The ELSA the Netherlands Law Review

Volume II

THE EUROPEAN LAW STUDENTS' ASSOCIATION

The ELSA the Netherlands Law Review

Volume II

The European Law Students' Association

THE NETHERLANDS

THE ELSA THE NETHERLANDS LAW REVIEW; VOLUME II

The publication may be cited as [2022] ELSA NL LR.

The ELSA the Netherlands' Law Review is a student-run, peer-reviewed journal of legal scholarship. The Review aims to serve as an academic forum that enables both students and legal professionals to analyse and discuss contemporary legal issues. While contributions are welcome from all members of the legal community, the Review, in particular, aims to provide law students and young lawyers with the opportunity to have their voices heard.

ISSN: 2772-6398 (e-version)

TABLE OF CONTENTS

The Derogation of Article 49(1)(d) of the GDPR as the Legal Basis for Direct Data Transfers to US Law Enforcement Agencies

Patrik Kovács[1]

Abstract

In 2018, the United States (US) Congress enacted the US CLOUD Act, which grants US law enforcement authorities the power to request the disclosure of personal data directly from service providers subject to US jurisdiction, regardless of the location of the data. The present tool facilitates the bypass of the existing mutual legal assistance treaty (MLAT) between the US and the European Union (EU) by US authorities. This might lead to several controversial questions since a proper EU legal basis does not exist for direct cooperation between US service providers; Article 48 of the General Data Protection Regulation (GDPR) excludes the enforcement of data production orders outside of an MLAT or other international agreements. However, some say that data transfers may be possible under Article 49(1)(d) of the GDPR if they are 'necessary for important reasons of public interest'.[2] This paper discusses the problem by reviewing the different opinions on the question and their theoretical outcomes and analysing the relevant primary and secondary sources.

[1] Graduated at Pázmány Péter Catholic University as a jurist in 2019. Started working as a paralegal at Bacskó Law Firm, Budapest then worked as an in-house paralegal at the Central Bank of Hungary until August 2021. Currently a student of the 'Law and Technology in Europe' Master's Programme at Utrecht University.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (GDPR), Article 49(1)(d).

1. Introduction

Traditionally, US law enforcement agencies have relied on the international process of mutual legal assistance for cross-border data requests,[3] although this might change in the future. In 2013, a US judge issued a warrant under the US Stored Communications Act (SCA), which is part of the Electronic Communications Privacy Act, that sought personal data, by Microsoft Ireland; therefore, the SCA warrant was incapable of seeking such information due to not having an extraterritorial effect.[4] This led to a lengthy legal dispute between Microsoft and the US government since Microsoft wanted to quash the SCA warrant. The case was dismissed in 2018 when the US enacted the Lawful Overseas Use of Data (CLOUD) Act regarding cross-border data requests to clarify the issue raised in the Microsoft case.

The CLOUD Act allows US authorities to request personal data directly from service providers, even if it is stored outside of the country.[5] This novelty may lead to potential conflicts with other legal systems if a service provider discloses personal data. Tensions may arise, especially with the EU and the GDPR. Article 48 of the GDPR seems to prohibit data transfers outside of the EU in the absence of a mutual legal assistance treaty (MLAT) or other international agreements.

However, some scholars argue that Article 48 of the GDPR does not prohibit data transfers if there are other provisions of the GDPR that can serve as a legal basis, for instance, if the transfer is necessary for important reasons of public interest. The present conflict of interpretations raises the question of whether Article 48 of the GDPR indeed blocks data transfers to third-country law enforcement agencies outside the scope of an MLAT or other international agreements. It is further crucial to consider whether it is conversely possible to disclose personal data based on other provisions of the GDPR, such as the *public interest* derogation of Article 49(1)(d).

To answer the question, Chapter two analyses the text of Articles 48 and 49 of the GDPR to determine in which situations their substantive provisions can apply. Then, Chapter three juxtaposes the opposing opinions of both sides while closely examining their arguments. Finally, Chapter four looks at the possible challenges that may originate from accepting these standpoints.

