General Data Protection Regulation: new ethical and constitutional aspects, along with new challenges to information law

Maria Bottis*

Ionian University,
DALMS, 72 Ioannou Theotoki,
Corfu 49100, Greece
Email: botti@otenet.gr
*Corresponding author

Fereniki Panagopoulou-Koutnatzi

Panteion University,
136 Syngrou Avenue,
11671, Athens, Greece
Email: ferenikipan@yahoo.gr

Anastasia Michailaki

Ionian University,
DALMS, 72 Ioannou Theotoki,
Corfu 49100, Greece
Email: amichailaki@gmail.com

Maria Nikita

University of Macedonia,
156 Egnatia Avenue,
54636, Thessaloniki, Greece
Email: Nikita_ma@yahoo.gr

Abstract: The EU 'General Data Protection Regulation' (GDPR) marked the most important step towards reforming data privacy regulation in recent years, as it has brought about significant changes in data process in various sectors, ranging from healthcare to banking and beyond. Various concerns have been raised, and as a consequence of these, certain parts of the text of the GDPR itself have already started to become questionable due to rapid technological progress, including, for example, the use of information technology, automatisation processes and advanced algorithms in individual decision-making activities. The road to GDPR compliance by all European Union members may prove to be a long one and it is clear that only time will tell how GDPR matters will evolve and unfold. In this paper, we aim to offer a review of the practical, ethical and constitutional aspects of the new regulation and examine all the controversies that the new technology has given rise to in the course of the regulation's application.

Keywords: General Data Protection Regulation; GDPR; constitutional rights; technological progress; scientific research; access to information; democratic principle; ethical aspects.

Reference to this paper should be made as follows: Bottis, M., Panagopoulou-Koutnatzi, F., Michailaki, A. and Nikita, M. (2019) 'General Data Protection Regulation: new ethical and constitutional aspects, along with new challenges to information law', *Int. J. Technology Policy and Law*, Vol. 3, No. 2, pp.172–187.

Biographical notes: Maria Bottis is an Associate Professor of Information Law at the Ionian University in Greece. In 2000–2004 she was appointed as a Faculty Fellow at Harvard University. She is the Director of the International Society for Ethics and Information Technology and she has instituted the International Conference on Information Law Series.

Fereniki Panagopoulou-Koutnatzi is an Assistant Professor of Constitutional Law at Panteion University, Athens. She has been for eight years a Legal Auditor at the Hellenic Data Protection Authority. She is the Chairperson of the Executive Committee of the Hellenic Delegation to the UNESCO Bioethics Chair.

Anastasia Michailaki is a PhD candidate at the Ionian University.

Maria Nikita is a PhD candidate at the University of Macedonia.

This paper is a revised and expanded version of a paper entitled 'GDPR: new ethical and constitutional aspects, along with new challenges to information law' presented at 9th International Conference on information Law and Ethics, Rome, 11-13–July.

1 Introduction

The EU General Data Protection Regulation (GDPR) constitutes the most crucial regulation on data protection during the last 25 years, as it is a regulation designed to affect data protection laws on an almost worldwide level, this actually being an intended consequence thereof. The fact itself that what we are faced with is a Regulation, rather than a Directive that would necessitate a legislative instrument of incorporation into the national legal system of each EU member state, shows us that the European legislator was not ready to accept any real deviation from the basic law on data protection throughout Europe. This Regulation, just like Directive 95/46/EC, applies across all private and public sectors, from healthcare and insurance to banking and education, and so forth. The Regulation, of course, was the result of a legislative process of dialogue, public consultation, negotiations, and all the activities prescribed by the law and beyond; still, after its entering into force, and after the two years given for the EU member states to prepare themselves for this considerable change, we note disparagement relating to a series of GDPR issues: its principles, the rights of data subjects, the obligations of data controllers, the role of the data protection officers, the financial and other consequences for private companies and the organisations of the public sector, and of course, the ramifications it has for private persons. The Data Protection Authorities around Europe

also find themselves in different circumstances that have been subject to important changes that they have to face successfully, irrespective of their actual abilities. Constitutional rights relevant to information and their balancing when in conflict must also be interpreted anew, under the GDPR rules. The unprecedented extraterritorial arm of the new law is also posing new challenging questions. At the same time, the new system operates under the threat of severe penalties for breaches. Most importantly, therefore, now that the GDPR has formally entered our lives, we need to check how these new data protection laws affect us in actual fact and assess what their true implications actually are, financially, ethically, constitutionally (rights affected) and otherwise.

2 Public sector organisations and the GDPR

The public sector organisations are the largest collectors and processors of personal data. Indeed, oftentimes they process sensitive data, which present the highest risk related to the rights of data subjects, i.e., the citizens. Therefore, it follows that, as these organisations are public, they also represent the State, and as such, they are the entities that should be more ready than any other to implement the GDPR. Still, what we often see when it comes to these public organisations is that they store data under questionable principles and for periods of time that lie out with data protection regulations, even if unknowingly so.

