ICT & SOCIETY

Algemene Verordening Gegevensbescherming in study associations

Nienke Wessel s4598350 - Radboud University

This article was written for the Radboud University course *ICT & Society*.

Introduction

As a member of the board of a study association at the faculty of my Dutch university, I have heard quite a bit about a recent change in privacy laws, which supposedly has great influence on the way associations are allowed to handle personal details of their members. As can be imagined, as soon as associations heard about the Algemene Verordening Gegevensbescherming (AVG) and that they were supposed to act accordingly, all hell broke loose and everyone started to panic: what were we supposed to do and how are we supposed to do that? The official starting date of this new law is May 25th 2018, so most associations are working hard in achieving the desired changes in accordance with this law. Associations are writing 'privacyverklaringen' (privacy policies) and are looking at alternative ways to save the information of their members on a computer. It might have become clear that this is concerned a matter of both privacy and ICT. While it is easy to make that assumption, it is good to think of how exactly these two things are part of the discussion. The goal of this paper is to find out how the general concepts of ICT and privacy relate to this new law, specifically to what the AVG entails for study associations.

The paper is divided into two parts. The first part is concerned with the ways in which the AVG interacts with computers and ICT. The second part is concerned with how the new law interacts with concepts of privacy. I analyze the case of the AVG by applying several definitions and theories about ICT and society and about privacy to it. There is often no consensus on the 'correct' definition of certain terms mentioned above, so the goal of this paper is not to provide the readers with the best definition or give a conclusive idea of how the case interacts with whatnot. Instead, I try to give an idea of how one can look at issues like these in different ways.

Algemene Verordening Gegevensbescherming

Before we start with the aforementioned parts, we first need to know what the AGV entails in more detail. This section is dedicated to giving an overview of the law and relevant concepts.

The law is not just a Dutch law, but a law made by the European Union. It came into existance to replace all kinds of different national laws concerning privacy. In The Netherlands, the law replaces the Wet bescherming persoonsgegevens (Wbp). All those different laws were based on the same guidelines, published by the EU in 1995, but these guidelines were made when the internet was new and far from what it is now. That is why these guidelines have been revised.

There are several things that change for Dutch people, both for the people as clients, as well as for companies and associations. The most important changes concerning associations are:

- Organizations need to be able to prove that they have permission from the person whose data they are working with. People also need to be able to revoke their permission just as easily as they gave it.
- People can ask for their data to be removed from the databases of third parties. In the previous law, people could already ask the organization to remove the data it has on them, but now the organization is also obligated to make sure the data of that person is removed from other organizations' databases, if they gave it to that organization.
- Organizations are responsible for protecting the data they use. That means they have to have sufficient protection for the system they use to keep the data. [1]

In the study associations of Nijmegen, the first point has mainly taken shape in the form of privacy policies. These are documents that state exactly what is done with each of the different types of personal data. For example, if an association keeps track of a home address, the privacy policy needs to state why (e.g. to send the association tabloid to the members). The second point has not taken a prominent role in the discussion. As for the third part, most associations are looking for better and saver places to keep databases.

Now that it is clear what the new law entails, we can move onto the first part of this article.

Part I: ICT and AVG

Even though the law is not restricted to ICT (or even assumes that an organization is using ICT for the processing or preserving of data), most people will automatically assume it is about computers, the internet, websites, servers, the cloud, etc. and how they handle the data (even though the law is just as well meant for information on paper).

Our definition of ICT (information and communication technology) is the following:

The advanced technologies for information processing and communication designed to encourage information and communication processes.

Before we apply (philsophical) theories to this case, let's take a look at how ICT and AVG interact intuitively, from the point of view of a study association.

