AUTORITEIT
PERSOONSGEGEVENS

Speech by Aleid Wolfsen, chairman of the Dutch Data Protection Authority

Symposium 'Data protection as the law of everything (?)'
September 22th, 2022 – Open Universiteit, Heerlen

Thank you!

'Every day will allow you to add something to the pleasure of others, or to diminish something of their pains', dixit Jeremy Bentham. Well said, I thought. His idea of the 'greatest happiness of the greatest number' being a 'measure of good and evil', on the other hand, I find a little less appealing. This can be quite detrimental to minorities. While it may be justified from a democratic point of view, it is not justified from the point of view of the rule of law, of fundamental rights.

This immediately brings us to the healthy tension between the rule of law and democracy; the daily practice of everyone working in the field of data protection and privacy law. Bentham himself was somewhat less concerned about this tension, as he found fundamental rights to be 'simple nonsense, rhetorical nonsense' and even 'nonsense upon stilts'.

I came across Bentham when former advocate general Bobek cited him in the introduction to his opinion on a decision by the Dutch Data Protection Authority.

I presume that the opinion of Bobek also inspired professor Berlee when thinking about an inspiring title for this symposium: 'Data protection as the law of everything (?)'. Where the question mark is even placed in round brackets. This combination of punctuation marks has the appearance of a question mark squared.

But firstly, 'the pleasure' that Bentham talks about. The pleasure that is definitely yours today, Anna. I often think back with fondness to our first meeting, the cups of cappuccino and the very inspiring conversations at the Janskerkhof square in Utrecht. At my eager initiative after reading your excellent dissertation on public records. We then invited you to give a lecture. Which – I can now reveal – was meant to entice you to switch. And our tactic succeeded. Fortunately.

Not much later, I received a call from the president of the executive board of this university. And then from the dean. Both asking whether it would be an idea to develop a standalone Master's degree in Data Protection and Privacy Law. My response to the questions of both the president and the dean was an emphatic 'yes'. And I also informed them that we, the Dutch Data Protection Authority, will certainly want a significant number of the graduates. During a second conversation, it also emerged that they were thinking of asking you to lecture a few hours a week – I repeat: a few hours a week... – on such a course. I thought that was a good idea as well.

The rest is history. You will understand: I am standing here with mixed feelings...

The loss is great, but the pleasure is greater. Because we are very excited that this Master is available now, and especially with this particular professor. This will really advance knowledge of these fundamental rights. And that is absolutely necessary. The digital transition has only just begun. The use of algorithms and AI is growing rapidly. That makes the line between 'How fantastic that this is possible' and 'What is

happening here is very dangerous' thinner by the day. Although AI also brings us many beautiful and good things. Make no mistake about that.

Congratulations to the Open University, congratulations to Professor Berlee.

And now to the theme of this symposium. Is the GDPR in fact the 'law of everything' and is the Dutch Data Protection Authority 'an enforcer of human rights in the digital sphere'?

Professor Bobek begins one of his opinions with a wonderful understatement: 'The GDPR is not a narrow piece of legislation'. Later, he becomes more (let's say) rough, with phrases like: 'The reach of the GDPR is virtually limitless', 'the apparently borderless scope of the GDPR', 'the all-embracing GDPR' and 'the centripetal effects which the protection of personal data has started to exercise on other areas of law and disputes arising therein'. The latter because, in his experience, the GDPR also seems increasingly involved in issues that are fundamentally about something other than personal data.

He stops just short of comparing it to a black hole. He considers the GDPR to be something that figuratively has about the same mass (with a ditto gravitational field), making it increasingly difficult to develop an escape velocity (to stay in that metaphor) high enough to stay away from it.

Which brings him to the almost desperate question: 'Humans are social creatures. Most of our interactions involve the sharing of some sort of information, often at times with other humans. Should any and virtually every exchange of such information be subject to the GDPR?'

Poignant comments and important questions.

