Revista catalana de dret públic #64

www.rcdp.cat

THE LIMITS OF PRIVACY BY DESIGN*

Antoni Roig Batalla**

Abstract

Privacy by design (PbD), an approach to systems engineering included in the European Union's General Data Protection Regulation, now forms part of the EU's legal safeguards. This article examines the scope of this reliance on privacy-enhancing technologies (PETs). More specifically, it assesses their limits and the problems with their real-world application. One aspect worthy of particular consideration is the lack of co-ordination between our legal and our technology communities: we shall be providing examples of supposedly privacy-enhancing technologies that are ineffective in practice, as well as those that are unlawful and, finally, those that do not take account of the legal concept of privacy in the design of the protection they afford. The article concludes by suggesting some possible ways of remedying this situation and of leveraging the full co-regulatory potential of privacy-enhancing technologies.

Keywords: privacy by design; PbD; privacy-enhancing technologies; PETs; co-regulation; law and technology.

LÍMITS DEL PRINCIPI DE PRIVADESA PEL DISSENY

Resum

El principi de privadesa pel disseny, incorporat finalment al Reglament general de protecció de dades, forma part ara de les garanties jurídiques. Analitzem, en aquest treball, l'abast d'aquesta crida a la tecnologia garant. Concretament, ens interessa valorar els seus límits o problemes d'aplicació. Un aspecte que mereixerà especial atenció és la falta de coordinació entre les comunitats jurídiques i tècniques, i les seves conseqüències. Així, descriurem casos d'ús de tecnologies pretesament garants que a la pràctica no ho són; també veurem casos de tecnologia garant contrària a dret, i, finalment, mencionarem casos d'eines que no tenen en compte el concepte jurídic de privadesa a l'hora de dissenyar-ne la protecció. Dedicarem la part final del treball a suggerir possibles vies per redreçar la situació i treure tot el potencial corregulador de les eines tècniques garants.

Paraules clau: privadesa pel disseny; eines garants de la privadesa; corregulació; dret i tecnologia.

* This article is a translation of an original one in Catalan.

** Antoni Roig Batalla, full professor of Constitutional Law, Department of Political Science and Public Law, Universitat Autònoma de Barcelona. Facultat de Dret, edifici B2, c. de la Vall Moronta, s/n, 08193 Bellaterra (Cerdanyola del Vallès). antoni.roig@uab.cat. 0000-0002-4760-9361.

Article received 02.09.2021. Blind review: 04.10.2021 and 06.10.2021. Final version accepted: 06.10.2021.

Recommended citation: Roig Batalla, Antoni. (2022). The limits of privacy by design. *Revista Catalana de Dret Públic*, *64*, 174–176. https://doi.org/10.2436/rcdp.i64.2022.3717

Contents

1 Relying on technology: privacy by design

If we take a look at Article 18.4 of the Spanish Constitution, we can gain some idea of the traditional relationship between law and technology: "The law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights."

This indicates how technology is regarded as something that, in itself or due to the risk it poses, calls for legal guarantees to ensure that it does not negatively impact fundamental human rights. Thus it is that technology entails new scenarios requiring protection by means of specific legal regulation. Law is the guarantor, and technology is the risk it protects us against.

However, privacy by design (PbD) would appear to represent a break with this traditional view of technology:

- Technology is now more than simply a risk.
- Technology could even be a part of the solution or a guarantor of fundamental rights.
- The law now relies upon technology to help defend fundamental rights.

This legal reliance upon technological collaboration is not co-regulation in the strict sense of the term. If it were, law would lose its monopoly on regulation in favour of technological regulation. Whilst it is true that legal principles and the right to privacy need to be respected by technological regulation, some degree of complementary or executive regulatory powers should be possible. Such a move would entail authorisation of an area of self-regulation that would respect legal principles and fundamental rights. But this is not what is happening. Lawmakers have taken this step for far more modest reasons: they understand the limits of regulation by principle and seek to take advantage of the protection that could be afforded by privacy-enhancing technologies (PETs). So, this is not a revolutionary shift, but rather progress towards greater effectiveness in traditional regulation (Schartum, 2016). More recently, attempts have been made to apply PbD to new and changing fields such as the Internet of Things (Tamò-Larrieux, 2018).

It needs to be borne in mind that this rapprochement with technology has not entailed getting any closer to the tech community, which, since the late 1990s and even more clearly since the start of the current century, has sought to infuse technology with ethics, using designs that foster privacy. This can be seen, for example, by its contributions to the European Union Agency for Cybersecurity (ENISA, 2014, 2016, 2019, 2021). The legal community's interest in PETs therefore predates the General Data Protection Regulation (GDPR), as discussed, for example, in Schaar (2010) and Rubinstein (2012). Still, it is with the provisions of Article 25 GDPR that PbD has taken on its current importance.[1] So it is that PbD forms part of a new stage in data protection, one that involves risk assessment and proactive responsibility (Bygrave, 2017, 2020). Nevertheless, this express inclusion in the GDPR has not resulted in any real dialogue with the tech community. As we shall see, the consequences of this lack of dialogue between it and the legal community have impacted the effectiveness of PETs.