Intuition

Let's assume we are a study association and we have some form of personal data of our members (e.g. a name or a birthday). We have somewhere between 100-500 members, so keeping all this data on paper is not very handy. That is why we have a

[1] This was already in the Wbp, but is in the AVG in a more elabarate way. Also, because of the AGV, people are reconsidering whether they were doing this part right, which means it got a more prominent position in the whole discussion and commotion surrounding the AVG than one would expect on the fact that most of it was already in the Wbp.

database where we keep all of the data. One of our more tech savvy members made it, so we are not sure entirely how it works, but our secretary can work with it, so it is fine. Maybe, our database is on one or two of the computers of our association. Or maybe our database is on some server or maybe even in the cloud. We also have a website where members have a profile. This profile contains basic information like their name and some achievements for the association. The profile is closed of for people that are not logged in. Besides this, the website also contains photos of activities we organized. However, you also need to be logged in to access it.

Looking at this association, we can point out several 'things' that are related to both ICT and AVG: we have data on the members that is part of the data AVG is about. This data is saved somewhere, in some database on some piece of technology. There is also a website where we display (parts of) this information.

So concerning (study) associations, the most important things are concerned with what types of data are collected and where they are kept. Not many study associations will keep those kinds of data on paper somewhere. Nowadays, they will probably put it on some form of automated technology.

Now we have an idea of what roll ICT plays in this case intuitively, we can zoom out a bit and take a more philosophical look at how ICT plays a part in this case. We do this by applying several philosophical theories about ICT and society in general and then discuss how these fit with the case. These theories are Instrumentalism, Technological determinism and the Mediation Theory.

Instrumentalism

In the theory of instrumentalism, technology is a collection of instruments that people use to achieve their goals. Instruments can be interpreted as objects only (such as computers or software), but also in a more broad way, as in skills or organizations. The theory comes in two types; one of them is that the instrument in its nature has positive or negative consequences (is ambivalent), the other that it is not in the nature of the instrument, but in what one does with it (is neutral).

When applying this theory, we see the website, the database, etc. as an instrument in achieving what we want: an easy way to keep track of the information of our members, an easy way for members to look at photos, etc. When we assume that technology is ambivalent, we look for the positive and negative consequences in these technologies. For example, one could say that a positive consequence of a database is that the information is in an easy to traverse structure. Or that a negative consequence of a website is that personal information someone might not want to share is easily found. When assuming that technology is neutral, we say that a database is not positive or negative on its own, but rather that one can do bad things with it. For example, a person could hack the database and in this way collect information that they are not supposed to have access to. This would be considered 'bad', but not in a way that the badness is inherent to the technology itself. In a way of 'guns do not kill people, people kill people'. We see that both types of instrumentalism are applicable to our case.

However, for both types, one can also argue that the theories do not fit as well as one would hope. For example, according to the ambivalent theory, it would be considered a negative consequence of the technology if a hacker hacked the

database and put all gathered information somewhere on the internet. This begs the philosophical question of whether the negative consequence (the spreading of information one wanted to keep private) really is inherent to the object (a database). Something similar could also have happened with a paper database. Would we blame the file cabinet then? Similarly, just as people argue that 'guns do not kill people, people kill people' is flawed, one can argue that the neutral technology theory is flawed.

A more general point of criticism that is generally mentioned is that technologies often have unintended consequences, while the instrumentalism theory just sees technology as a way to achieve goals. This underplays the role of those unintended consequences. Think of the use of social media, and the consequences that follow from it. See for example [1] for a discussion on how Google has unintended consequences.

(Technological) determinism

This theory assumes that the way in which technology and society interact, is that technology causes changes in society. For example, we can say that technology made that a new law concerning privacy was developed, as the old law was seen as not sufficient anymore. We can also take a look at how technological developments changed the way (study) associations operate: the emergence of cheap and easy ways to store data online has changed the way associations do their administration, from paper to computer. Also, the ease with which we can now put thousands of photos online (of for example activities of our association) has made it almost all organizations do so nowadays. When looking at the bigger picture, we see that now that it is possible to collect huge amounts of data on people, organizations do so and use it to change the way they work.