In order to answer, I will start with the Lisbon Treaty. This gave the Charter the legal status of a treaty and thereby codified the right to protection of personal data as a new and independent fundamental right. Furthermore, the Union legislature was empowered to enact legislation dealing with the processing of personal data. In order to give substance to this new fundamental right. The GDPR and Directive 2016/680 are based on this legislative power. And the GDPR is certainly 'broader' than the old privacy directive.

Anything that qualifies therefore under the GDPR or Directive 2016/680 is thereby brought within the scope of EU law. I mention the Directive only for completeness, but will otherwise leave it out today.

Not only does the entire Charter apply to everything that falls within the scope of EU law, the so-called general principles of EU law also apply. Such as the principles of proportionality, legitimate expectations, equality, defence, transparency and legal certainty, as well as the prohibition on arbitrariness. And all of this should of course always be assessed in the light of the core values of the EU: respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights (all human rights), including the rights of persons belonging to minorities.

The Lisbon Treaty therefore was a 'big' decision and a decision with big implications.

As a result, not 'any' and not 'every' information has been brought within the scope of EU law, but it is as soon as that information can be qualified as 'personal data' and the 'processing' thereof takes place 'by automated means' or ' forms part of a filing system or are intended to form part of a filing system'. There are two exceptions: Purely personal or household activities and processing by government agencies to

ostensibly protect national security. And, of course, there are also various Regulations and Directives that further refine the general regime of the GDPR, thus also providing substance to this new fundamental right. I will speak later about infringements.

Thus far, I imagine that I haven't told you much that is new to you. But the GDPR immediately starts in the plural: It 'protects the fundamental rights and freedoms' of 'natural persons' and – naturally – 'in particular their right to the protection of personal data'. But what other 'rights and freedoms'?

Obviously the fundamental right to privacy, the right to respect of one's private life. A core fundamental right that codifies civil liberty and is one of the core moral values of our legal order. This fundamental right should obviously be interpreted broadly: in dubio pro libertate.

After all, it concerns the autonomy and self-determination of citizens and their identity. Who you are, what you do and how you wish to represent yourself. Citizens are unique as human beings, they decide for themselves what they consider a worthwhile and meaningful life and who gets to know what about them.

There are many facets to private life: These include thoughts, conscience, expressions and communications, faith and beliefs, family life, freedom of movement, the home, medical information and bodily integrity, pregnancy and its termination, sexual orientation, trade union activities, payment behaviour, habits, memberships and not forgetting... life itself and the right to decide when it ends. And an extended facet in the form of the right to the free enjoyment of property, including intellectual property.

Facets that are sometimes codified as independent fundamental rights and sometimes not. Codifying one or more of the aforementioned aspects of private life as an independent fundamental right helps to clarify and objectify such aspects of private life. And therefore, in creating legal certainty. But this obviously hardly changes the scope of the core fundamental right itself – privacy, private life and freedom. After all, freedom is not limited to one such aspect.

In the Netherlands, by the way, the constitutional legislature once started codifying only some aspects of this freedom and thus not this freedom itself. It was not until 1983 that the right to privacy, freedom itself, was codified. This was a revolution of Copernican proportions for (what we call) the 'ordinary' legislators. Since then, in all the aspects mentioned, including personal data, parliament itself decides whether an interference with that freedom is allowed or not allowed.

Although that no longer had any effect on the level of protection as such. In fact, parliament had codified this fundamental right long before this by ratifying the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Textbooks still sometimes ask what the 'rather unclear concept of privacy' actually is 'after deducting' the aspects of that freedom that are already codified. But, obviously, it is the exact opposite. The question is always: What does codifying individual aspects of private life add?

Digitalisation has the effect of digitising a lot of information about people – including all the aspects of private life mentioned above. People are datafied. Digitalisation and datafication obviously cannot and should not independently lead to any curtailment of citizens' freedoms. The freedom to continue to have the ability to determine and dispose of – in a nutshell – that data, that personal data. In other words: informational self-determination has also become a self-evident part of the right to privacy partly as a result of this digitalisation and datafication. Also as a kind of extended aspect of privacy. Even when that

data is neutral in nature. After all, if this were not the case, the right to privacy in the digital world would slowly but surely become largely illusory.