We have every reason to expect that the way data are processed by the public sector organisations will change because of the GDPR. These organisations have to appoint a data protection officer, solely by reason of their nature as public bodies. Public organisations also need a different justification for processing data, beyond 'legitimate interest' as a ground. Thirdly, if a public body wants to transfer personal data to a third country that is not bound by the GDPR, 'consent' of the data subject cannot legitimise this transfer by itself; we need to see a specific agreement between the government authorities involved. There is, therefore, a clear differentiation in how the GDPR sees the obligations of public sector organisations in this case, vis-à-vis those of private ones. This differentiation may be the result of the well know distrust of the 'state' in Europe: whereas in the USA, it is private companies and the representatives of 'private power' that are seen as being the most 'dangerous forces' against citizens' safety and privacy data, the exact opposite holds true for Europe, where the same danger appears to stem from governmental power.

Irrespective of whether this selection of different legislative treatment is correct in Europe, public sector organisations will find themselves in difficult positions in order to comply with the GDPR. The immense variety of public sector organisations, of course, cannot be left out of this discussion. A 'one-size-fits all' regulation is, most unfortunately, not the proper choice here, as a public body obliged, for example, to appoint a data protection officer can range from a five-person staffed community public library to a more than a thousand employee Ministry of Health. These immense discrepancies cannot be just disregarded. Public bodies deal with all the complex domains of education, healthcare, defence, fire-brigading, police, justice, transport, etc., so we can only expect great differences in the way these public bodies will implement the GDPR requirements, which poses at least a question mark to us, as one of its legislative purposes is, clearly, harmonisation. All the more, these public bodies have different resources and funds to allocate in order operate; others are, let us say, rich, whereas

others have considerably limited financial resources; others are overstaffed, while others are significantly understaffed; others are, therefore, efficient in their function and others are not so at all. Many of these organisations will simply be unable to fully comply with the GDPR, as they will lack the necessary IT systems, adequately trained staff, generally educated personnel (i.e., not only IT-wise) – and so on. If we take this argument further, we must expect to see the same divergence of compliance with the GDPR in public bodies throughout the EU, which is a divergence that will ultimately be tremendous, and which will be, most unfortunately, a prime example of the digital divide of our times.

3 Private enterprises and the GDPR

Compliance with the provisions of the GDPR is an ongoing procedure for private enterprises that process personal data. Logically, all private sector organisations, companies, societies, etc., process personal data and will have to comply with the GDPR on a much stricter level than what they used to under Directive 95/46/EC on data protection; the threatened high fines, which will be proportional to the companies' earnings, are but a small example of this differentiation. But this compliance also comes at a higher cost, as they will have to train employees on data protection, appoint, where necessary, a data protection officer, ensure the data processing information systems are GDPR compliant, and also see to that data shall have to be encrypted and/or classified, access will have to be limited to particular persons and the list of these persons must also be GDPR compliant, implement constant monitoring of all activities and safeguards that are required by law, and all this, of course, translates into increased costs. Of course, it follows that these costs will be passed on to the customers, at least for the most part; it may also mean cuts to other previously standard costs so as to set off the losses due to the GDPR rules.

Many private enterprises will outsource all matters of GDPR compliance to experts, companies or persons. The problem is that we still do not know the level of these new costs. If data subjects elect to exercise their rights to access, erasure, correction, portability and so on at a large-scale, this will mean for a company that compliance, threatened by large fines, will cost quite a lot. In the case of a staged large-scale filing of requests, such as, for example, triggered by a labour union on behalf of the employees, a company may very well face a disproportionate burden in order to meet these requests. The GDPR does not seem to offer any safeguards in this case, for example by disallowing the specific abuse of rights by data subjects-claimants via also providing a corresponding penalty.

We have also come across examples of over-compliance by private companies when the GDPR came into force. For example, many companies e-mailed all their customers/users in order to regain consent for data processing,[1] which was both unnecessary as well as a nuisance to these e-mails receivers (Gottlieb, 2017). Another setback here was the false sense of compliance given by this over-compliance to both the companies themselves and the data subjects/customers. The result was to spend time and resources for this correspondence, the erasure of data when no answer was sent for no legal reason, and the loss of a chance to devote this time and money to actual compliance, and of course, to other meritorious business activities in parts of the businesses' real purpose of operation.

No matter what happens in the end, private enterprises will pass their new costs of GDPR compliance on to their clients which will, in turn, increase the prices of the products or services that they offer to the public (Ponsoldt and David, 2007). It is questionable, however, whether this result is desirable overall, even if it could be supported that data protection is a primary societal goal. If data protection costs are this high, then perhaps the GDPR will face very negative, yet reasonable, criticism in the future. At this moment, there are no guarantees that the GDPR will succeed in its important goals, and this ambiguity is further accentuated as Directive 95/46/EC appears to have presented us with many indications of failure that led to the GDPR in the first place, as a much more austere legislative instrument.

4 The citizen as a data subject and the GDPR

The GDPR affects the rights of the ordinary citizen, the data subject, to a great extent. In fact, within its main goals, we have the protection of citizens from the abuse and misuse of their personal data, just like in Directive 95/46/EC. Therefore, we need to reflect upon the ways in which this increased protection, in comparison with the protection envisaged in the 1995 Directive, benefits the ordinary person, as well as consider the consequences of the implementation of the GDPR for ordinary people.