[3] Alexander A. Berengaut, Lars Lensdorf, 'The CLOUD Act at Home and Abroad – Addressing the challenges of cross-border data access by law enforcement on either side of the Atlantic' (2019) 20, no. 4 *Computer Law Review International* 111, 111.
[4] Jessica Shurson, 'Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law' (2020) vol. 28 Issue 2 *International Journal of Law and Information Technology* 167, 170.
[5] 18 U.S.C. Article 2713.

2. The substantive provisions of Articles 48 and 49 of the GDPR

Chapter V of the GDPR sets out the conditions for transfers of personal data to third countries or international organisations. Its first provision, Article 44, emphasises - as an overarching principle - that cross-border data transfers are lawful if other requirements of the GDPR apply as well, to guarantee the protection of data subjects.[6] In contrast, Articles 45 and 46 determine the criteria of transfers based on an adequacy decision or transfers subjects to appropriate safeguards.

In this case, the most relevant provision is Article 48 of the GDPR, which states that:

> Any judgement of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.[7]

Three main conditions can be identified in Article 48 of the GDPR, which must be fulfilled for the application of this provision: the expressions of (i) 'any judgement of a court or tribunal and any decision of an administrative authority'; (ii) 'international agreements'; and (iii) 'without prejudice to other grounds for transfer pursuant to this Chapter.'[8]

Condition (i) is clear: Article 48 applies to cross-border data transfers ordered by a third country's court or other authority and not for voluntary disclosures or requests from private parties.[9] However, some questions may arise concerning condition (ii): what kind of international agreements does Article 48 include? Does Article 48 apply to agreements that are outside of the scope of the GDPR, but within the scope of Union law? The aforementioned situation is typical in the case of international agreements dealing with criminal law or criminal procedure.[10] Since Article 48 of the GDPR covers data transfers to third country authorities under international agreements, the term 'international agreements' should be interpreted broadly.[11]

Finally, condition (iii) is the most cited expression of Article 48 that pertains to whether service providers can answer direct cross-border data requests under other provisions of the GDPR. This is because condition (iii) of Article 48 refers to the possibility of data transfers both under Articles 45-47 and under the

---

[6] European Data Protection Board 'Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679' EDPB (2018), 5.
[7] GDPR (n 2) art 48.
[8] David J Kessler, Jamie Nowak and Sumera Khan, 'The Potential Impact of Article 48 of the General Data Protection Regulation Cross Border Discovery from the United States' (2016) vol. 17 *Sedona Conference Journal* 575, 587-591.
[9] ibid 587.
[10] ibid 588.
[11] Christopher Kuner, 'Article 48. Transfers or disclosures not authorised by Union law' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR). A Commentary* (1st edition, Oxford University Press 2020), 835.

derogations of Article 49.[12] Therefore, this expression is a link to Article 49 of the GDPR, besides the first paragraph of Article 49, which sets out a layered approach for Chapter V: the derogations of Article 49 can be used only in specific situations when Articles 45-47 of the GDPR cannot be the legal basis of cross-border data requests.[13]

Since these derogations are for specific situations, when there is no other adequate protection for the data to be transferred, but 'the risks to the data subject are relatively small, or where other interests (public interests or those of the data subject himself) override the data subject's right to privacy'.[14] Hence, all these derogations must be interpreted restrictively to avoid the exception becoming the rule.[15]

Article 49 of the GDPR contains several derogations for specific situations. However, in their joint assessment, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) identified four relevant derogations from the possible options, which can form the legal basis for the data disclosures answering SCA warrants: (i) the transfer is necessary for important reasons of public interest (Article 49(1)(d)); (ii) the transfer is necessary for the establishment, exercise or defence of legal claims (Article 49(1)(e)); (iii) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent (Article 49(1)(f)) and (iv) the transfer is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject (Article 49(1)(g)).[16]