So what does a new and independent fundamental right to personal data protection add to that core fundamental right to privacy?

Because the codification of this aspect also certainly leads in itself to some form of reciprocity. Indeed, the right to privacy partly protects the processing of personal data, and the right to the protection of personal data partly protects privacy. In other words: It is, in any case, closely related to the right to respect for private life. This can sometimes lead to confusion. But not to anyone who is slightly more than averagely versed in the law of fundamental rights. After all, this reciprocity is no different from the codification of various other aspects of private life, such as the secrecy of communications or the inviolability of the home.

The 'broader' answer to the barely overestimated importance of the codification of the right to dataprotection is actually surprisingly simple: In the digital world, the right to the protection of personal data protects much more than just the core moral value of privacy. It also protects other core moral values of our legal order: Equality, democracy and solidarity. Core values that are also protected in constitutions by individual fundamental rights: 'Equality' in the non-discrimination provisions, 'democracy' in the political participation rights and 'solidarity' in the fundamental social rights.

In the same way as a constitution always codifies safeguards – partly also in independent fundamental rights – in order to accomplish this, such as an independent judiciary and due process with good access to the legal system.

These core moral values of society may also be compromised when processing personal data. Those familiar with the investigation into Facebook and Cambridge Analytica will be aware of the dangers of being able to freely exercise political participation rights. You can read about the threats to non-discrimination provisions in our investigations into the Dutch Tax and Customs Administration. The Dutch Central Bank and the Financial Markets Authority have recently issued strong warnings about the threats that digitalisation poses to solidarity in our society. As well as the fact that the right to an effective remedy may be jeopardised by the use of non-transparent algorithms and AI.

Digitalisation and automation become datafication and combination, algorithmisation, innovation and transmission, and can degenerate into marginalisation, manipulation, discrimination and worse. The core moral values of our legal order must therefore be respected and upheld, especially in this digital world.

Consider for a moment the increasingly thin line between 'How fantastic that this is possible' and 'What is happening here is very dangerous'. Then everyone's possible question mark about this new and independent fundamental right will turn into an exclamation mark. Also read the legislator's heartfelt cry in the GDPR: 'Natural persons should have control of their own personal data'. Regardless of whether that data is sensitive or not. And this, in turn, explains why precisely this fundamental right has been elaborated in such detail and objectified in the GDPR, including through concepts such as 'personal data', 'processing' and 'automated means'.

Fundamental rights are, in principle, absolute. With any fundamental right, the starting point for thinking of the constituent is: 'we, the people'. Only citizens themselves can enable or permit interferences by pure expressions of will. But, at the time of codification, almost all constitutional legislatures create the option

for representatives of the people, on behalf of those citizens, in their capacity as 'ordinary' legislators to also enable interferences by means of secondary law. This is in order to make 'living together' possible.

The same applies to the EU constitutional legislature. This can be found in Article 52 of the Charter: subject to strict conditions. A core provision that applies to all infringements of all fundamental rights. The entire GDPR – and all other regulations, directives, laws transposing directives and national legislation – must be read, interpreted and applied through that 'lens'.

This means, shortly and to the point, that: all processing must be traceable to pure expressions of will by the citizens concerned themselves (by consent or contract) or to pure expressions of will by their representatives, parliament (the law).

'Your right to swing your fist ends at the tip of my nose', an American judge once said evocatively. Translated to privacy or data protection this means: Your freedom to walk throughout the city ends at my closed front door and your freedom to process information ends at my personal data. And that 'tip of my nose', that 'front door' and those 'personal data' can only be 'bypassed' on the basis of such a pure expression of will. Citizens can express that will verbally, but when it comes to involuntary interferences: No digital code, without a paper code.

The core constitutional concepts for being able to set 'limitations' are: 'Provided for by law', 'respect the essence of the fundamental rights' and 'observe the principle of proportionality'.