It is definitely hard to come to any certain conclusions at this time. The implementation of the GDPR commenced on May 25, 2018 and it is still very early to judge. But we can start from the start: How many people really care about the protection of their personal data and how is this determined and evidenced? If we judge from the constant uploading of personal data in social media, such as Facebook, it would appear that people do not really seem to care all that much about data protection – or at least not in this case. We should also see how older/younger citizens, or citizens from countries that were always democratic and citizens from countries that were behind the iron curtain or highly educated/less educated or illiterate citizens see the protection of their personal data under the GDPR. Information on what the GDPR actually is and what rights people have is certain to vary in terms of dissemination in the member states of the EU. It follows that people have access to very different levels of information on the GDPR within the EU, never mind the logically great differences in their understanding of the GDPR in any way (as people do not understand the same information offered to them in the same way or with the same success).

Do we have evidence that citizens actually care about the GDPR? A reasonable thought is that they may care, but that they may also simultaneously understand that the flood of technological applications in their smartphones, CCTV cameras, etc., makes proper data protection difficult to believe in; all movement and speech seems to be tracked and monitored anyway. In this case, would not they think that any GDPR at all is just a cover-up and that this is quite an unenforceable Regulation, as the law never catches up with technology anyway and so it is rendered practically irrelevant? One more click of the mouse, granting a license for the processing of personal data could very well become the epitome of the application of the GDPR in a citizen's life. However, this was certainly not the reason behind the whole GDPR legislative adventure.

There was, of course, intense publicity surrounding the GDPR and most of the citizens in the EU, at least those living in urban areas, are bound to have taken notice of this Regulation. We do, therefore expect to have achieved at least a certain level of

GDPR awareness. Since all public bodies and many private ones have to appoint a data protection officer, under the threat of heavy fines, this awareness has to have become even more intense. Data that people have to share of their own will, giving their consent, also makes them aware of the GDPR, but are data subjects also aware of the personal data they offer unwillingly though their smartphones, computers and other devices and applications? In many cases, if data is not offered, the service is denied, so the data subject is, in fact, obliged to give their data. This of course, depends on the importance of this application to the purported user – but we also all know how important these new technologies are to our everyday life: the bottom line ultimately is that people just have to consent.

5 New markets related to the GDPR

The GDPR led to a whole now data protection-related market. It is not only lawyers who started to acquire a new domain for services, such as the training on the GDPR to facilitate compliance with the new Regulation.

Information technology consultants, business executives, data protection officers and other experts became intensely involved with the application of the GDPR. A whole new field of training and educating on the GDPR was born, which is something that is entirely new, as Directive 95/46/EC did not give rise to this new market. Institutions were formed or extended their services to offer GDPR education, training towards compliance and safety for the mainly big businesses that are threatened with great fines. These changes took place not only in the EU but also abroad, as the GDPR's reach spans beyond the EU, in view of the fact that it applies worldwide under circumstances provided by Art. 3 of the Regulation.

Important resources, such as time and money, are invested when it comes to GDPR compliance by data controllers and data processors. The mission of the GDPR is to enhance awareness on data protection and ensure that a new and strong data protection mentality is shaped in people, whereas compliance with the Regulation also ensures that businesses avoid administrative penalties. But these businesses and private enterprises will not normally be able to comply with the GDPR using their own resources; they will have to seek the services of specialists on personal data, external consultants, and continuously train their own personnel to remain compliant with the strict rules of the new Regulation.

6 The impact of the severe penalties and the key role of the supervisory authorities

The perceived change in the nature of the relevant penalties from 'educational', which is what they were perceived as being until recently, to 'quasi-revengeful', is certainly worth considering. It is true that the small fines that had been imposed so far against companies were received, on many instances, with a sense of irony, while they were also seen as being ineffective in terms of adopting friendly practices towards data protection. Indeed, there have been more than a few data controllers who, following a cost-benefit assessment, found that the imposition of a fine would be preferable to compliance with

the relevant data protection legislation. The imposition of heavy fines will compel businesses to change their mentality and proceed to the adoption of friendlier data protection practices. Nevertheless, the application of very large fines may lead many businesses to a stalemate, given that, in certain cases, businesses conduct unauthorised processing, they do not keep necessary records, they do not carry out risk impact assessment studies, etc., and they do so unwillingly. Furthermore, what will happen in terms of the public sector which, in certain countries, constitutes the largest potential 'risk-taker' when it comes to personal data? (Mitrou, 2018) Will those high fines be imposed on the careless employee or will they be passed on from one public treasury to the next one? And, if the actual issue is lack of space, how will this be addressed? Large hospitals, courts of law and public authorities do not have safe storage areas where classified access should be available. The reality is that, in many cases, court files are stored in car-parks, patient records kept in hospitals are accessible to visitors and no-one has the time to decide which ones should be destructed after the period for which they must be kept has lapsed.