Of the aforementioned derogations, the most relevant is Article 49(1)(d), which authorises the accessing of cross-border data if it is 'necessary for important reasons of public interest'.[17] A subsidiary provision clarifies that the necessary public interest must be 'recognised in Union law or in the law of the Member State to which the controller is subject'.[18] This means that a public interest of a third country, such as a criminal investigation in which the data transfer is requested, is not sufficient for the application of this derogation.[19] Furthermore, the public interest must be an important one because Article 9(2)(g) refers to a *substantial* public interest as the basis for processing sensitive data.[20]

---

[12] Theodore Christakis, 'Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?' in Randal Milch and Sebastian Benthall (eds), *Building Common Approaches for Cybersecurity and Privacy in a Globalised World* (New York University School of Law 2019), 62.
[13] EDPB Guidelines (n 6) 5.
[14] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' WP29 (1998) D65025/98, 24.
[15] European Data Protection Board and European Data Protection Supervisor, 'Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence' EDPB and EDPS (2018) (EDPB and EDPS Initial legal assessment), 6.
[16] EDPB and EDPS Initial legal assessment (n 15) 6-7.
[17] GDPR (n 2) art 49(1)(d).
[18] ibid, art 49(4).
[19] EDPB and EDPS Initial legal assessment (n 15) 6.
[20] Christopher Kuner, 'Article 49. Derogations for specific situations' in Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR). A Commentary* (1st edn, Oxford University Press 2020), 849.

3. The different interpretations of Articles 48 and 49 of the GDPR

First, according to the interpretation of the EDPB and the EDPS, Article 48 determines the prerequisites of the enforcement of judgments and decisions of third country authorities under EU or Member State law, which corresponds with the title of the Article: 'Transfers of disclosure not authorised by Union law'.[21] The joint assessment highlights the legislator's intention to 'enshrine by law a protection against unauthorised access to personal data'.[22] Furthermore, as has been shown above, the public interest of a third country is not sufficient on its own to permit a derogation under Article 49(1)(d) of the GDPR; thus, the *public interest* derogation cannot serve as a legal basis due to the requirement of its recognition in Union law or Member State law.[23]

The EDPB/EDPS joint assessment dismisses the other possible derogations as well. Although the vital interest of the data subject could be a valid legal basis to answer SCA warrants, since there is an MLAT between the EU and the US, this derogation should not be used as a legal basis to transfer personal data.[24] Compelling legitimate interests cannot be a legal basis because the often joined protective orders of SCA warrants, which aim to maintain the secrecy of the data request, do not comply with the data processor's notification responsibilities stated in the last paragraph of Article 49(1).[25]

Consequently, according to the EDPB/EDPS joint assessment, service providers are not entitled to disclose or transfer personal data to US law enforcement agencies unless the transfer was requested through a mutual legal assistance procedure.[26] With this interpretation, the EDPB/EDPS joint assessment reiterates the former statement of the EDPB in the previously published EDPB guidelines of Article 49 that

> [i]n situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to an existing mutual legal assistance treaty or agreement.[27]

However, some scholars and practitioners state that this interpretation 'goes beyond the text of article 48',[28] and that this provision does not necessarily prohibit data transfers outside of an MLAT. For instance, according to some participants of research carried out by Sergio Carrera and Marco Stefan, the wording of Article 48 of the GDPR is unclear; hence, it is controversial whether it deters the disclosure requests of third-country law enforcement agencies or not.[29] The participants find Article 48 ambiguous, since, on the one

[21] EDPB and EDPS Initial legal assessment (n 15) 3.
[22] ibid 3.
[23] ibid 6.
[24] ibid.
[25] ibid 3.
[26] ibid.
[27] EDPB Guidelines (n 6), 5.
[28] Kuner, 'Article 48. Transfers or disclosures not authorised by Union law' (n 11) 830.
[29] Sergio Carrera, Marco Stefan, 'Access to Electronic Data for Criminal Investigations Purposes in the EU' (2020) *CEPS Paper in liberty and security in Europe* No. 2020-01, 24.