This article seeks to show the limits of this fascinating regulatory reform and suggest what we believe could be some ways of improving it (along the lines of Klitou, 2014). Said limits to be examined below are:

- The lack of any assessment as to the need or otherwise for a PET in a given situation.
- The use of ineffective PETs.
- The lack of clear criteria for choosing between different PETs.
- The existence of PET solutions that are, in fact, unlawful.

1 Art. 25 GDPR: Data protection by design and by default

> 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

– The use by PETs of a non-legal concept of privacy.

– The absence of privacy metrics to assess whether PETs really do enhance privacy and (if they do) to what extent, and whether they continue to do so over the course of time.

– The lack of any institutional platform for guaranteeing dialogue and updating guarantees.

2 Are PETs always needed?

Privacy by design can add guarantees that complement traditional legal protection. Even so, these may not always be necessary. Imagine that traditional regulation provides a suitable level of protection: in this case, the addition of a technological guarantee not only fails to improve on said level of protection, but could also be counterproductive. In reality, all technology, including PETs, can contain an element of risk in terms of privacy protection. This is why it only makes sense to incorporate PETs when the pros outweigh the cons. And, when there is no need for complementary protection, the cons will always outweigh the pros.

That's why, before we even consider the need for PETs, the first thing we need to decide is whether adequate protection can be provided using traditional regulation, be this with guiding principles or using procedural regulations. Whilst it may not always be the case, sometimes proper organisational guarantees may suffice. One case in which traditional regulation, with its principles, laws and procedures, does not – in our opinion – require complementary PETs (or, if it does, only in a few minor cases), is that of body scanners used for security purposes in airports.[2] The European Union has banned one such scanner type (that using ionising radiation) for health reasons.[3] No other kinds of scanners are limited by this ban, even though they must follow some principles and procedures that we believe are enough to ensure privacy, without the need for complementary PETs.

The rules in this instance contemplate as a general principle the option of choosing between a body scanner or other more traditional methods: passengers must be given the alternative of a frisk/pat-down, with or without the use of sniffer dogs.[4] This means that the use of a scanner is not obligatory but optional, and another search option must be offered if requested, with no financial impact or delays making the choice impracticable. Another principle, this time associated with data retention, is the ban on storing or printing images for any longer than strictly necessary for analysis purposes and never after passengers are cleared.[5] So, here we can see the application of data protection principles, such as data minimisation and purpose limitation.[6]

Provisions on the effective implementation of these and other data protection-related principles are also provided. Thus, the person reviewing the image must be located in a separate place from which they cannot see the passenger.[7] This measure is designed to protect the passenger's privacy, such that the reviewer only has

2 Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security (OJ L 299, 14.11.2015), and subsequent amendments thereto, the latest by means of Commission Implementing Regulation (EU) 2021/255 of 18 February 2021.

3 Point. 4.1.1.2.*e* of the aforementioned Commission Implementing Regulation (EU) 2015/1998.

4 Point 4.1.1.10:

> Passengers shall be entitled to opt out from a security scanner. In this case the passenger shall be screened by an alternative screening method including at least a hand search […]. Before being screened by a security scanner, the passenger shall be informed of the technology used, the conditions associated to its use and the possibility to opt out from a security scanner.

5 Art. 4.1.1.10.*a*:

> Security scanners shall not store, retain, copy, print or retrieve images. However, any image generated during the screening can be kept for the time needed for the human reviewer to analyse it and shall be deleted as soon as the passenger is cleared. Any unauthorised access and use of the image is prohibited and shall be prevented.

6 The principle of data minimisation is included in Article 5 GDPR: "1. Personal data shall be: […] c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')." Article 5 also includes the principle of purpose limitation: "1. Personal data shall be: […] b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."

7 Art. 4.1.1.10.*b*: "The human reviewer analysing the image shall be in a separate location so that he/she cannot see the screened passenger."

access to the information on the monitor screen. This protects all the passenger's information not required for security purposes and also prevents any possible discrimination or profiling. Similarly, the reviewer should also not be able to link the passenger's image with any other identificatory information, like their name, passport number, etc.[8] This adds to the notion that only a security screening is being carried out and access is gained solely to that information strictly required for flight security and safety. Furthermore, the principle of bodily or personal privacy is also enforced by means of procedural measures: if a passenger so requests, the check must be performed by a man or a woman, as they choose. This means that a passenger may request that they be reviewed by someone of the same sex, for example.[9]

This example shows that, sometimes, organisational measures can help ensure that activities respect fundamental rights without the need to introduce PETs, or only employ them on an occasional basis. One such occasional use of PETs could be to allow or require the blurring of passengers' faces to prevent them being identified at security controls. Nevertheless, it should also be borne in mind that even PETs may be improperly used and need to be included within organisation systems that guarantee privacy. Privacy procedures need to be regularly reviewed, in line with advances in both technology in general and PETs in particular.