In addition to the above, the issue of increasing bureaucracy in supervisory authorities (Gola, 2017) in view of the increased powers that they have been vested with also comes to the forefront, especially considering that it is far from easy for them to recruit new staff.[2] Can those independent authorities bear the heave burden of the Regulation? Clearly, the answer cannot be the same for all supervisory authorities. Even if they are staffed with the best of employees, the superiority of some of these European authorities in terms of the number of their staff vis-à-vis that of others, leads us to the conclusion that effective supervision cannot take place, in practical terms, at the same level for everyone.

In addition to supervision, independence itself also bears a high cost: How can we be certain that the members of independent authorities will not engage in activities that constitute a conflict of interest, when they consider their salaries as being mere 'pocket money' if compared to those enjoyed by members of other independent authorities? A comparative overview of the salary situation amongst the members of the independent authorities throughout the EU gives rise to wide disparities. From the practice so far, one may also ascertain that the control of authorities on this point is not always substantive (Panagopoulou-Koutnatzi, 2016).

7 The uncharted waters of extraterritoriality

Furthermore, how will the GDPR be applied outside the European Union, meaning how will the principle of extraterritoriality, as asserted by Article 3 of the GDPR, be enforced? How will a European institution impose sanctions on a non-European entity with regard to legislation that the latter has not become a party to? Are there adequate mechanisms in existence? These questions are also of concern to the writers of the present article and they will, no doubt, find their answer in practice, given that what we are faced with at present is a piece of legislation of monumental extraterritoriality.

At this point, it should also be noted that the extraterritorial application of a right puts the traditional perception on sovereignty and the territorial application of rights to the test, whilst also stirring the constitutional discourse on matters pertaining to the institutional autonomy and self-sufficiency of state entities. In this sense, it would not be out of place to be led to the provisional conclusion that the GDPR appears to be

attempting to shift constitutional guarantees that not even war or military intervention were able to change. The aspiration of the GDPR seems excessive, as it seeks to overcome the obstacles that were set by the ECtHR case-law on matters of extraterritoriality,[3] thus testing the traditional doctrine and imposing obligations on non-European citizens and businesses without the intercession of an act of sovereignty on the part of the state that they are citizens of or the state where they are established in. In this sense, the global digital economy revives, through its technical means, the question on global justice by proclaiming the obvious point regarding the lack of borders when it comes to the internet and the need for a global response to the issues arising from it [Panagopoulou-Koutnatzi, (2012), p.110; Geraris, (2010), pp.42–43]. The first reaction could be that the effort towards a global response takes place unilaterally, without all the contracting parties having joined the dialogue, and most importantly, without them having consented to it. Nevertheless, a more mature approach could lead us to the conclusion that extraterritoriality, as a dynamic concept, is spread to such an extent that the rights of data subjects who are located within the EU are affected (for example, in instances of e-commerce and profiling).

It is, nevertheless, true that the period of mockery and irony on the part of American companies was followed by a period of concern and compliance. Companies outside the EU have complied or are at a stage of achieving compliance with the new regulatory framework, while Japan has taken a further step by incorporating a large part of the GDPR in its national law.

8 The challenge posed by the principle of consistency

Is the uniform application of personal data within the scope of application of the GDPR possible (see Recital 10 of the GDPR)? Is it the case that something like that would appear to be utopic? Is the uniform imposition of administrative fines, pursuant to Recital 150 of the GDPR, feasible? At the same time, could the principle of consistency act as an alibi towards the uniform proliferation of practices? For example, if the monitoring of driving behaviour by an employer were to be allowed in a country, under certain conditions, on the basis of a decision issued by a supervisory authority, could this practice be spread to other jurisdictions pursuant to the principle of consistency? It is expected that these questions will be answered on the basis of the administrative practice of the supervisory authorities.

9 Further issues of constitutional consideration

9.1 Access to information

It makes sense that there is concern about whether our enthusiasm for personal data protection has led to the neglect of other constitutional rights. Would it not be helpful if the same authority that protects personal data would also protect the corresponding right to access to information, on an equal footing? Access to information and protection of personal data should primarily act complementarily and only secondarily contrarily [Vlachopoulos, (2016), pp.124–125; Vlachopoulos, (2007), p.74]. The contemporary and harmonised trend seen in European legislation, which favours the

equal treatment of individual rights, is the establishment of a single administrative authority for the protection of personal data, as well as for the freedom of information[4] [Panagopoulou-Koutnatzi, (2017b), pp.340–341]. Therefore, when there are other constitutionally protected competing rights, such as the freedom of information prominence should not only be given to the protection of personal data. This position is fully aligned with the Regulation, which emphatically highlights in Recital 4 that:

> "The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the charter, as enshrined in the treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

At the same time, pursuant to Article 85, the Regulation lays down the right to freedom of expression and information, balancing the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes. The ability of fulfilling the right to information is expressly granted to the state legislature on the basis of Article 85, which stipulates that "Member States […] reconcile the right to the protection of personal data with the freedom of expression and information." In this sense, it is stressed that the right to personal data protection is not an absolute and tyrannical right (Anthopoulos, 2017). In essence, the fundamental principle of Directive 95/6/EC is reiterated, highlighted, but also updated, and it sets the protection of personal data and the free movement of data on an even playing field, straight from its title.[5] In practice, the Directive did not seek to establish an absolute right, with the protection of private life being its ultimate goal, but rather the liberalisation of the movement of data within the EU, its final goal being not to hinder the exercise of four community freedoms, having the fundamental right to private life as its boundary [Christou, (2017), p.19]. It is also noted that, in the relevant discourse relating to the drafting of the Directive, the arguments relating to its economic aspects and the internal market were at the forefront[6] [De Hert and Gutwirth, (2017), p.61]. In the spirit of what has been discussed above, it is concluded that national authorities are not doing all that they ought to and that they will do so only once they change and become authorities for the protection of data and access to information.