hand, it states that data transfers can be carried out if they are based on an international agreement, such as an MLAT, while, on the other hand, it seems that Article 48 is contradicting itself with the 'without prejudice to other grounds of transfer'[30] expression.[31]

Therefore, it appears that Article 48 of the GDPR implies that third countries' law enforcement data requests should comply with primary and secondary EU data protection law standards rather than authorising the disclosure of data.[32] The legislative history of Article 48 of the GDPR also strengthens this argument. Although Article 48 intends to limit the direct transfers of personal data, its phrasing is suitable since it is ambiguous. Thus, if the drafters of the Regulation had wished for service providers to generally refuse direct requests, they would have explicitly stated so instead of referring to mutual legal assistance treaties.[33]

Christopher Kuner, professor of law and co-director of the Brussels Privacy Hub at the Vrije Universiteit Brussel, also argues against the opinion of the EDPB and EDPS. He states that Article 48 of the GDPR does not necessarily block the direct requests of third-country law enforcement agencies since it allows data transfers under the other legal grounds of Chapter V.[34] According to Kuner, the EDPB views the provision of Article 48 as a duty of data controllers not to comply with data requests from third country law enforcement authorities outside of the scope of an international agreement.

However, the article only speaks about the recognition and enforcement of such orders and not about the duty of data controllers.[35] This means that the EDPB misinterprets the provision because the words of 'recognised' and 'enforceable' are used in their formal legal sense.[36] Accordingly, they refer to the international legal process of recognition and enforcement of foreign judgments by the national authorities and neither the 'recognition' nor the 'enforcement' by a private actor.[37] A reading of Article 48 in conjunction with Recital 115 of the GDPR seems to strengthen this understanding. Recital 115 of the GDPR states in its last part that:

> Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, *inter alia*, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.[38]

Moreover, mutual legal assistance treaties of data transfers between law enforcement agencies are outside the scope of the GDPR. Therefore, it may be questioned whether Article 48 of the GDPR gives any

[30] GDPR (n 2) art 48.
[31] Carrera et al. (n 29) 24.
[32] ibid.
[33] Christakis (n 12) 7.
[34] Kuner, 'Article 48. Transfers or disclosures not authorised by Union law' (n 11), 830.
[35] ibid.
[36] ibid 833.
[37] ibid.
[38] GDPR (n 2) Recital 115.

additional protection for data subjects because data processing as the result of a transfer without a proper legal basis under Article 6 of the GDPR would already violate the regulation.[39]

In its *amicus curiae*, the European Commission also identified the public interest derogation as a possible legal basis of data disclosures and the requirement of its recognition in Union law or Member State law. The Commission referred to the fight against serious crime and law enforcement international cooperation in that respect as a feasible interest because Article 83 of the Treaty on the Functioning of the European Union (TFEU) classifies several areas of crime with a cross-border dimension.[40] Kuner goes even further and states that there is no need to limit the important reasons neither for the crimes mentioned above nor for crime-fighting: the TFEU and other treaties contain other important values as well. Thus, the *public interest* derogation may be a proper legal basis in cases which involve these public interests.[41]

However, the *amicus curiae* of EU Data Protection and Privacy Scholars in the Microsoft case disconfirmed these opinions. Firstly, due to the obligation of the restrictive interpretation of the derogations, their application would lead to a broad interpretation, which would undermine the protection of personal data provided by the GDPR.[42] Additionally, as stated earlier, the public interest of third countries is not enough to comply with the provision of Article 49(4) of GDPR; it needs to be recognised by Union or Member State law. Nonetheless, such a broad interpretation of *public interests* as the one outlined, for instance, by Kuner, would undermine the limitation of cross-border data transfers because if a third country could bypass the MLAT process, Article 48 would lose its whole purpose.[43]