3 Ineffective PETs

Something else that needs to be borne in mind is the fact that not all PETs afford the same level of protection. Some may be useful in specific or favourable circumstances, but see their protective capacity limited in more open situations, with sensors and the Internet of Things (IoT). Proper awareness of the limits of using a tool can help prevent placing one's trust in non-existent protection or baselessly accepting a supposed protection that does not, in fact, exist. It is important that we learn that not all PETs provide the same protection and that some only work in certain contexts, but such knowledge lies beyond the purview of the legal community, which has now placed its trust in PbD technologies.

A good example of PETs with limitations are those employed for privacy policies. There are now technologies that permit the personalisation of a screen's content depending upon whether the user is or is not authorised to view the information in question. Thus, in the presence of an unauthorised user, any on-screen data deemed sensitive or otherwise worthy of protection (such as people, signs or car plates) is hidden or otherwise camouflaged (Aved & Hua, 2012). Imagine their use in video surveillance: they would apply, in real time, privacy filters that would guarantee that the recorded image was only fully available to users authorised in accordance with privacy policies (Shen et al., 2015). Another option would be to halt the playing of content on-screen if someone not authorised by the system to view it enters the room. Devices could, for instance, have parental controls or be personalised: imagine a screen that allows a company's workers to check their personal meeting agenda. In the presence of someone else, the screen might show only those meetings between the two, but not those with other people. Generally, privacy policy-related access controls can be established (Werner et al., 2019). Such protection is based on the automation of privacy policies and access controls and sometimes also leverages semantic web services. Whilst interesting as PETs, they are often limited. A hacker could access content remotely (without being physically present in the room) and thereby bypass personalised access controls. To prevent this, a higher level of protection is required: for example, by encrypting the information to make it unusable to any unauthorised recipient.

It therefore becomes clear that any decision on which is the right PET to use in a given situation requires technical knowledge. The mere use of a PET does not always necessarily guarantee effective protection of privacy. In short, proper use of PbD requires adequate and/or effective protection, not the mere use of any kind of technology that could, in the end, prove ineffective.

We can conclude this section by stating that the legal community's reliance on technology must be qualitative: even though it does not completely predetermine the actions of the tech community, it presupposes that this is an adequate and effective technology. PETs therefore need to prove this effectiveness; if not, we would

8 Art. 4.1.1.10.*d*: "the image shall not be linked to any data concerning the screened person and his/her identity shall be kept anonymous."

9 Art. 4.1.1.10.*e*: "a passenger may request that the image of his/her body is analysed by a human reviewer of the gender of his/her choice."

be in the paradoxical situation that PETs would add to the risks faced by the individuals and organisations placing their trust in them. The problem is, though, that no mechanism has been put in place to confirm this effectiveness. If we are to take PbD seriously, we need to establish proper certification and audit mechanisms. It must be noted that the GDPR establishes a new principle of proactive responsibility and accountability that requires data controllers not only to comply with the Regulation's provisions, but also to be in a position to prove that they do.[10] Moreover, Articles 42 and 43 of the GDPR provide for the possibility of certification. Use should therefore be made of this option to certify PETs for specific contexts and on a time-limited basis. Obviously, the certification of technologies needs to be subject to relevant review in line with trends in the technical capabilities of potential hackers.

4 Which are the best effective PETs?

It is engineers who possess the knowledge required to establish whether a tool is effective or not under given circumstances. It is also no coincidence that the best publications on PETs are those penned by engineers or computer scientists (see, for example, Torra, 2017). This is perhaps why jurists have preferred not to specify the exact technology to be used, thereby leaving experts in the field room for manoeuvre and for updating. In this regard, Article 25 GDPR obliges controllers to implement "appropriate technical and organisational measures" to guarantee data protection principles. What's more, data protection law has laid down some specific principles that can provide some general guidelines: for example, said Article 25 GDPR highlights the principle of data minimisation, which can be linked with Article 25.2, that is, with data protection by default. Thus, only personal data which are strictly necessary for each specific purpose of the processing should be processed. A more extensive list of personal data processing-related principles can be found in the Regulation's Article 5, whilst the principle of proportionality also provides us with three criteria (or "tests") for weighing up any restrictions on fundamental rights. The first of these (mentioned above) is the "purpose test", which holds that the tool must be adequate for the risk to be avoided: anything that does not provide effective protection is not a true PET. The second criterion is the "strict necessity test", which states that preference should be given to tools that are less invasive of fundamental rights. This is a legal criterion that is far more difficult for PETs to comply with, as we shall see below. The third and last criterion is the so-called "balance test", whereby one needs to make an overall assessment of whether the restrictive measures provide more advantages than disadvantages. However, it should be noted that these principles currently suffer from limited legal cover. Not only are they (perhaps inevitably) vague, but they are also not 'living' criteria: by this, we mean that these criteria have not been properly either updated or specified, despite the efforts of data protection authorities to adopt highly valuable reports on the issue. Also worth taking into account are consultative technical committees such as the former Article 29 Working Party, the European Data Protection Board and ENISA, among others.[11] Anyone seeking to remain up-to-date on PETs really needs to keep abreast of these groups' work and reports.

