that reduce the strength of symmetric cryptographic algorithms beyond the quantum square root attacks known today. For public-key cryptography (both encryption and digital signatures), approaches are being studied that are typically faster than the current schemes, but most of them have much larger keys. For some of them, evaluating the concrete security level is challenging, and it cannot be excluded that novel quantum algorithms will be discovered that may weaken their security. It can be expected that it will take three to five years before these schemes will start appearing in cryptographic standards, and that it will take another two to four years before efficient implementations are widely available. This is a concern for encryption schemes because even in 2016 there is information that should be protected for ten years; this would mean that those schemes should be used today. This is less of an issue for digital signatures, and one could re-sign all documents every three to five years with improved algorithms with larger keys.

Finally, the Minister wanted to know how the autonomy of citizens can be ensured in Big Data processes. This relates to the question whether a focus on informed consent is still tenable, what possibilities citizens have for effective control over their data, what responsibility citizens have to contribute to the quality of the data in databases, and, more in general, how maintaining quality of information can be guaranteed. Both Van der Sloot and Bennett and Bayley have suggested that the current regulatory framework primarily focuses on individuals, their rights, and their interests. The protection of the individual, they feel, is important and should be maintained. Still, it should not be the sole approach in the Big Data era.

First, individuals are often incapable of protecting their own interests through individual rights because they are often unaware of their personal data being gathered and because it will be impossible for them to keep track of every data processing which includes (or might include) their data, to assess whether the data controller abides by the legal standards applicable, and if not, to file a legal complaint. Consequently, individual rights should be supplemented with more general forms of legal protection, such as more and stricter obligations and duties of care for controllers.

Second, the interests involved in Big Data processes often transcend individuals and their interests and affect group and societal interests. Both Van der Sloot and Bennett and Bayley have suggested to focus not only on legal rules but also on ethical evaluations and, hence, to consider using Ethical Impact Assessments in addition to Privacy Impact Assessments.