Concerns have been raised regarding the new regime of quasi self-regulation, on the basis of which it is expected that authorisation issued by the supervisory authority for the provision of sensitive personal data will not be required. Article 36, Paragraph 5 of the Regulation stipulates that "Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health." If the Member State does not establish an authorisation regime, the data controller will be deciding about their issuance, following examination, on his/her part, of whether the conditions of the GDPR are fulfilled. It is noted that the decision not to grant authorisation by a supervisory authority is not one that is entered into lightly. Practice has shown that the prior granting of authorisations by a supervisory authority makes its work notably more

difficult as, due to the heavy workload involved in the authorisations that are to be granted [Kardassiadou, (2012), p.25], the exercise of far more important supervisory, advisory and regulatory functions carried out by the authority are inevitably hampered. The outcome of this is that the authority ends up carrying out its work with great difficulty, and on many occasions, with significant delay. Indeed, if we take into consideration that a large number of applications are filed on an 'urgent basis' due to the shortly upcoming hearing dates involved, as well as that many applications have not been duly completed because of lack of authorisation on the part of the applicants or lack of sufficient justification concerning their legitimate interest, etc., the work of the authority becomes even more difficult (Mittleton, 2013).

In this way, nevertheless, the choice of data controllers not to provide data so as to preclude the possibility of being involved in court disputes in case of doubt is rendered not only easier but also legally safer. If, however, the right to information were to be established on an equal footing with that of the right to the protection of personal data, no such concern would present itself.

9.2 The democratic principle

The GDPR has an immediate effect on the strengthening of the democratic principle, through a transparent procedure towards determining the election result. In this case, the companies that utilise artificial intelligence methods play an important role in shaping popular will. All candidates rely on their services, as they constitute the main information point for the overwhelming majority of voters – and particularly those of a younger age (Nielsen, 2017). Elections are not won by the person who puts forward more convincing arguments, but rather by him/her who uses the most effective technology in order to manipulate voters, at times even in a manner that is utterly emotional and unreasonable. Data that have been accumulated, collected and stored through algorithmic technologies have been likened to the new 'currency of power', as they may be used directly towards the micro-targeting of voters, with a potentially decisive effect on the elections [Council of Europe, (2017), p.30]. It is true that less well-known candidates may not have the means to utilise the most effective manipulation technologies that help in predicting voters' preferences (Grassegger and Krogerus, 2017). Even though political advertisements are now regulated and there are impartiality requirements in place that are imposed on public service broadcasters, there are no equivalent measures established in relation to the use of algorithmic predictions of voters' preferences and behaviour, which may actually have just as significant an effect on voters – if not a bigger one [Council of Europe, (2017), p.31]. The impact on the election result was particularly apparent in the case of Brexit and that of the American elections in 2016. The Brexit referendum was determined on the difference of 600,000 voters, meaning just 1% of registered voters, who had been the target of companies engaged in voters' manipulation through the use of propaganda, psychology and technology (Cadwalladr, 2017). Similarly, there was also extensive discussion about Cambridge Analytica in the case of the American elections (Cadwalladr, 2017).

In view of the above, it is deemed necessary that democratically authorised legislative bodies should adopt strict legal rules on key internet matters, instead of simply adopting codes of conduct and ethical self-regulation, so that artificial intelligence can serve public rights. A main priority in this area is the application of the principle of transparency, with

the aim of preventing the conflict of interest for those who work in these companies (Nemitz, 2018). The companies in question cannot be left to their own devices or enjoy the trust of society in order to serve the interests of citizens. A key specimen of such vertical legislation is the GDPR, which constitutes a glaring example of the ability to enforce law over new technological advances, meaning a neutral law in respect of technology, but also of the outcome of the compromise made between the protection of the rights of citizens and other competing rights, such as research, innovation and technological progress (Nemitz, 2018). Through the application of the principle of transparency (Article 12 et seq. of the GDPR), the citizen should be able to comprehend – at least to some degree – the way in which algorithmic decisions are made. Accordingly, pursuant to the application of the principle of transparency, companies that are hiding behind artificial intelligence applications will be precluded from secretly forming popular will when it comes to elections.

9.3 The freedom of scientific research

Artificial intelligence and the processing of megadata may catapult the freedom of research; the exploitation of all this information, however, must take place under the conditions of the protection of personal data. It must also be pointed out that the carrying out of scientific research is given some precedence by the GDPR, in the sense that no excessive guarantees of personal data protection, which may practically impede the conduction of scientific research, may apply. Pursuant to Recital 33, it is possible to grant overall consent for some areas of scientific research, to the degree that this is permissible by the intended purpose. The main aim of this particular provision is the facilitation of scientific research, so that the researcher can be relieved of the burden of multiple consents when the purpose of his/her research changes [Panagopoulou-Koutnatzi, (2014), p.30].