Although the GDPR does not predetermine which PETs should be prioritised, it does mention some, such as pseudonymisation (Art. 25.1), although clearly without any intention of providing an exhaustive list. Another practical resource for engineers are the risk impact assessments and the associated potential solutions (Art. 35 GDPR). Risk-based regulation is more specific than principle-based regulation and thus easier to apply; however, the drawback of risk-reduction-focused legislation is that is difficult to include values and rights. One example to illustrate this point is the regulation of nanotechnologies (Roig, 2018): the risk reduction requirements for a specific project must be complemented with sustainability ones to incorporate social and collective values not taken into account when defining secure materials. Risk reduction is an approach that needs to be included within the scope of regulatory debate, but we must not reduce all social problems to a question of optimisation, nor should we ignore general interests, which can only be defended by legislators.

10 Art. 5 GDPR: "2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')" – that is, the principles relating to processing of personal data.

11 See the relevant web page of the European Data Protection Board for the Article 29 (Data Protection Directive) Working Party. For the EDPB itself, see its Internet portal. For ENISA, see its web page. Also of interest is the work of the high-level expert group on artificial intelligence [last consulted: 20 February 2022].

Whatever the case, these GDPR provisions do not contemplate true collaboration between the legal and tech communities working on PETs. There is thus a risk that there could be PETs that, whilst legal, are ineffective (or will become so over time due to a lack of updating), as noted above, and of effective but disproportionate PETs, as we shall now see.

5 Effective but disproportionate PETs

We have noted above that a PET's effectiveness can only be certified by someone with the right technical know-how. However, simply certifying that it provides effective protection is no panacea. One temptation faced by experts in technology is to add layers of protection to thwart any possible hacking attempts. Although this makes complete sense from a standpoint of effectiveness or of making hackers' lives difficult, from a legal perspective, some kinds of ironclad protection come with too high of a price tag in terms of fundamental rights. One example that can help illustrate this point is provided by building or facility access controls based on the use of biometric data.

It is easy to understand the interest in the use of biometric data for access control purposes if you think like a security expert: such data is far more difficult to replace or copy than a simple card or code. However, paradoxically, the risks to users are greater than those of other, less effective technologies. For example, imagine that an access code has been compromised (i.e., has fallen into the hands of an unauthorised person): in such a case, a mere change of access code can be a quick and effective remedy. However, if biometric data is used, although it may not be such an easy task to copy or replace, if someone somehow (for example) obtains a copy of someone else's fingerprints, the solution is not so simple. The biometric data used by the PET cannot be replaced and, what's more, the risk spreads to all those other services (banking, transport, etc.) that use the same – and now compromised – biometric data. This is why the use of biometric data for controlling workers' access to business is sometimes regarded as disproportionate. For example, France's National Commission on Informatics and Liberty (CNIL) has warned that the first step that must be taken is to justify the use of a biometric device: if conventional access cards suffice or if the assets to be protected are not particularly sensitive, the use of a biometric access system by a company is not justified.[12]

However, for our purposes, let us suppose that there are safety concerns in a given case that justify the use of biometric data protected by a PET. The engineer in question may have chosen a measure that is far more difficult to overcome for a hypothetical hacker, such as one using multimodal biometric technology (Anakath et al., 2019). Instead of requiring just one kind of biometric data, this technology bases its level of security on a combination of two or more sets of such data: iris, fingerprint, heartbeat, etc. This provides a much greater degree of effectiveness, making unauthorised use very difficult indeed (Purohit & Ajmera, 2021). However, as we have already said, efficiency is not everything. From a legal standpoint, it is an undesirable option, as not just one but multiple sets of biometric data are compromised. A better choice would be PET based on "untraceable" or "cancellable" biometrics (Manisha, 2020). This more respectful biometric technology works as follows: the tool does not store any original biometric data taken for comparison when taking an access decision. Instead, it keeps the biometric data altered or encrypted by a program, such that the system can perform the assigned task (like allowing authorised people access) without risk. If a hacker cracks the system, they will not find any original biometric data, just this derivative data. So, whilst this modified data can be used for identification and access authorisation purposes, it is of no help whatsoever in reproducing the original biometric data. This is how this kind of PET provides all the advantages of biometric data without the associated risks.[13]

This being the case, how can engineers know they should give preference to untraceable rather than multimodal biometric PETs? Better effectiveness would lead them to opt for multimodal biometrics. Perhaps the only solution is an interdisciplinary team that also includes jurists. In any case, they will find no law or regulation to guide them here: there is no list of legal preferences on biometric data systems. This is something to be found in only a few doctrinal papers (and not even contemplated in others) and that needs to be revised

12 See the relevant web page of the CNIL [last consulted: 20 February 2022].

13 Note that we are now beginning to see the appearance of *cancellable* multimodal biometric systems, designed to provide the best of both worlds (Gupta et al., 2021).

in the light of the appearance of new technologies. As we have already noted, the disconnect between the two communities does little to help resolve these issues. And, even when both communities seek to protect "privacy", they might have a different definition of the term, as we shall now see.

