# Smart Data Protection

Peter Blume

## 1 Yesterday and Tomorrow

Writing an article, celebrating an anniversary, there are several possibilities. An option is to look back and view the years that have gone by. How was it in the beginning and what has been achieved? Did research follow a clear path and did it lead to the desired destination? With respect to the Swedish IRI this is a tempting possibility. From almost nothing and in the midst of a skeptical university environment, to say the least, the institute was instigated by Peter Seipel, demonstrating that persons and not just systems have importance. It was an innovative event although only few was aware of this at the time. Through the years, major insights with respect to legal informatics have been achieved, important contributions to the curriculum have been made and are visible today, significant research results have been produced, and a recognized role in law making has been achieved. IRI is well-known not just nationally but also internationally. Much has been achieved and the results but also the mistakes which sometimes are just as productive have made an impact and there is much to be proud of. This impressive past demonstrates that the future appears promising and that celebrations are in order.

The nostalgic tour is accordingly tempting but it will not be made here where the opposite path is taken. The look to the future. The past contributes to the future but the main interest is the future as it may be viewed and predicted from the perspective of the present. It is by far certain that assumptions about the future are correct or at a later stage even expedient but in the field of it law, both the formal and the substantive part, the future is always with us; developments are constantly moving and affecting the legal environment. The researcher cannot stay where he or she is because the law and the formative technology is changing all the time presenting new challenges and new question marks. This is the fascinating but also the frustrating characteristic of it law. Sometimes the legal environment is overwhelming dynamic. Although not everything changes and basic knowledge of the relationship between law and information may often be a constant and fruitful platform the ground is moving and it is likely that this will be the case for many years. The old saying, “panta hrei”, that you never step down in the same river, can be applied to it law. Although you can only contemplate the future from the present this has to be the direction. Accordingly, the following mixes the present and the future.

Focus in the following is on data protection which today is one of the main fields of legal informatics/it law. It is by far as technical as other parts of it law and many, but not all, its aspects may be considered without a detailed knowledge of information technology even though they are often determined by this technology. There is challenging insight and problem solving but the main reason for the attraction of data protection law lies in its impact on the basic values of society and its appeal to civil society and citizens in general. Every citizen is affected by data protection even though it is not always obvious for the single person. It is not necessary to argue that this legal domain is relevant and this is recognized in general. Data protection law is broad and in some sense this law is everywhere due to the fact that it covers all kinds of personal data. Personal data is processed in all parts of society and there is some truth in the observation that

in the information society the importance of personal data may be compared with the role played by oil in the industrial society. Personal data constitute a driving force. Public authorities and private enterprise need personal data to exist and the fundamental and often complex issues emerge because the data relates to individual citizens. In principle, the law as it is drafted relates to data and not individuals but in practice the privacy interest of the individual is the reason for data protection law and it is the individual who benefits from it.

Questions related to divergent interests, control, privacy and integrity emerge and pose difficult value and political problems. They create a dynamic context and they are linked to the technology in the sense that the different issues are connected to the methods of processing. In this way data protection becomes a child of modern digital technology and its legal policy agenda is often determined by new kinds of technology or new applications of this technology. Cloud computing being a well-known example. From a general point of view, data protection law constitutes a regulation of the technology enabling the acceptable use of the technology at the same time aspiring to control how the technology is applied. This is not an easy agenda and data protection is ambitious law.

## 2 Briefly on History

Data protection law has a fairly long history when perceived in an it law context and it is has a future which is partly known. This future is the general data protection regulation (GDPR, 2016/679) which formally began and made its impact 25.May 2018. In this sense, it is easy to write about the future and the GDPR will also be the starting point in the following sections but it is not the final word and there is a future beyond the GDPR although it is unknown when it starts. The Regulation will be assessed every fourth year according to section 97 but it will be many years before formal changes are made. It took four years to enact the Regulation and the prospect of amendments is not tempting. However, as changes will take place constantly it is expedient to consider both the near and the distant future. This is also necessary as the future today much quicker than previously becomes the present. Time has become something different not least due to the technology. Science fiction quickly becomes fiction.