10 The reactions thus far

But what has happened thus far? A sense of concern is being spread, in fact, at times, with great zeal and at aimed at the wrong direction. A characteristic example can be seen in the panic that took over companies when they sent out a message to their entire client list regarding the granting of consent in the context of the new regulatory framework, which is something that was not, to a large extent, actually required (Gottlieb, 2017). More than a few companies spent a considerable amount of money for the dispatch of such messages, rather than investing it towards ensuring their compliance with the new rules. Indeed, quite a number of companies erased a large number of their contacts, without good reason, thus losing a significant part of their clientele, and consequently, of their business activity. At the same time, and although this is not provided for in the GDPR, the certification of data controllers has now started to take place, without good cause and for purely commercial reasons,[7] as reference to certification is only made in relation to data processing activities carried out by data controllers and processors, pursuant to Article 42, Paragraph 1 of the GDPR.

But have any steps been taken towards the right direction in this respect? In view of the fear regarding the imposition of high fines, a new mentality on the protection of personal data is gradually being developed. As mentioned earlier, companies are

beginning to comply, however the road is still long and rocky, and at times, uncharted. Mature voices of respected experts on the protection of personal data put forward their concerns about the correct interpretation of the provisions of the GDPR, without hesitation. The question now is, should we now just 'face our ignorance' [Efthymiou, (2018), p.53] or is it best to deal with our concerns at a later time, when the waters will have been charted? Would it be better if we could reconcile with the fact that there is no right or wrong interpretation at all times,[8] but rather that we struggle, well-intentionally, with different versions of the better option?

11 Could it be that the text of the GDPR is lagging behind, following technological advances?

Has the text of the GDPR itself is already beginning to be surpassed by technological progress? A characteristic example can be seen in Article 2 of the GDPR on automated individual decision making, including profiling, which expressly stipulates that in the event of automated processing, the data subject has the right of securing human intervention on the part of the data controller, the right to express an opinion and to question the decision taken. At the same time, the right of an individual to receive information on the logic involved in the making of such a decision in the context of the assessment in question is also recognised, set out, in practice, in the context of the information duties enshrined in Articles 13(2)(f) and 14(2)(g). This reasoning is not always feasible, however, as the manner in which decisions are made through artificial intelligence is no longer technically known and verifiable.[9] In fact, it is often argued that the text of the Regulation is characterised by marked disaffection towards the making of automated decisions, without making any reference to the advantages offered by the use of artificial intelligence in the decision-making process [Schulz, (2017), margin no. 2]. Also, there has been severe criticism regarding the fact that the text of the Regulation only offers protection against the making of decisions on the basis of automated processing, whilst it does not adequately address the issue of profiling [Schulz, (2017), margin no. 2; Gola, (2017), margin no. 37].

12 In lieu of an epilogue

Is the Regulation perhaps excessive and utopic, or could it be that certain categories of data require a maximum level of protection? [Panagopoulou-Koutnatzi, (2019), p.13]. The all-conquering time shall be the main judge of all this: as time will pass, enthusiasm will abate and maturity will ensue. Independent authorities will, no doubt, also be decisive co-players in this journey of personal data protection: depending on the stance that they will take, but also on how strict they will be in terms of imposing sanctions, and mainly, depending on the severity of the fines that they will impose, protection will either be intensified or eased up. But will protection be uniform within the European framework? How will the challenge of the principle of consistency unfold? Are the related aspirations perhaps too excessive? Is it not somewhat contradictory that we should seek something more than Directive 95/46/EC, when it seems that even its fundamental purposes were not, to a large extent, fulfilled? Let us take some time and allow some

leeway to the supervisory authorities, hoping that, after a while, we will be reviewing their practices and notice impressive results in the area of compliance, yet not to the detriment of equally important constitutional rights.

This paper is concluded with a temporary pause: and we shall use this semi-colon in our trail of thought, because we still have a lot to learn in the area of personal data protection. The more we read and raise questions, the more we discover gaps in our knowledge. "You have read, but not understood; for, had you understood you would not have condemned", writes the unsurpassed Alexandrian poet, Constantine P. Cavafy ("You have not understood/Ουκ έγνως").

Acknowledgements

This paper is composed within the framework of a research project titled 'The new data protection law in Europe – a regulation for the future' within the framework of the Operational Programme "Human Resources Development, Education and Lifelong Learning" of NSRF – Partnership Agreement 2014–2020 and is co-funded by Greece and the European Union – European Social Fund [Law 4314/2014 in accordance with the requirements of European Regulation (EC) 1303/2013].

References

Altiparmak, K. (2004) 'Bankovic: an obstacle to the application of the European Convention on Human Rights (ECHR) in Iraq?', *Journal of Conflict and Security Law*, Summer, Vol. 9, No. 2, p.213 et seq.