6 PETs based on a non-legal concept of 'privacy'

It may come as a surprise to learn that reliance on PETs may give rise to tools based on a concept of privacy that – oddly enough – has little or nothing to do with the legal definition of the word. Indeed, engineers often create tools that protect a 'privacy' that is not a complete fit with that as understood by jurists. To understand this point better, let us take a look at the use of PETs in social media networks. It is common knowledge that the legal protection afforded to privacy is based on an individual right to protect a space that the individual in question regards as personal and private and wishes to prevent others knowing about. Although this may appear to be a classic liberal right, its modern configuration appeared little more than a century ago in the United States, at a time when national newspapers posed a very serious risk to people's dignity and reputation. It was not enough to move states to guarantee the restoration of one's personal and professional reputation: the risk was generalised and called for a legal response. This came in the form of the right "to be let alone". However, the privacy protection envisaged by engineers for social media networks has little to do with this.

It is true that protecting the privacy of social media users has the goal of preventing a hacker accessing content regarded as private or which is aimed solely at acquaintances or contacts. However, network analysts soon saw that, to protect the privacy of a single social media user, a collective perspective was needed: you have to protect the entire "social graph" of all said user's contacts. This is because, if just one of the contacts has open privacy settings, individual protection for one single user becomes ineffective and their content could become public. Indeed, statistical analysis can even be used to infer non-open content in a social graph or identify users from all their contacts.

So it is that it is not enough to apply PETs to a single user, and it is not enough to anonymise one single user, as jurists might think. You have to anonymise users' entire social graph (see, for example, Gao et al., 2019). This gives rise to a shift in the concept of privacy that, although supposedly individual, is actually, for technical reasons, collective. It is this collective privacy that is designed to be protected in social media, not individual privacy. A tool for individual encryption or managing privacy policies can always be of use but provides no real protection against some kinds of statistical attacks.

There are a number of collective protection options available. There is, for example, that of *k*-anonymisation or group anonymity (e.g., Rajabzadeh et al., 2020). This is a form of protection that prevents an attack from individualising information: at most, such an attack obtains a group of *k* units – say, 1,000 people – all with certain characteristics. The attacker cannot know, however, whether a specific individual is included in this group or not. The higher the *k* (10,000 rather than 1,000 people, for instance), the greater the protection. So, the privacy afforded by this technique can be defined as a guarantee that nobody will ever be able to individualise a profile: they will only have obtained groups of *k*-anonymous people all with the same profile.

Another collective protection technique is that of differential privacy (Dwork, 2006; Yang et al., 2021). This is based on the premise that a hacker has discovered information on one user and, based on this information, attempts to infer that of their contacts. The goal is thus to protect a user even when another user has been compromised. We are not therefore dependent solely on one person, but rather on everyone, in the case of a user whose information becomes known. A further form of collective protection comes from game theory or different kinds of inter-user co-operation techniques. It has been confirmed that what is most effective for the security of all users is a collaborative attitude with others, rather than an individualistic approach. The complexity of collective protection techniques is increasing, as the goal now is to divide up a social media network's structure into different segments to ensure enhanced accuracy. The aim with this is to deal with smarter attacks that are not only statistics-based, but also based on semantic information and meanings (Gu et al., 2019). Such accuracy would allow protection to go beyond that afforded by techniques like differential privacy, which are now 15 years old and can today seem a little conventional (see, for example, Yiping et al., 2019).

The fact is that this collective protection of privacy is something new in law: if you want to protect an individual user's privacy, you have to protect the entire social graph. If all we do is to implement techniques to protect the individual privacy of a single user, they won't be effective. So, how can it be that two communities speak of privacy in such different terms? Well, it is simply because there is no metric for privacy that can show jurists how individual protection, even anonymisation, is simply not enough in social media networks, something that the tech community has known for some time now, at the very least since Cynthia Dwork's 2006 work on differential privacy. The concept of social media network privacy entails the *sine qua non* requirement of collective protection, one that is as yet unknown to the legal community. Also, let us not forget that, without effective protection, there is no right to privacy. So, by anonymising a single user's data, no actual protection for their privacy is provided. Without collective protection, there is no right to privacy on social media networks. Individual privacy arises from the protection afforded the very network itself.

We would like to conclude this section by casting our gaze a little wider. Some readers might imagine that this article is advocating techno-regulation: in other words, that privacy always be protected with PETs. The fact is, however, that social media networks have also revealed the limits of technological protection. At most, social media network protection can protect the privacy of statistically average users, that is, those who habitually interact with others. Such users are protected if guarantees such as those mentioned above are implemented. However, those who have higher-than-average interactions by, for example, posting more information or having more contacts than usual, are not protected by such PETs. They are simply too easy to individualise statistically. This means that the last line of defence in affording them protection consists in education and information: you need to know that, if your behaviour is unusual, there is no real effective protection. This needs to be explained in education systems, and general statistical information on the web should be provided so that users can camouflage their behaviour amongst that of the majority of other users.