Even though the GDPR currently is the future it is by far detached from the past. Data protection is a child of modern information technology. As many other children of this technology it has even more distant parents as it may be viewed a child of the general right to privacy that has roots way back before digital technology became a societal player. Back to the time when the computer was only a dream. The most famous text in privacy and data protection literature, almost always referred to in American law review articles, is from 1890, The Right to Privacy with the famous statement that citizens have the right to be let alone.[1] The article is motivated by the then modern technology, photography, and

1 Samuel D. Warren, Louis D. Brandeis: *The Right to Privacy*, 4, Harvard Law Review (1890) p.193-220. – Much law is interconnected and in this case the inspiration at least in part came from torts law.

in this it is founded on the relation between law and information. The importance of informational control and the right not to be surveilled can be traced to this article.

However, data protection is a peculiar and independent child, as even though it has a much more limited scope than privacy it is much more complicated than its parent. Its aim in life is to achieve many different purposes, and also purposes that do not always relate to the same interest or lead in the same direction. It is a complex and often difficult child although it tries to be loyal to its parent and also recognizes its debt to its parent. With respect to the GDPR this is also the case in connection to its close relative, the data protection directive. Privacy has general importance even though the link to the European convention on human rights is not as close as it used to be. While the recitals to Directive 95/46 referred to the ECHR the recitals to the GDPR refer to the EU Charter.

It is not quite certain when data protection as an idea was born but legally this was the case in Hessen in 1970[2] and the first full born child was conceived in Sweden through the Datalag (1973:289) in 1973. In many ways this is the most famous Swedish contribution to the formal field of legal informatics and though this act is long gone and much is obsolete it will always be a major contribution. This contribution should not be forgotten although it will not be discussed in this text.

Some years after the Datalag emerged other national statues were enacted, e.g. in Denmark and West Germany (1978). At the national level data protection is an European invention. However, in 1980 the OECD issued guidelines that were coordinated with the Council of Europe convention 108/81. Only slowly and sometimes reluctantly other European countries introduced legislation. The laws of this period were characterized by more or less directly emphasizing the register, i.e. centralized electronic data processing, the main frame computer. Accordingly, the focus was mainly upon the state as processor of personal data which underlined the human rights perspective. This was natural when taking account of the available and applied technology. As it is well known focus has now changed and the private sector is now just as much or even more[3] the theme in data protection law. The information technology has changed character and it is available for everybody and today also necessary for everybody. Anybody can be a data controller, article 4 no.7, implying that data protection law is relevant not just for all data subjects but also for more or less all persons as controllers. All have rights and obligations. However, the state and the infamous Big Brother still form an essential part of the law, and Big Brother, although only rarely mentioned today, is very much alive, manifested in extensive surveillance.

The technological developments, cheaper and mobile computing, form the background for modern data protection law that takes its starting point in Directive 95/46 EC. This legal act is the most important in the story of data protection and

2 Hessiches Datenschutzgesetz from 7.October 1970.

3 Many of the rules of the GDPR are drafted with respect to data processing in the private sector and it is therefore often considered whether these rules fully or partly should apply to the public sector.

even more important than the GDPR which is the focus of this article. It is the Directive that changes the face of data protection and it does so by introducing the concept of processing and letting this concept determine the framework of data protection law. The Directive makes data protection broad and comprehensive and processing still constitutes the current paradigm of data protection. Without the Directive there would be no GDPR. This paradigm provides a very extensive field of data protection and as a starting point it has none or little importance which kind of processing takes place. As long as the processing is digital or aimed at a file it is covered by the rules. Compared with the original register acts the Directive represents a kind of revolution and as stated above it is interesting to notice that with respect to the basic demarcation of the legal regulation, the GDPR is a loyal continuation of the Directive as indicated at the start of Recital no.9.[4] Even though there is much more personal data now than when the Directive was enacted no basic changes have been made in the legal approach.