However, it is difficult to apply this theory directly to both associations and the AVG. The difficulty lies in that it talks about big, long term patterns of change in technology and society. That makes it hard to apply it small-scale on short term things. This leads to another difficulty of the theory: not every piece of technology has led to (significant) societal changes. Does this make that piece any less a piece of technology?

Mediation theory

In this theory, technologies are mediators of human-world relations [2]. For example, we use technology to connect with other people, or our work and we change relationships with it. You also interact with the world through technology. For example, when looking at a meter, you learn new information about the world.

In our case, this means the website provides us with a way to look at photos and relive memories. For the database, the database helps us learn about the people in the database.

One point of criticism of the theory is that it is only about how humans interact with the world trough technology, the changes technology does to the world are always interpreted as a consequence of humans interacting with the world through this technology. For example, a computer failing and thus resulting in the flooding of a river, is interpreted as a person interacting with the world. One can wonder however, what person would be interacting and if they are really interacting in any way.

Conclusion part I

The different technologies each shed a different light on the case. While the instrumentalism technology feels natural at first, some problems arise. The determinism technology focuses more on long term patterns, than on how a specific piece of technology is interacting with society at any given moment. The mediation theory seems best fit, but is not perfect either.

Now that we have a better idea of how the casus relates to society, we will look at a specific part of society, namely privacy, in the second part of this article.

Part II: privacy and AVG

In order to answer the question of how privacy and AVG interact, we need a definition of privacy. We know that most associations are setting up documents called 'privacy policies', but is the word 'privacy' really warranted here? Before we move on to that discussion, we try to work with our intuitive sense of privacy and try to determine what level of privacy we are talking about. Often, the following levels of privacy are distinguished:

- Personal level: this is about privacy in person to person interaction. For example, when you share intimate thoughts with a friend, but you do not want them to end up with anyone else, your privacy can be violated if they are shared.
- Institutional level: this is about privacy in citizen-government interactions. This is not about you on a personal level, but the part of you that interacts with the government, the citizen in you.
- Commercial level: this is about privacy in client-company interactions. Questions like "is it okay for this company to make money with my data?" come into play here.

Returning to our case, we see that it is not that obvious as to which level our case belongs, as none of the cases seems to fit perfectly. The personal level is not perfect here, but is not as far-fetched as it may seem. When looking at a photo of someone (and that someone would rather have you did not, but it was on the website of your shared association, so you could) we can say privacy at a personal level is violated. Also, study associations are usually small and everyone knows each other. That means someone in the board who knows a member might violate the privacy of that member by looking in the database and finding some information that that member rather would have not to be known by this board member. So the personal level plays a role here, but it is not the main role in our case.

The commercial level is somewhat relevant. Even though associations do not strive for profit (so also not for profit by using the data), the relationship between a member and the association is in many ways similar of that between a company and a client. Members usually pay the association to become a member and it is clearly a private sector thing. Also, the AVG puts commercial organizations and associations (as well as foundations and other non-profit organizations) in the same group. So one could argue that the main role in our play is taken by the commercial level. However, it seems unsatisfactory, considering that there is no goal for profit here.

One could also argue that the institutional level might be the most important level here, even though there is no real interaction with the government (as associations are not run by the government). What makes the level fitting here, is that in both associations and the government there is no goal of making profit and that in both cases the members/citizens choose who makes the decisions in the association/government (can you imagine that customers could choose who runs the company).

In short, none of the 'traditional' levels of privacy is satisfactory here. The institutional level seems good if we ignore the definition (i.e. that it has to do with the government) and just look at the organization type we are talking about. The commercial level is also okay, but neither are perfect.

Now we move on to our different definitions of privacy. As it turns out, it is not easy to provide a good definition of privacy. We discuss several definitions here and see how well each of them fits our case. The definitions we use here are the same as discussed in [3].