Anthopoulos, C. (2017) 'Personal data and rights', *Ethnos [Nation] Journal*, 18 January [online] http://www.ethnos.gr/xaralampos_anthopoulos/ (accessed 25 May 2019)

Bampiniotis, G.D. (2002) *Dictionary of the Modern Greek Language*, Lexicology Centre, Athens.

Cadwalladr, C. (2017) 'The great British Brexit robbery: how our democracy was hijacked', *The Guardian*, 7 May [online] https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy (accessed 25 May 2019).

Christou, V. (2017) 'The right to protection from data processing', *Foundation-Interpretation-Perspectives*, Sakkoulas Publishers, Athens, Greece.

Council of Europe (2017) *Study on the Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms) and Possible Regulatory Implications* [online] https://rm.coe.int/study-hr-dimension-of-automated-data-processing-incl-algorithms/168075b94a (accessed 25 May 2019).

De Hert, P. and Gutwirth, S. (2017) 'Personal data protection in the Strasbourg and Luxembourg jurisprudence: constitutionalisation in action', *Administrative Law Journal [EfimDD]*, Papakonstantinou, E. (Trans-Ed.), p.57.

Efthymiou, M. (2018) 'Only a few kilometers', *Stories on History, (In Collaboration with Makis Provatas)*, p.53, Pataki Publications, Athens.

Geraris, C. (2010) 'Personal data and new challenges', *Media and Communication Law [DiMEE]*, p.42.

Gola, P. (2017) 'Einleitung', in Gola P. (Ed.): *Datenschutz-Grundverordnung Kommentar* [online] https://beck-online.beck.de/Dokument?vpath=bibdata%2Fkomm%2Fgolakodsgvo_1%2Fewg_dsgvo%2Fcont%2Fgolakodsgvo.ewg_dsgvo.vor1.htm&anchor=Y-400-W-GOLAKODSGVO_1-NAME-ID_6 (accessed 25 May 2019).

Gottlieb, C. (2017) *The GDPR Soft Opt-in Opt-out*, 11 September, Linkedin [online] https://www.linkedin.com/pulse/gdpr-soft-opt-in-opt-out-carl-gottlieb (accessed 25 May 2019).

Grassegger, H. and Krogerus, M. (2017) 'The data that turned the world upside down', *Vice*, 28 January [online] https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win (accessed 25 May 2019).

Hellenic Data Protection Authority (HDPA) (2015) *Annual Report 2015* [online] http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/FILES%20ANNUAL%20REPORTS/ANNUAL%202015%20V2.0%20WEB%20VIEW2.PDF (accessed 25 May 2019).

Kardassiadou, Z. (2012) 'The processing of personal health data by health and social security providers', *Law in the Digital Age, 3rd Pan-Hellenic Conference E-Themis*, Union of Greek Jurists e-Themis (Ed.), Legal Library Publications, Athens, p.13.

Knight, W. (2017) 'The dark secret at the heart of AI', *MIT Technology Review*, 11 April [online] https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/ (accessed 25 May 2019).

Marouda, M.D. (2014) 'The "effective control" as a precondition for the application of the law of occupation and interaction with the extra-territorial application of human rights', in Perakis, S. (Ed.): *No More Permanent Than Temporary? Situations of Military Occupation and International Law*, Ostria Publications, Athens, p.111 et seq. (147).

Mitrou, L. (2018) *GDPR "X-ray": The Rights, Obligations and the Adaptability Problems*, 25 May, CNN Greece [online] https://www.cnn.gr/eidhseis/tag/74101/lilian-mhtroy (accessed 25 May 2019).

Mittleton, P. (2013) 'Health data protection: overview and practical issues', Paper presented at the *Conference Minutes on the 15 Years of the Hellenic Data Protection Authority*, Athens, Greece, to be published.

Nemitz, P. (2018) 'Constitutional democracy and technology in the age of artificial intelligence', *Royal Society Philosophical Transactions A*, DOI: 10.1098/RSTA.2018.0089 [online] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3234336 (accessed 25 May 2019).

Nielsen, R.K. (2017) *Where Do People Get Their News?, The British Media Landscape in 5 Charts*, 30 May, Medium, Oxford University [online] https://medium.com/oxford-university/where-do-people-get-theirnews-8e850a0dea03 (accessed 25 May 2019).

Panagopoulou-Koutnatzi, F. (2012) *On the Freedom of Blogs. New Technologies as a National, European and International Challenge to the Freedom of Dissemination of Ideas*, Sakkoulas Publications, Athens-Thessaloniki.

Panagopoulou-Koutnatzi, F. (2014) 'Review of historical sources and information protection', *Media and Communication Law [DiMEE]*, p.28.

Panagopoulou-Koutnatzi, F. (2016) 'Exercising control on independent authorities', *Applications of Public Law 2016*, p.253.

Panagopoulou-Koutnatzi, F. (2017b) 'The constitutionally defended protection in the case of release decision-making by the Hellenic Data Protection Authority (HDPA) for data provision', *Administrative Trial [DiDik]*, p.337.