'Law' refers to the aforementioned pure expression of will by the democratic legitimacy, i.e. by parliament. And the respect-the-essence-guarantee is also clear.

Then we have the 'principle of proportionality': the connection, the scales, between the core of the rule of law (in principle, the absolute fundamental rights) and democracy (which can allow infringements by 'simple' majorities). The principle by which the constitutional legislature (primary law of 'we, the people' as a whole) compels the 'ordinary' legislature (secondary law) to exercise caution and care. But which also protects minorities from 'ordinary' democratic majorities. At its core: codified decent manners and civility.

And then the most difficult key words/concepts of the principle of proportionality: 'Strictly necessary'/'proportional' (the reconciliation of an objective of general interest with the fundamental rights affected by the measure).

For starters, this means, among other things: 'Clear and precise rules', 'foreseeability', 'minimum safeguards', 'legally binding under domestic law' and 'substantive and procedural safeguards'. Ending with the familiar three-pronged 'appropriateness', 'the principle of subsidiarity', and finally 'proportionality stricto sensu'. This way, we limit breaches to what is really strictly necessary.

'To observe the principle of proportionality' is conceptually simple, but in practice notoriously difficult. And it forces everyone working in data protection land to be able to 'play tennis' with the entire Charter, with all the general principles of EU-law and with the core values of the EU, both backhand and forehand.

This is perhaps extra difficult in the Netherlands, since the Dutch Constitution does not have this constitutional requirement. Its existence in the Netherlands was constitutionally short-lived: it was only

incorporated in the State Regulation of 1798. This is difficult to understand from a rule-of-law perspective, but is a fact. And the respect-the-essence-guarantee is also not a part of the Dutch Constitution.

But a violation of this EU-constitutional principle of proportionality leads to unlawful legislation. Even though such a law was created democratically. Such laws, or parts thereof, must be disregarded by any government agency, by us and by the courts.

Because the Data Protection Authorities have always operated within the scope of EU law, we have never known otherwise. But parliamentarians, administrators, civil servants and judges who have at some point been 'overtaken' by EU law or are required to switch between different 'spheres of operation' at regular intervals should realise during such a 'switching' within the scope of EU law, the Dutch prohibition of a judicial review changes into a judicial review requirement. This requires the necessary rule-of-law nimbleness of mind.

During our legislative advice, the proportionality test is often at the heart of our rule-of-law review. Many specific complaints often relate to this principle as well. And thus, with processing operations based on legislation, there is always a double proportionality review: first on the legislation itself in a general sense and then on the processing in the specific case.

I hope my comparison with tennis inspires you a little bit. And also this digression on the principle of proportionality. Indeed, it touches on the key questions for today. Because it is precisely in the application of this principle, in the implementation of this constitutional duty, that everything must – said simply – be weighed against everything.

The interests that the legislator wants to 'promote' to legal interests and the associated rights and possibly duties weighed against all legal interests already codified in fundamental rights. As I noted earlier: protection of personal data now falls entirely within the scope of EU law. And the entire Charter applies to it, including the general principles of Union law and the core values of the EU already mentioned.

And data controllers faced with enforcement activities can of course also invoke the protective effect of the Charter – including the rights in the chapter on 'Justice' and the general principles of law.

Time for some reassurance. We have established that legislation or a decision to carry out specific processing cannot and should not lead to an outcome contrary to the principle of proportionality. But apart from this, the outcome in specific cases of data processing may also not lead to an unreasonable or unjust outcome.

The Charter has even explicitly codified this in Article 8 and it is reiterated in Article 5 of the GDPR. By means of: 'fair', and in the Netherlands, 'redelijkheid en billijkheid'. In German: Treu und Glauben. 'Bona fides' in Roman law. This always plays a complementary or limiting role in all law. Even if there is consent, even if something is necessary for the performance of a contract, even if there is a law and even if it is not theoretically disproportionate, all parties must always behave mutually in accordance with the additional and limiting requirements of this fairness when exercising rights or fulfilling obligations.