7 How can you tell if a PET is effective?

The legal community does not appear to have paid the technology community much attention following its initial reliance on protective technologies. For example, as we have noted above, tech experts have not been told that they should chose untraceable instead of multimodal PETs. Nor has the tech community advised jurists that they have been using a concept of privacy entailing collective protection on social media networks. Furthermore, we jurists have not shown a great deal of interest in finding out whether these supposedly protective technologies actually afford such protection in the real world.

This lack of concern in the legal community shows its great unawareness of technology's regulatory capacities. According to the law, PETs should only implement legal principles, which should *per se* make them useful in protecting privacy. All the options available to engineers are hidden in a kind of black box, out of which emerges a tool implementing these legal principles. Technology is viewed as a tool for implementing the law, not as a co-regulatory option. And that is why PETs' ineffectiveness and even their protection of other concepts of privacy fail to provoke any reaction. Regulation, which is viewed as purely legal in nature, is not regarded as being affected. Well, we believe that this is not the case.

The tech community is convinced that it needs to validate the effectiveness of its solutions and does so outside the scope of the law – and without the legal recognition it deserves. Some metrics are mere risk assessments that set the goals to be achieved and make classifications depending upon the levels obtained (Alsubaei et al., 2019). Such work should be easily accepted into the field of law after the GDPR's inclusion of impact assessments. Some metrics are aimed at specific sectors, such as those focusing on social media networks or graph anonymisation (Casas, 2019, 2020; Zhang et al., 2019). Others, however, take a more general – and more interesting – approach, and aim to assess the guarantee of privacy based on the hacker's expectations of obtaining information (Rebollo et al., 2013). It is here that technological privacy is close to legal privacy: a user's expectation of privacy is associated with a hacker's ability to access the former's data. Most ideas, however, seem to focus on a balance between a tool's accuracy and guarantees of privacy (Sheikhalishahi et al., 2021), so they only try to become less accurate when the aim is to protect a user's privacy.

In short, privacy is a fundamental, defined individual right that needs to be preserved in its entirety. Engineers, on the other hand, view PETs as an arms race, as if they were dealing with cryptography or security. It seems

increasingly clear that there will never be a definitive technology that completely guarantees privacy. The goal can only be, in the best of cases, to counter and hinder attacks as far as possible, and temporarily. Privacy is a battleground of short-term victories (or of short-term defeats, depending upon how you look at it), involving efforts that are as necessary as they are limited. Nothing more, nothing less.

8 The necessary institutionalisation of reliance on technology

With a metric for privacy, we can begin to assess the level of protection provided by PETs. It will then be possible to reject a tool as not fit for purpose (the first criterion of the proportionality test) and establish a ranking of different effective tools, with preference being given to those less invasive in terms of rights. This would permit proper implementation of an assessment of its strict necessity (the second proportionality test criterion). It will also provide valuable information to assess whether the measure has more upsides than downsides – the third criterion in the proportionality test. Despite these advantages, this information will not be truly useful unless it is backed by an institutional platform that can guarantee, the presence, firstly, of legislators and, secondly, of affected stakeholders and users.

The European Union has conceived of tools for better regulation and for co-regulation.[14] A joint community of jurists expert in privacy and tech experts specialising in PETs would provide a good way of improving regulation. As already noted, decisions on different PETs require working together, not an a posteriori interpretation of principles or criteria. The European Commission, as part of its Better Regulation programme (in place since the start of the previous decade), has increasingly been linking impact assessments with a prior assessment of the results of pervious legislation. In this sense, the Regulatory Scrutiny Board is responsible for advising legislators.

However, the European Union has not yet taken any step towards an institutionalisation of the co-regulation of digital platforms with the participation of legislators that adopts any kind of cyclical dynamic. By *cyclical dynamic* we mean regulatory strategies that replace the traditional regulation-implementation sequence by the creation of permanent regulation-implementation-regulation cycles. We believe that a combination of both ex ante and ex post impact assessments could be one way of doing this. Whatever the case, the REFIT and Fit for Future platforms are more limited tools for the simplification and efficiency of and participation in traditional legislative techniques.[15] Their potential for transforming the regulation of new technologies remains to be seen.

The governance of artificial intelligence and algorithms would appear to provide another good example of the appearance of co-regulatory platforms (Roig, 2020). In these cases, the specialist public authority will need to play an active role in invigorating these platforms.[16] This therefore opens up an opportunity for regulatory dynamism in the field of new technologies.

For the time being, however, it would appear that, in the very best of cases, informal platforms will begin appearing from European research programmes, with partial co-legislative responsibilities (Roig, 2018). This is the case with the field of nanotechnology, where informal platforms have begun to appear around European projects, whose outcomes have subsequently been adopted by legislators. The problem with this informal or non-institutionalised approach is the lack of any participation by legislators. In other words, they do not include anyone arguing in defence of the general public interest. True co-regulation cannot do without legislators. The gap between regulation and implementation is narrowing, and it appears that we will see the progressive appearance of increasingly cyclical forms, which will be institutionalised to a greater or lesser extent.