A basic consideration is whether data protection law is efficient and actually provides citizens with a sufficient protection of their personal integrity and privacy with respect to information. Data protection law is characterized by using many words including very fine words but the question is whether it sustains the protection it is aimed at. This issue has been topical from the start and it has often been assumed that data protection law is not as efficient as it should be. The data controllers do not sufficiently respect the rules and it is difficult to ensure that they perform better. The fundamental problem is that data protection aims at achieving a situation that contradicts the possibilities the technology provides to private enterprise and public administration. For example, modern e-government and data protection does not fit well together. A major asset of the technology is that it enables quick and broad data processing combined with data sharing. In general it is the ability of the technology to be a platform that can process data in almost any way which makes it useful and which shapes modern society and makes it into a digital society. This society prioritizes networking that presupposes access to personal data. Data protection restrains this ability in order to ensure that the digital society is a civilized society conforming to democratic values. A main purpose is that there is trust and that citizens view the digital society as their society.

Data protection is an obstacle. For this reason data protection has been in stormy waters from the beginning and it is still very wet. Even though data protection law in general is recognized today and even though there are new and updated rules its performance is still doubtful. In many respects it is not welcomed law and there is still much opposition. Data protection has an impact but it is difficult for it to fulfil its purpose to its full extent. No law is completely perfect and it is always an ambition that it should be more efficient than it is and this is a necessary goal for data protection which is a quite a low point.

The GDPR faces this challenge by increasing the seriousness of its different rules. It imposes high administrative fines (Article 83) that have led to panic at many controllers and processors. These sanctions will not increase the

4 The GDPR is drafted on the basis of the Directive. The question has been which rules should be continued, which should be amended, and what new rules are needed.

understanding or even the love of data protection but even though it is common knowledge that criminal sanctions are not a magical tool it is likely that data protection rules will be respected to a higher degree in the future. Maybe the GDPR in this respect is founded on the old saying of Caligula that it does not matter if you do not love me as long as you fear me. There is little doubt that data protection law is feared today.

Data protection has to be adjustable as the technology constantly changes and new ways of data processing emerges. The aim of the GDPR is to sustain the purpose of data protection and to ensure that it stays alive. The understanding of changes indicate that flexible rules must be preferred instead of traditional legal rules. There must be openness on the expense of predictability. Rules should not be linked to specific kinds of digital technology but to the contrary be neutral. It is this mode of drafting that made the Directive almost 20 years old regardless of for example cloud computing, and the GDPR in the same way contains many flexible rules that are not founded on a specific digital technology. Such rules promote a sense of constant changes or innovations. For this reason, the consideration to risk is a fundamental part of the GDPR as it is outlined below in sections 4 and 5.

## 3 Data Protection by Design

The feeling for change and the application of open adjustable rules is evident in the introduction into European law of the concept of privacy by design in GDPR article 25[5]. Originally, this is a Canadian concept but article 25 is an independent rule. Data protection by design is flexibility at the highest order as the exact meaning of design is and probably should not be determined once and for all and as it accordingly from the beginning is not obvious when data processing does not meet the design requirement. Design is an open but binding invitation to be aware of data protection. It may be seen as a wake up call. This is to a large degree deliberate. Against this background, it is not obvious that it should be possible to sanction a data controller solely for not having design but regardless of this assumption lack of design is included in article 83(4) on administrative fines[6].

In other words, the question is whether there are certain actions and procedures that signify design and whether they are not covered by other rules in the GDPR. Article 25 does not prescribe certain methods but merely mentions two examples that may signify design. First, that there should be minimal use of personal data but this rule already follows from article 5(3) and is a basic principle of data protection. This is often taken for granted but the controller must always be able to explain why it is necessary to process data in personal form. It is likely that many controllers do not consider this question but there is no doubt that they

5 This rules also covers protection by default but this issue is not included here.

6 At least in Danish practice there has been a tendency to let decisions have authority in many data protection rules resulting in uncertainty about what has been decisive. This might also be the fate of the design rule.

should. The second example is that pseudonyms should be considered used by the controller. Pseudonyms are defined in article 4 no.5 and are mentioned as examples in other rules so this consideration is not entirely new. Pseudonyms are personal data but they increase data security as they limit access to the data even though they are not an exclusive security measure in a strict sense.