Finally, it is unlikely that service providers would be able to decide whether a warrant would serve the public interest.[44] As a consequence, the derogations of Article 49 could not apply 'without swallowing the privacy regime that the MLAT requirement is meant to protect'.[45]

[39] Kuner, 'Article 48. Transfers or disclosures not authorised by Union law' (n 11), 830.
[40] Brief for the European Commission on Behalf of the European Union as Amicus Curiae, *United States v. Microsoft Corp.*, 138 Supreme Court Reporter 1186 (2018), 15.
[41] Kuner, 'Article 49. Derogations for specific situations' (n 20), 850-851.
[42] Brief for EU Data Protection and Privacy Scholars as Amicus Curiae, *United States v. Microsoft Corp.* (2018), 138 Supreme Court Reporter 1186 (Amicus Curiae of EUDPPS), 10.
[43] ibid 12.
[44] Christakis (n 12) 15.
[45] Amicus Curiae of EUDPPS (n 42) 10.

4. Challenges of the Permissive Standpoint

The possible consequences of accepting the restrictive standpoint on cross-border data transfers between law enforcement agencies and others seem straightforward: private parties cannot answer direct requests of any third-country law enforcement authority, so these requests must go through a mutual legal assistance process. Nonetheless, accepting the permissive viewpoint and allowing service providers to comply with SCA warrants directly would imply many risks.

Firstly, under the US regulation, governmental entities are entitled to:

> Apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.[46]

The indicated provision creates conflicts with the rights of data subjects granted by the GDPR. On the one hand, Article 13(1)(f) of the GDPR obliges the data controller to inform the data subjects about data transfers of their personal data to a third country to ensure the ability of the data subjects to exercise their rights. Data controllers may also be obliged to notify the competent data protection authority of the transfer, according to Article 49(1) of the GDPR. Furthermore, the data subjects have the right of access under Article 15(1) to obtain information on whether their personal data is being processed or not, although the preclusion of notifying them about a transfer would undermine the affected data subject's right.[47]

On the other hand, according to Article 21(1) of the GDPR, the 'data subject shall have the right to object (…) at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1) (…)'.[48] In case of an objection, the controller can no longer process the data unless it demonstrates that its compelling legitimate interests override the data subject's interests, rights and freedoms.[49] Subsequently, while the verification of this condition is pending, the data subject can request the restriction of processing their personal data.[50] However, a preclusion of notification would also undermine this safeguard.[51]

Additionally, the preclusion of notifying data subjects about SCA warrants may threaten the fundamental rights of data subjects. For example, the substantive privilege protections, such as the protection of legal professional privilege could be undermined since the lack of notice of an SCA warrant would deprive

---

[46] 18 U.S.C. Article 2705(b).
[47] Brief for European Company Lawyers Association as Amicus Curiae, *United States v. Microsoft Corp.* (2018), 138 Supreme Court Reporter 1186 (Amicus Curiae of ECLA), 18.
[48] GDPR (n 2) art 21(1).
[49] ibid.
[50] ibid, art 18(1)(d).
[51] Amicus Curiae of ECLA (n 47) 18.

the lawyers' and their clients' right to protect the privileges 'that attach to the data sought by the warrant'.[52] Even if the level of protection varies among Member States, the recognition of privileges is common in Member States' domestic law as well as EU law.

As Advocate General Kokott noted in the *Akzo Nobel Chems v Commission* case:

> Legal professional privilege not only serves to ensure the rights of defence of the client but is also an expression of the lawyer's status as an independent legal adviser and 'collaborat[or] in the administration of justice' who gives legal advice 'to all those who need it'.[53]

However, the cross-border transfer of privileged materials, especially in the absence of a proper notification, undermines the protected privilege because the lawyer would not be able to give appropriate advice to their clients nor provide any safeguards to take the necessary steps to secure the rights provided by EU law.[54] In addition to the aforementioned points, companies complying with SCA warrants may face serious financial consequences.