14 See on this matter the communication *Better Regulation. Joining forces to make better laws*.

15 Commission Decision of 11 May 2020 establishing the Fit for Future Platform (C(2020) 2977 final). Commission Decision of 19 May 2015, establishing the REFIT Platform (C(2015) 3261 final).

16 On 21 April 2021, the European Commission presented the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (SEC(2021) 167 final; SWD(2021) 84 final; SWD(2021) 85 final). Article 56 to 58 of this Proposal contemplate and govern the European Artificial Intelligence Board, which could become an important player when it comes to organising co-regulation spaces. Nevertheless, we need to wait for the definitive text and its practical implementation in the coming years. There is also talk that there could be a State Algorithm Assessment Agency by 2023. Together with certification, one could also imagine, in this case, a dynamising function, with co-regulation platforms.

9 Conclusions

This new reliance on PETs does not represent a break with the current paradigm of the monopoly of the legal system's regulatory powers. It simply entails adding another tool for implementing the principles and rights contemplated in the law. Or, at least, that was the initial idea. This article has attempted to outline the limitations that we believe affect this original view of PETs.

The first of these limitations, and one often not contemplated by jurists, is whether it is actually worth using PETs. Paradoxical as it may seem, PETs may entail new risks, and the decision on whether to employ them must be subject to an assessment as to whether they are worth the while – whether their advantages outweigh their risks.

There is also a growing need to assess PETs' effectiveness. An ineffective tool may not only entail risks, as noted above, but could also give a false sense of protection or be used to legitimise a regulatory measure.

To a great extent, the problem stems from a lack of collaboration between the legal and tech communities. It will be simply impossible to organise the co-regulation of PETs without some legal body examining and validating the prioritisation of some PETs over others, given their impact upon fundamental rights and general principles.

This should, at the very least on a dialectic basis and with constant updates and reviews, help us avoid the generalised use of supposedly effective PETs that could actually end up compromising fundamental rights.

This collaboration between the two communities needs to make clear the use of non-legal concepts by PET engineers. The dialogue between them could give rise to a number of points of great interest to the legal community. Is it possible to protect the right to privacy without PETs? If so, we jurists need to make an effort to refresh and bolster the law's protective capacities if we do not wish, either by act or omission, to become complicit in its irrelevance as a practical guarantor of said right.

It does seem clear that technology will not do away with the need for regulation: indeed, it may well accentuate it. However, it may come to pass that we have a number of different 'regulations' in place at the same time: some recognised, but ineffective, others used but informal or with little to do with the principles of law and its values and fundamental rights. Such a scenario is neither desirable nor, in fact, inevitable.

The time has come to officially institutionalise the partnership between the two communities. There are already some examples of incipient co-regulation, such as that of nanotechnology, but they are not concerned with protecting general interests, rights or principles. Governance of artificial intelligence may provide another opportunity in this regard. We need to pay close attention to ensure that this can also present us with the chance to properly shape a platform for PETs.

References

Alsubaei, Faisal, Abuhussein, Abdullah, & Shiva, Sajjan. (2019). A Framework for ranking IoMT solutions based on measuring security and privacy. In Kohei Arai, Rahul Bhatia & Supriya Kapoor (Eds.), *Proceedings of the Future Technologies Conference (FTC) 2018* (pp. 205–224).

Anakath, Arasan, Rajakumar, S., & Ambika, S. (2019). Privacy preserving multi factor authentication using trust management. *Cluster Computing*, *22*.

Aved, Alexander J., & Hua, Kien A. (2012). A general framework for managing and processing live video data with privacy protection. *Multimedia Systems*, *18*, 123–143.

Bygrave, Lee A. (2017). Data protection by design and by default: deciphering the EU's legislative requirements. *Oslo Law Review*, *4*(2), 105.

Bygrave, Lee A. (2020). Article 25. Data protection by design and by default. In Christopher Küner, Lee A. Bygrave & Christopher Docksey, *The EU General Data Protection Regulation (GDPR). A Commentary* (pp. 571–581). Oxford University Press.

Casas Roma, Jordi. (2019). An evaluation of vertex and edge modification techniques for privacy-preserving on graphs. *Journal of Ambient Intelligence and Humanized Computing*.

Casas Roma, Jordi. (2020). DUEF–GA: data utility and privacy evaluation framework for graph anonymization. *International Journal of Information Security*, *19*, 465–478.

Cavoukian, Ann. (2011 [2009]). *Privacy by Design: The 7 Foundational Principles*.

Dwork, Cynthia. (2006). Differential privacy. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone & Ingo Wegener (Eds.), Automata, Languages and Programming. ICALP 2006. *Lecture Notes in Computer Science* (Vol. 4052). Springer. https://doi.org/10.1007/11787006_1

European Union Agency for Network and Information Security (ENISA). (2014). *Privacy and data protection by design. From policy to engineering*.