There is uncertainty with respect to the design requirement and this is expedient unless a strict legal approach with emphasis on predictability is taken. Regardless of uncertainty, design is something in itself as it very broadly states that the controller has to think data protection and organize the data processing in such a way that data protection in all respects is ensured. There is no fixed standard and the means will differ from situation to situation depending on the nature of the line of business and the connected data processing. Design is an individual approach. This is not common in legal regulation and it will be interesting to observe whether this understanding is recognized in data controller practice and especially by the supervisory authority. In particular, the authorities will face difficulties and will have to avoid the temptation to fence design into fixed traditional rules. Practice must be flexible and free resembling the idea of the design concept. There will be similarities between processing situations but in principle each case will be different. This is not very "legal" and in this way the design rule poses a challenge to the supervisory authority.

Design is culture when it is viewed as something in itself and this is an expedient approach in order to enhancing data protection as design does not have meaning if it merely is viewed as a headline for other obligations. The controller and his employees and others involved in the processing have to think data protection and the question is how they do that. As indicated only a tentative answer is possible today. There has to be an idea of the importance of personal data and how to protect the data together with an understanding of the reasons sustaining protection. As stated, design is culture and this culture has to be integrated into the processing. This implies that the controller must understand the way in which the GDPR views personal data and the instruments that it deploys. Even though design is an independent concept it is the instruments laid down in the GDPR that provides inspiration for design and good data protection. In this sense, substantially design is not something original but an invitation to employ all relevant instruments in a way that fits the specific situation and framework. Additionally, the controller must furthermore be aware of new instruments that are developed in the coming years. There is not design once and for all. The controller must be alert.

In general, it is the combination of data processing and data protection that is the starting point when design is achieved. In this way, the controller is looking to the future even though applying instruments that are presently known. This is a challenge, and it will be interesting to observe how the design rule works when the GDPR is applied in practice. The basic question will be whether the future will be accepted and respected in the present.

## 4 Risk

The GDPR is oriented towards the future in other ways. First of all it is based on risk. It is the possible risk of data misuse related to a certain kind of data processing that determines the actions which must be taken by the controller and the processor. There is not a common principle of risk in the GDPR and the concept is not defined in article 4. It is not clear what risk actually means but none the less the consideration to risk underlines many of the rules. In general, this makes data protection dynamic and requires that the data controller considers future implications of his processing. It is not sufficient to take account of the present situation as it must be considered how it may or will develop and affect the protective interests of the data subjects. Current risks are important but the dynamic approach attracts most interest. The future is not known and this means that there is uncertainty attached to an assumption of risk when it determines the protective measures that must be applied. However, the technology is innovative and the law has to be the same. In this way the new regime is demanding on the controller and as a reflection also on the data protection authorities. The question is how risk is assessed and accordingly how the good controller may fulfil his obligations. This is not in general very clear and the GDPR is not helpful in this respect as its rules are written from the perspective of the present. However taking account of how the technology changes and new modes of data processing emerge it is expedient to look to the future and consider possible dangers or risks for the data subjects.

A main example of the importance of risk is the assessment of the processing of sensitive data according to article 9 and 10. It is a simple assumption that usage of this kind of data is more likely to infringe the integrity of the data subject than processing of ordinary data. This is well known and the question is whether the consideration to risk leads to something new and whether the controller must do something else compared to the Directive that did not make risk an explicit issue. It is not obvious that processing of sensitive data in itself always poses a risk in the sense that the future is different from the present. Many data controllers know that they have to be especially aware when processing sensitive data even when they are within the formal boundaries of article 9 (2). The risk concept does not seem necessary in order to determine what the controller must do and accordingly it is not obvious that the GDPR in this sense imposes new duties for the controller. Even so, the inclusion of risk may increase the awareness of the controller.