Nonintrusion theory of privacy

In this theory, privacy is described as being let alone or being free from intrusion. This definition of privacy is based on the idea of physical privacy. One should note that these definitions come from 1890 ([4]) and are therefore harder to apply to nowadays' cases of privacy. When applying this theory to our case, we find that privacy policies have little to do with privacy as they say nothing about the right of a member to be left alone or being free from (physical) intrusion.

Seclusion theory of privacy

Just like the nonintrusion theory, the seclusion theory has a rather physical idea of privacy. Here, privacy is identified with being alone or being inaccessible to others [5]. In this definition of privacy¸ a privacy policy for an association is not any more meaningful than in the nonintrusion policy.

Both policies are concerned with physical access to an individual, where the privacy policies we are talking about have little to do with physical access. This is probably because the intuitive definition of privacy has shifted a lot over the years with the growth of the internet and technological developments. That is why we now move on to privacy definitions that find that privacy is about information in some way, and not about physical access.

Control theory

In this theory, one enjoys perfect privacy if and only if one has control over information about oneself. This definition is perhaps more in line with what you would expect to be a definition for privacy. It is also makes the name 'privacy policy' somewhat more sensible. For example, most privacy statements say that you can decide whether you want to be on pictures and what you have to do to get a picture removed, thus giving you more control over that information. Also, by accepting the privacy statement of the association, you basically choose to share the information mentioned in it with your association, thus giving you more privacy according to this definition.

One could wonder, however, if someone that chooses to share anything and everything with the whole world really has privacy, as this theory states they do.

Limitation theory

According to this theory, privacy is when access to information about that person is limited and restricted in certain contexts. In this view, a privacy policy restricts the association in what it can do with the information about a person and what information it can have about that person and therefore increments the privacy of that individual.

However, this theory downplays the role of someone's choice here. In for example the case of pictures on the website, this theory would state that someone has more privacy if he asks for this pictures to be removed, because it means the information about that person is more restricted when there are no photos than if there are photos. However, one could argue from an intuitive idea of privacy that there is also privacy if the person chooses to let the photos be there.

The Restricted Access/Limited Control Theory

In this theory, one has privacy in a situation with regard to others if in that situation the individual is protected from intrusion, interference and information access by others. Also, the theory distinguishes between normatively private situations and naturally private situations. In the latter case, one has privacy by natural means. Think of when one is camping in the woods. In normatively private situations, norms and laws have been established to protect the privacy. This is not the case with camping; you can easily lose your privacy there and it would not be considered unethical or immoral to let someone lose their privacy there. In normative privacy it would be considered so. For example, you can violate someones privacy by entering their house without permission.

Even though this theory is different from the limitation theory, applying it to our case yields similar results. Note that it is all about normative privacy in our case, as we are talking about a law which tries to secure privacy. There are no natural boundaries in our case, except for perhaps lacking internet connection.

Conclusion part II

Different theories of privacy say different things about whether the 'privacy' in 'privacy statement' is warranted. Older theories that are more concerned with physical access do not agree with a privacy statement, but probably also not with our intuitive sense of privacy nowadays. The theories concerning information flows do agree with the concept of a privacy policy, but in different ways and put emphasis on different things.

Conclusion

It seems that even on a very specific case, it is interesting to apply several philosophical theories and theories of privacy. It sheds a different light on the case and challenges our intuitive definitions of concepts.

References

1. Carr, N.: Is google making us stupid? The Atlantic
2. Verbeek, P.: Cover story: Beyond interaction: a short introduction to mediation theory. Interactions **22**, 26–31 (2015)
3. Tavani, H.T.: Philosophical theories of privacy: implications for an adequate online privacy policy. Metaphilosophy **38** (2007)
4. Warren, S., Brandeis, L.: The right to privacy. Harvard Law Review **14**, 193–220 (1890)
5. Gavison, R.: Privacy and the limits of the law. Yale Law Journal **89**, 421–471 (1980)