Firstly, companies that fail to comply with the provisions of the GDPR can receive administrative fines under Article 83 of the GDPR; they can be subject to fines of up to 10,000,000 euros or up to 2% of their total worldwide annual turnover.[55] However, in cases of infringement of 'the transfers of personal data to a recipient in a third country or an international organisation pursuant to Article 44 to 49',[56] they can face an administrative fine of up to 20,000,000 euros or up to 4% of their total worldwide annual turnover.[57]

Secondly, according to Article 82(1) of the GDPR, '[a]ny person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered'.[58] Therefore, companies might face administrative fines and civil liability actions as well, filed by data subjects affected by an SCA warrant.

---

[52] ibid 19.
[53] Case C-550/07 P *Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v European Commission* [2010] ECR I-08301, Opinion of AG Kokott, para 148.
[54] Amicus Curiae of ECLA (n 47), 20.
[55] GDPR (n 2) art 83(4).
[56] ibid art 83(5)(c).
[57] ibid.
[58] ibid art 82(1).

5. Conclusion

As has been demonstrated, there is a dispute in the interpretation of Articles 48 and 49 of the GDPR. While some institutions of the EU, as well as legal scholars, state that Article 48 blocks the bypass of a mutual legal assistance treaty, others tend to say that this provision does not stop direct data transfers as responses to SCA warrants. In finding a solution for this issue, Chapter two analysed the substantive provisions of Articles 48 and 49 of the GDPR and identified the main conditions of the former for its application. Subsequently, having found the *public interest* derogation under Article 49(1)(d) of the GDPR to be the most relevant, this paper then determined the requirements for its application.

Chapter three examined the opposing opinions on the topic and the arguments that are often propounded. While both sides have strong arguments, the application of Article 49 derogations would mean a too broad interpretation. The public interests of third countries are not enough in themselves to comply with the provision of Article 49(4) of GDPR, and service providers are not able to decide whether a warrant serves the public interest. Hence, the derogations of Article 49 are not applicable in case of direct data requests.

Nonetheless, the picture would be incomplete without an assessment of the kind of risks a permissive approach entails; Chapter four examined these questions. As may be seen, many issues may arise: the rights of data subjects granted by the GDPR and the basic principles of the Regulation could be undermined, conflicts would emerge concerning the privilege of the legal profession, and companies may face high financial risks.

In light of the foregoing arguments, it is ascertainable that since the derogations of Article 49 of the GDPR must be interpreted strictly, and the emerging risks would override any important public interest, transferring personal data as an answer to a direct data request of a third-country authority would not comply with the GDPR.

THE DESIRABILITY OF DATA PROTECTION MECHANISMS VIS-À-VIS THEIR EFFECTIVENESS & GENERATIVITY:

A Search for Improved Regulatory Solutions to the GDPR in the AI Regime

Carmen Enciso[1]

Abstract

The Internet encompasses tens of thousands of networks operating independently, interlinked by means of multi-lateral and bi-lateral data exchange agreements. The present article will consider the question of how to best regulate the extent and means of data protection in the European context, zooming in particular on the un-/desirability for data protection by design mechanisms vis-à-vis their effectiveness and generativity. It will be argued here that although the GDPR was a clear advancement from its preceding instruments, future demands of data protection and generativity in the digital economy will require a clearer and more risk-based regulatory framework, putting scalable data protection mechanisms of risk management and data stewardship (rather than overly relying on consent and notice mechanisms), built-in privacy mechanisms (PETs), and industry incentives for generative privacy models at its centre. A hybrid model of public and private stakeholders has been argued to be the best fit for developing the updated framework in the upcoming decade, shifting away from the duality of 'personal' and 'anonymous' data, and implementing instead a risk-based classification system of data similar to that taken in the AI Act regulatory approach. Lastly, this article proposed that market initiatives seeking to promote decentralized cloud services and data stewardship models should be much more incentivised in the market by lawmakers and regulators alike. The latter measures may potentially provide simple infrastructure solutions on the internet layer that could ultimately both improve market generativity for tech firms as well as allow data subjects to gain more effective control over their data in the upcoming decade. In short, we must take Ostrom's Law to heart, and understand that 'governance models which work in practice can also work in theory.'