The inclusion of ordinary personal data in data protection law makes the concept of risk especially relevant and maybe disturbing. It could be argued that risk understood as some kind of warning is relevant when the controller takes the context in which ordinary data is processed into consideration. This is another starting point than the normal approach where context does not play a decisive role. Certain kinds of processing situations mainly including ordinary data impose a risk that makes special precautions necessary. It is in this way the future becomes a necessary factor that can enhance the level of data protection. In particular, the consideration to risk is important with respect to situations where the context does not change the data from ordinary to sensitive, but merely signifies a danger for the data subjects. It is here the controller has to be especially alert.

Data security is a special area. With respect to the measures that have to be applied in order to achieve data security risk is a reasonable concept to take into account. Security must consider future developments, including unwarranted openness, and in this way diminish the risk that security measures are compromised. In this area it is easy to see the usefulness of applying risk but this is to a large degree not new compared to the Directive.

There is a difference between today and tomorrow. A controller must be aware of possible future situations where the nature of processing changes and if possible take account of these situations. There may be risks that are not topical now but if they occur then the controller must be ready to act although it is not always evident how he should act. This is also an issue for the supervisory authority. Data processing does not in general have to be notified and this means that the authority in most cases has to look back at a processing that is taking place currently or has definitely occurred. In many cases, it seems difficult but not impossible to assume that because the controller has not applied a risk approach this has led to some kind of data misuse. It is always easy to look back but it should be taken into account that the controller has tried to look ahead. It is likely that the evaluation theme is the present and even though risk may be a good approach its practical implications are not in most cases evident or easy to comprehend for the controller. The authority will have to demonstrate that the controller could and should have taken another approach and a possibility is to apply the concept of lawfulness in section 5(1a) as a starting point.

In any case, the dynamic technology poses problems as only few controllers actually understand the technology or are able to use it. Even though digital technology in general is perceived as progress and everybody uses it this technology also casts a kind of shadow over data processing and protection. In some sense, we are dancing in the dark and not really seeing who we are dancing with. However, in some situations assistance may be gained from either a processor or a DPO. Risk is all in all not an easy concept to work with, and this is also the case when the GDPR as described in the next section especially focusses on processing that entails a high risk for the data subject.

## 5 DPIA

In article 35 it is stated that the controller in certain circumstances has to perform a data protection impact assessment. The controller must conduct an analysis that clarifies whether the planned data processing poses a high risk for the data subject and if this is the case determine the means that may reduce or remove this risk. A possible future has to be prevented and the measures have to be viewed as necessary in order to carry out the processing. This has to be verified by the supervisory authority (article 36). The DPIA is only necessary when there is a high risk, not just a risk. A DPIA is a burden on the controller and is only imposed when the processing is dangerous.

In this respect, the GDPR takes a specific approach in article 35(3) stating situations where there may be a high risk. This is the case when processing aims at profiling the data subjects in order to make decisions, and when sensitive data

is processed, and when the processing purpose is to surveil people in public spaces. This list is not exhaustive but provides guidance to the controller. Maybe this rule solves the issue discussed above in section 4 and maybe not because these examples are static and at least not directly future oriented. Without specific deliberation, high risk is linked to current processing in the sense that it is assessed from the perspective of today whether there is a risk. However, this may to some degree be changed as the data protection authorities are required to issue lists stating when a DPIA has to be carried out. It is accordingly recognized that a controller often will not know when there is a high risk that makes an analysis necessary. It may still be the perspective of the present that dominates. Undoubtedly, this is realistic and it makes the application of risk less dynamic that it could have been.