Panagopoulou-Koutnatzi, F. (2019) 'Introduction', in Kanellopoulou-Boti, M. and Panagopoulou-Koutnatzi, F. (Eds.): *Bioethical Issues IV, Health Data and Genetic Data*, p.11, Papazissis Publications, Athens.

Ponsoldt, J.F. and David, C.D. (2007) 'A comparison between U.S. and E.U. antitrust treatment of tying claims against Microsoft: when should the bundling of computer software be permitted?', *Northwestern Journal of International Law and Business*, Winter, Vol. 27, pp.447–449.

Schulz, S. (2017) 'Art. 22: Automatisierte Entscheidungen im Einzelfall einschliesslich Profiling', in Gola, P. (Ed.): *General Data Protection Commentary [Datenschutz-Grundverordnung Kommentar]*, C.H. Beck-Verlag, Munich, Beck-online [online] https://beck-online.beck.de/?vpath=bibdata/komm/GolaKoDSGVO_1/EWG_DSGVO/cont/GolaKoDSGVO.EWG_DSGVO.a22.htm.

Vlachopoulos, S. (2007) *Transparency of State Actions and Protection of Personal Data. The Boundaries Between Disclosure and Secrecy in the Executive Powers*, Ant. Sakkoula Editions, Athens-Komotini, Greece.

Vlachopoulos, S. (2016) 'Access to public documents', in Kotsalis, L. (Ed.): *Personal Data, Analysis-Comments-Application*, Nomiki Vivliothiki, Athens, Greece.

Williams, J. (2005) 'Al Skeini: a flawed interpretation of Bankovic', *Wisc. Int'l. J.*, Vol. 23, No. 4, p.718 [online] https://hosted.law.wisc.edu/wordpress/wilj/files/2012/02/williams.pdf.

Notes

1 See Article 24 GDPR, which states that the controller will have to ensure and also demonstrate that the processing of the subject's data is in accordance to the GDPR.

2 For the understaffing problems of the Hellenic Data Protection Authority (HDPA), indicatively cf., HDPA (2015, p.22 et seq.).

3 ECtHR, Bankovic and others v. Belgium and 16 other states (Application no. 52207/99) 12 December 2001 and relevant commentary by Altiparmak (2004, p.213 et seq). In the said decision, the Court, by examining the question of the jurisdiction of the States, as understood in the context of admissibility as per in ECHR Article 1, laid down the jurisdiction of the State as the precondition to determine the question of the liability of States. In this way, the Court concluded that the jurisdiction of the Member States, under the concept used in ECHR Article 1, is essentially territorial, i.e., limited to the territory of the Member States (Para. 59). An exception is the exercise of effective control over a particular area outside the territory [cf. ECtHR, decisions Cyprus v. Turkey (Application no. 25781/94), 10 May 2001 and Loizidou V. Turkey (Application no. 15318/89), 18 December 1996]. More careful was the ECtHR later decision, Al Skeini and others v. the United Kingdom (Application no. 55721/07), 7 July 2011. In the said case, the question was raised as to whether the death of six Iraqis in the course of operations of British Forces occupying Basrah (which lay in the sector of responsibility of the British) is a violation of the ECHR. The Court held that all plaintiffs were under the jurisdiction of the United Kingdom and that, effective 1 May 2003 up to 28 June 2004, the United Kingdom had jurisdiction over the murder of civilians in the course of military operations of British soldiers in Basrah. In the Al Skeini case, the Court seems to having overturned its earlier case-law, abandoning the geographical criterion that it had adopted in the Bankovic case. The Court attempts to determine what effective control is, without defining such a concept, but leading, through its application to the general environment prevailing in Iraq at that time, to the recognition of occupation. It does not adopt the opinion that if there is effective control, this must refer to all the rights deriving from the ECHR, but it raises the application of only those rights directly related to such control (Para. 137). Cf. analysis of the decision by Marouda [2014, p.111 et seq. (147)] and Williams (2005).

4 The Federal Commissioner for Data Protection and Freedom of Information [Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit] in Germany and the Information Commissioner's Office in the United Kingdom.

5 In this context, Paras. 3, 8 and 10 of the Preamble to Directive 95/46/EC are of major importance, providing for the following: "(…) (3) whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded (…) (8) whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping

with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed (…) (10) whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the community."

6 Commission Document on the Protection of Individuals in relation to the Processing of Personal Data in the Community and Information security. COM (90) 314 final, 13 September 1990: "The diversity of national approaches and the lack of a system of protection at community level are an obstacle to completion of the internal market. If the fundamental rights of data subjects, in particular their right to privacy, are not safeguarded at community level, the cross-border flow of data might be impeded …." The legal basis for the Directive was Article 100a (now Article 95) of the Treaty.

7 Announcement of the Hellenic Data Protection Authority (HDPA), G/EX/5556/21 June 2018, clarifications regarding the certification of data processing acts in accordance with the GDPR.

8 The etymology of the word 'interpretation' by God Hermes (cf. Bampiniotis, 2002, the notion 'I interpret'), if considered that this God functioned as a mediator between Gods and humans, as an interpreter of the will of Gods to mortals.

9 Food for thought by Knight (2017).