European Union Agency for Network and Information Security (ENISA). (2016). *Privacy enhancing technologies: evolution and state of the art. A community approach to PETs maturity assessment*.

European Union Agency for Cybersecurity (ENISA). (2019). *Pseudonymisation techniques and best practices. Recommendations on shaping technology according to data protection and privacy provisions*.

European Union Agency for Cybersecurity (ENISA). (2021). *Data pseudonymisation: advanced techniques & use cases. Technical analysis of cybersecurity measures in data protection and privacy*.

Gao, Jianliang, Wang, Jianxin, He, Jianbiao, & Yan, Fengxia. (2019). Against signed graph deanonymization attacks on social networks. *International Journal of Parallel Programming*, *47*, 725–739.

Gu, Qiuyang, Ni, Qilian, Meng, Xiangzhao, & Yang, Zhijiao. (2019). Dynamic social privacy protection based on graph mode partition in complex social network. *Personal and Ubiquitous Computing*, *23*, 511–519.

Gupta, Keshav, Walia, Gurjit Singh, & Sharma, Kapil. (2021). Novel approach for multimodal feature fusion to generate cancelable biometric. *The Visual Computer*, *37*, 1401–1413.

Klitou, Demetrius. (2014). A solution but not a panacea for defending privacy: the challenges, criticism and limitations of privacy by design. In Bart Preneel & Demosthenes Ikonomou (Eds.), *Privacy Technologies and Policy* (pp. 86–110). First Annual Privacy Forum, APF 2012. Springer.

Manisha Kumar, Nitin. (2020). Cancelable biometrics: a comprehensive survey. *Artificial Intelligence Review*, *53*, 3403–3446.

Purohit, Himanshu, & Ajmera, Pawan K. (2021). Optimal feature level fusion for secured human authentication in multimodal biometric System. *Machine Vision and Applications*, *32*(24).

Rajabzadeh, Sara, Shahsaf, Pedram, & Khoramnejadi, Mostafa. (2020). A graph modification approach for k-anonymity in social networks using the genetic algorithm. *Social Network Analysis and Mining*, *10*(38).

Rebollo, David, Parra, Javier, Díaz, Claudia, & Forné, Jordi. (2013). On the measurement of privacy as an attacker's estimation error. *International Journal of Information Security*, *12*, 129–149.

Roig, Antoni. (2018). Nanotechnology governance: from risk regulation to informal platforms. *NanoEthics*, *12*(2), 115-121.

Roig, Antoni. (2020). *Las garantías frente a las decisiones automatizadas. Del Reglamento General de Protección de Datos a la gobernanza algorítmica*. Bosch Editor.

Rubinstein, Ira S. (2012). Regulating privacy by design. *Berkeley Technology Law Journal*, *26*(3), 1409–1456.

Schaar, Peter. (2010). Privacy by design. *Identity in the Information Society*, *3*(2), 267–274.

Schartum, Dag Wiese. (2016). Making privacy by design operative. *International Journal of Law & Information Technology*, *24*(2), 151–175.

Sheikhalishahi, Mina, Saracino, Andrea, Martinelli, Fabio, & La Marra, Antonio. (2021). Privacy preserving data sharing and analysis for edge-based architectures. *International Journal of Information Security*.

Shen, Jie, Cai, Ying-Jue, & Luo, Lei. (2015). A context-aware mobile web middleware for service of surveillance video with privacy. *Multimedia Tools and Applications*, *74*, 8025–8051.

Tamò-Larrieux, Aurelia. (2018). *Designing for privacy and its legal framework: data protection by design and default for the Internet of Things*. Springer.

Torra, Vicenç. (2017). *Data privacy: foundations, new developments and the big data challenge*. Springer.

Werner, Jorge, Westphall, Carla Merkle, Azevedo Vargas, Andre, & Westphall, Carlos Becker. (2019). *Privacy policies model in access control*. IEEE International Systems Conference. Orlando, Florida, United States. https://doi.org/10.1109/SYSCON.2019.8836759

Yang, Liu, Yong, Zeng, Zhihong, Liu, & Jianfeng, Ma. (2021). Spectrum privacy preserving for social networks: a personalized differential privacy approach. In Yongdong Wu & Moti Yung (Eds.), *Inscrypt 2020, Lecture Notes in Computer Science* (Vol. 12612, pp. 277–287). Springer.

Yiping, Yin, Qing, Liao, Yang, Liu, & Ruifeng, Xu. (2019). Structural-based graph publishing under differential privacy. In Ruifeng Xu, Jianzong Wang & Liang-Jie Zhang (Eds.), *Cognitive Computing – ICCC 2019* (pp. 67–78). *Lecture Notes in Computer Science* (Vol. 11518). Springer.

Zhang, Cheng, Jiang, Honglu, Cheng, Xiuzhen, Zhao, Feng, Cai, Zhipeng, & Tian, Zhi. (2019). *Utility analysis on privacy-preservation algorithms for online social networks: an empirical study*. Springer.