It is interesting to notice that the DPIA framework is not related to the applied technology but to the processing situations. A high risk may occur regardless of whether the controller knows how or why the applied technology functions as it does. This could be a limitation but as mentioned in any case the prescribed analysis is a method to determine risk with respect to how the actual processing should be carried out. This is a step in the right direction but a step only to be taken when it is assumed that the risk is high and a step that is mainly taken by controllers in the private sector. As a DPIA is a burden for the controller the assumption in the GDPR is that they will only be necessary in few cases. It is possible voluntarily to perform a DPIA and in those situations they will merely be a internal instrument at the controller.

In the public sector an analysis performed in connection with the enactment of a statute that authorizes the processing is sufficient according to article 35(10). This is somewhat strange. The GDPR covers with few exceptions, article 2(2), all personal data processing and there is no systematic distinction between the private and the public sector but none the less many of the rules make this distinction and provide a special and privileged position for the public sector. In principle, the supervising authority can decide whether the legislative process in this respect is actually sufficient but it is likely that it in practice will be assumed that a DPIA is not needed in the public sector. The public authority escapes this burden. The notion of high risk is recognized but the practical consequences in the public sector are probably few.

## 6 Smart Data Processing

The GDPR is aware of the fact that information technology is constantly changing and that this reflects in new kinds of data processing and new risks for data protection. As previously mentioned rules are drafted in a technology neutral way so they may be applied to situations not known today. This is how it has always been in data protection law. As it will be extremely difficult to amend the GDPR it is likely to have a long time span just as the Directive had and in practice it will be adjusted to kinds of processing lying beyond the horizon. From this perspective, the future is interesting and it is relevant to take account of situations that could occur in the near future and therefore meaningfully may be considered

today. An obvious example is the application of so-called smart technology, including robotics.

Basically, there are two kinds of robots, the mechanical and the intelligent. The mechanical robot performs fairly simple labor tasks, e.g. fixing cars in the car production factory, and this robot has no general interest with respect to data protection. The intelligent robot performs human tasks simulating the human brain and may be a factor, and a disturbing one, with respect to personal data processing. This kind of processing may pose a challenge and make it difficult to ensure that the different rules are adhered to. Developing artificial intelligence has been a dream for centuries but today it is increasingly becoming a reality and is a field of science that develops in a quite rapid pace. No one knows how far it may go. The fully intelligent agent has not been constructed but it is more than distant imagination. This agent may become an integrated player in the processing of personal data.

The intelligent robot is a machine but when it is a robot the machine appears more friendly, more human, and more easy to accept. Regardless of such impressions, intelligence substitutes man and this must be taken into account when considering how data protection will be affected and how it is achieved. A basic question is whether the intelligent robot is a good development that does not pose an obstacle for data protection or whether the robot is a dangerous development that entails that processing of personal data comes out of control with lack of transparency. Additionally an important question is whether it becomes uncertain how data is processed and who is responsible as the controller. Another and more positive issue concerns to which extent artificial intelligence may be utilized in the service of data protection.

From the general perspective follows two approaches. AI and robots are conceived as progress that improves the life of humans while still maintaining that humans are in control. There is nothing to be afraid of and the main task, if necessary, is to adjust the legal rules so they conform with the situation created by AI. These rules must confirm the importance of data protection and ensure the rights of data subjects. The rules must also determine the obligations that the controller has to meet when using robots to process personal data. Robots may even be intelligent in the sense that they take care of personal data and maybe such robots represent the ultimate data protection per design. This is the perspective taken in the following but there is another point of view that looks at AI as something disturbing and challenging. Humans have been playing God and AI will transfer power to the machine. It will be the smart robot acting as an independent agent who processes personal data and decides which rules in reality determine the processing. Data processing and protection will come out of control. The robot will be the controller and also the processor. This caution that reflects warnings from science fiction should not be neglected as there are dangers. However, as stated it is the positive perspective that frames the following.