After all, justice is the goal of law and every piece of legislation. Something is not just because it is incorporated in a law, but instead it is incorporated in the law because it is just. Laws codify ethics, morality, good and evil in general, the 'big goodness'. And if this then turns out to be unjust in a specific

case, it should be corrected by fairness, by 'the small goodness', as the 20th century French philosopher Emmanuel Levinas once aptly put it. That is also what 'we, the people' want.

Many citizens obviously greatly enjoy all the beautiful and good things that the digital revolution brings us. There is no doubt about that. But citizens also want to remain masters of their own private domain in the digital world. Even there, they want to keep a grip on their lives, continue to make their own choices and decide for themselves whether they may be guided, selected, followed, spied on or judged in the process.

And decide for themselves who they want to allow into that private domain and who is allowed to process what intimate information and for what purpose. Free will should not be eroded there either. It is precisely here that the 'du glaubst zu schieben, aber du wirst geschoben' from Goethe's Faust is a permanent danger.

And it is precisely in this often invisible world, too, that the core moral values of our legal system must not be violated. Citizens do not want to be spied on, discriminated against or excluded. And such activities can often take place 'invisibly', at the touch of a button or a line in an algorithm. Being viewed or 'processed' in advance as a suspect is also taboo.

The use of algorithms and AI adds urgency to all this, as citizens are often unaware of this. This often makes the possibility of private enforcement effectively illusory. Whereas 'to be free to choose, and not to be chosen for, is an inalienable right in what makes human beings human', as the 20th century British philosopher Isaiah Berlin so astutely wrote.

The serious and grave dangers also seem to me to be precisely the reason why this fundamental right was not codified 'bare', but instead the choice was made to codify it in the well-known three-pronged approach: 1. The fundamental right itself, 2. the restriction options, and 3. an independent supervisory authority, unlike all other fundamental rights, as an 'essential component' of the fundamental rights themselves.

The digital revolution has already led to an awful lot of convenience, enjoyment, comfort, better care and services, and many, many innovations. Our well-being and prosperity have really improved a lot as a result. But the same revolution, when processing personal data, can therefore also seriously harm the core moral values of our legal order: freedom, equality, democracy, solidarity and fair justice.

And the overall moral foundation of those core values, human dignity itself, can also be harmed. The GDPR – and any EU and national legislation that complements and/or elaborates on the GDPR – are means of facilitating that transition on the one hand and preventing or ending that harm on the other.

I have reached the conclusion of my lecture. Processing personal data activates the protective effect of the GDPR and thus the entire Charter, all general principles of law and the core values of the EU. The stringency of the European Court of Justice (ECJ) in this respect has now rendered a complementary effect of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) unnecessary. We have therefore archived this European Convention, with much thanks for services rendered.

As a supervisory authority, we have an advisory role to begin with: after all, prevention is better than cure. We warn when things are in danger of going wrong. We therefore also exercise preventive oversight of national legislators. But we also have an enforcement role when boundaries are crossed. In which role we

can also impose fines where necessary and appropriate. In order to restore legal relationships, remove unlawfully enjoyed benefits (after all, violating fundamental rights should never be rewarding) and provide additional penalties where necessary and appropriate. Which can and should never lead to a disproportionate or unreasonable outcome. This is how we monitor that thin line between 'fantastic' and 'very dangerous'.

But then again: The GDPR as the law of everything? The right to protection of personal data as an all-overriding fundamental super right? The Data Protection Authorities as enforcers/supervisors of human rights in the digital sphere?

Please do your own judging and answering.

Indeed, I myself would not immediately know which core moral values of the EU or national legal system and which fundamental rights or general principles of law we would then not respect or uphold if the violation of any of those values, fundamental rights or principles in the digital rule of law, in the digital legal order leads to unlawful processing or if processing leads to the violation of any of those values, fundamental rights or principles.

Only then can we prevent erosion of those core values, fundamental rights and legal principles in the digital world. Not even a constitutional court can add anything more to that.

The Master of Data Protection and Privacy Law is not starting a day too early. I predict a big future for it. Under the inspired leadership of Professor Berlee. Get to work!