When the machine or the robot is intelligent it is able to make decisions and these may determine the processing of personal data and affect the integrity of data subjects. Such decisions may not always be transparent even for the human data controller. An example being an intelligent system that can assess job applicants while utilizing information about the qualifications that are required in

the specific job. The problem is whether there is sufficient knowledge available about how the machine works and reaches its results. The logic used by the machine must be transparent but it may easily be questioned whether the system or the employer is the actual controller. This is especially relevant when it is the system who selects the persons who are employed; i.e. when the system functions as more than merely decision support. This part of the brave new world is already a reality today.

Article 22 of the GDPR concerns this issue in the same way more or less as previously determined in the Directive (article 15). According to this rule a data subject has the right to have a negative fully automated decision based on a profile reviewed by a human unless the system is used within a contractual relationship or it has authority in statute. These are vast exemptions and accordingly there is not complete openness. The review does not have to change the result. It is accordingly accepted that such decisions are made although they cannot include sensitive data unless the data subject has given his consent or decisive societal interests sustain processing. With respect to ordinary personal data there are no real limitations. In article 13 it is stated that the data subject must be informed about how the system operates and which logic is employed. There are also limitations at this point as private interest, i.e. commercial secrecy and intellectual property rights, and public interest, i.e. state security, according to article 23 may sustain that this information is not provided. It is not certain that there is transparency for the data subject but at least it is presupposed that there is transparency for the controller. Whether this actually will be the case is doubtful and will be demanding on the controller.

Accordingly, personal data may be processed automatically in a way that is kept secret for the individual. The robot may process personal data in a secluded manner. It is tempting to conclude that the GDPR does not provide sufficient protection with respect to the data processing of tomorrow. Artificial intelligence is not really visible in the GDPR. Article 15 in Directive 95/46 was a rule that looked to the future when it was enacted in 1995 and it was probably the most advanced provision in the Directive. It is disappointing that article 22 of the GDPR more or less is the same rule now that the future has come much closer and is almost topical.

Article 22 or other rules in the GDPR do not go very far and in particular it should be observed that they do not really take account of big data. This is disturbing as the use of big data through data mining techniques linked to knowledge based systems increases the accessibility of the data. Big data is a challenge as the gathering of extensive amounts of personal data reveals the individual person, makes him transparent and informational naked. Big data symbolizes the frightening observation that the computer knows more about a person than the person himself. This data is normally used commercially but also as a means of surveillance sending a signal of a future society which is open in a negative way. The individual becomes too transparent and there may not be any place to hide in the future. While it in general may be uncertain how artificial intelligence will influence the possibility of data protection, application of big data is well-known and the GDPR has missed an opportunity to impose limitations.

This observation presupposes that a meaningful rule could have been drafted and this must be considered. Drafting such a rule faces the same challenge as the data protection by design rule as it should add value and consist of something that is not already part of the GDPR. It should enhance data protection law. Some of the GDPR rules are relevant with respect to big data. Article 5(1a) stating that processing must be lawful is always relevant but this is in reality not especially helpful although it provides the supervisory authority a platform to act. This is also the case with respect to article 5(1b) that prescribes that the purpose has to be legitimate and furthermore that personal data may only be processed when purpose limitation is respected. It will often be doubtful whether this is the case and as described below it is not obvious how big data conforms with purpose limitation and how this in practice is determined. Article 5(1c) on proportionality may also be mentioned. Another perspective could be article 5(2) that stresses accountability which is also a general principle of the GDPR. Controllers who apply big data have to ensure that the data protection rules are respected even if the controller is a machine. Other rules could probably also be mentioned.

However, these rules do not very precisely limit or regulate usage of big data or other kinds of processing which is founded on artificial intelligence. The question is accordingly whether these general rules are sufficient or whether a special designed rule could more precisely determine data protection with respect to artificial intelligence. Such a rule could be drafted in different ways. One option might be to introduce a more tight purpose principle stating that when personal data is compiled from a multiple number of sources or automatically compiled then they can only be used with respect to a purpose compatible to the collection purpose[7]. In order to ensure that such a rule promotes transparency the original purpose must be precise and easy for the data subjects to understand in accordance with the principles of article 12. Although this rule will restrict this kind of data processing to some extent it will mainly promote transparency which is not in itself sufficient but often the realistic goal. It must be added that such a rule will go against the trend in the GDPR. In section 6(4) the purpose limitation rule is modified and it is made possible within the boundaries of article 23 in national law to have rules that make it possible to process data for a incompatible purpose. Accordingly, this might not be a realistic way to go.

Another option is to make article 13 more precise and to prescribe that the human controller must document how the robot or machine functions and accordingly how it processes personal data. A controller may not use an intelligent robot or machine if he does not know how it functions. Such a rule may have exemptions in order to accommodate commercial interests but not in all respects as it could in some situations be sufficient that this information is only disclosed by the controller to the supervisory authority and not to the data subject. The machine should not be a mystery and the authority can act on behalf of the data subjects. It is ensured that at least the controller knows how the intelligent system works and such user transparency should be necessary. This rule promotes accountability and in the brave new world created by artificial intelligence it is

7 This means a more strict rule than section 5(1b) as it is not sufficent that the purpose is not just incompatible.

essential that there is at least some kind openness. The controller must be trusted and a basic goal is that data subjects are not afraid and do not have a reason to be so.

It may be considered whether actual restrictions could be instigated. This is not the usual position in data protection law. The rules set up conditions for processing but do not normally outlaw specific kinds of processing. A rule prohibiting use of big data through data mining is not a possibility and will not be realistic. The same is the case with respect to application of robots and AI. Transparency is still the key word and besides a need to know principle covering the controller it is as indicated above a possibility is to extend or make more precise the obligation to provide information in articles 13 and 14. When data from many sources are used in some kind of action towards the data subject information must be provided both with respect to all the sources and how the data has been combined with respect to a certain purpose. This is likely to increase openness and maybe even trust.

Much more can probably not be achieved. It is uncertain what artificial intelligence will bring to data protection and whether this kind of processing will endanger the integrity and privacy of data subjects. The future is and always will be uncertain. It is not obvious how data protection law should react. The aspiration must be smart data protection.

## 7 Smart Data Protection

Finally, it is natural to consider whether there can be smart data protection. The question is whether AI and other forms of smart technologies can be applied in order to make data protection more efficient and data subject friendly. It is a common assumption that most persons do not know that they are data subjects and do not know their rights or their position or how to act in this respect. Placing the controller in the lead role signifies this assumption as it is the controller that guarantees the lawful protection of the individual data subject. Data protection is dependent on this agent who is not always interested in providing data protection as the controller is forced by the law to play this role.

New technology could maybe remedy this situation and it could make the data subjects and the supervisory authorities more efficient. Today, it is mainly with respect to exercising the rights the robot might make a difference increasing transparency. The controller will be able to use AI and make transparency real and increase the information level. There are no exact rules on the mode in which the different rights should be provided to the data subject, and improvements will accordingly not meet legal obstacles. The controller should feel free to experiment.

At the same time, the supervisory authority ought to encourage use of new technology in a data subject friendly manner and invite AI to join the data protection environment. AI and the robots may be good contributors with respect to increasing data security. Smart security could be a catch word. The robots could be the PETs that combat the PITs.

Finally, a basic issue is whether smart techniques and especially robots could and maybe should act as independent agents in data protection law. A question is

whether a robot can be a controller. According to GDPR article 4 no.7 anybody can be a controller. As a starting point there are no limitations. In this respect, it is important to notice that most controllers are not individuals but public authorities and private enterprises. In some sense they are not humans even though it is human beings that represent them. From that perspective, it will not be strange to have a robot as controller. However, playing the role of controller presupposes that all the tasks assigned to the controller can be carried out. The answer depends accordingly on an assessment of these tasks. Today, this test will not be passed as the intelligent robot is not fully developed, but it does not seem unlikely that it will be in the future.

Data protection law may join the brave new world in a positive way, and maybe citizens will be protected better by the robot than by the controller of today, or maybe, this could be the risk, data protection will diminish. The future is the future.