[1] Carmen Enciso is completing her double YUFE and European Law School Tracks with specialization courses in Law&Tech at Maastricht University. She has been involved in various moot courts, winning Best Team, Written Submission and Speaker at the 2020 ICL-ELSAMCC, and second place at the 2021 Nuremberg Moot Court. At the T.M.C. Asser Institute, Carmen assists the Director of the Centre for the Law of EU External Relations (CLEER). She also runs the EMaas Law Review as its present Director and her publications include articles on the new hacking powers under the *Wet Computercriminaliteit III*.

'It is essential for the success of future legal protection against "information-induced harms" that [future alternative frameworks to the current one of personal/anonymous data duality with high-intensity of positive compliance obligations] are grounded in a better understanding of information and its relationship to people, in well-understood and articulated problems that it intends to solve and in the fully mapped mechanics of the information-induced harms it intends to avert.'

Nadezhda Purtova[2]

1. Introduction

The creature that is the internet today reflects many idiosyncratic choices about how to build a global network – choices, that we should never take for granted, or, for independently made from the interests of network actors.[3] The same applies to the Web, that 'collective hallucination' on which to run on the internet.[4] We must always remember those choices did not have to be made that way. We could have ended up with a set of networks similar to the legacy 20th-century telephone systems. The folks who came up with Internet protocols were certainly not well-funded, nor had they any particular expectation of enriching themselves from it, *á la* San Fran style. In that sense, there is a 'commons', that partially exists via modest government subsidies that fund research projects to build the internet.[5] Yet the rest is left up to connected users so as to figure out for what exactly is it that they wish to use a network.

The essence, thus, of the Internet, is a set of protocols that allows any interconnected points of presence to communicate with one another and to not have to overly concern themselves about how exactly it is that the bits will work their way from point A to point B. As is well known, for Zittrain, the inherent generative nature of this 'essence' meant that such technologies be designated as 'generative technologies.'[6] According to him, the core feature of a generative technology is that it welcomes contributions from nearly any corner of the Earth and applies them to the Internet. Meaning, that upon becoming a point of presence on the Internet i.e., upon beginning to exchange bits with other millions of entities (servers), where the latter seek to claim a path to your front door and obtain your bits, your 'data', there can be no gatekeeping from any third-parties which can be set up as a form of top server. From a purely utopian perspective, one can see the appeal of this argument in its extreme, and the need for safekeeping its observance in internet governance models. For instance, when it comes to data protection regulation and the call for an improved regulatory promotion of data exchange and re-use.

---

[2] Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) *10 Law, Innovation and Technology* 40.
[3] Bruno Latour, 'On Actor-Network Theory: A Few Clarifications' (1996) *47 Soziale Welt* 369.
[4] Jonathan Zittrain, 'The Internet Is Rotting' (*The Atlantic*, 30 June 2021) <www.theatlantic.com/technology/archive/2021/06/the-internet-is-a-collective-hallucination/619320/> accessed 3 May 2022.
[5] CERN, 'The Birth of the Web' (*Conseil Européen pour la Recherche Nucléaire*, 2020) <https://home.web.cern.ch/science/computing/birth-web> accessed 3 May 2022.
[6] Jonathan Zittrain, 'Law and Technology: The End of the Generative Internet' (2009) *52 Communications of the ACM* 18.

Yet, in practice, can we truly link the implementation of data protection by design mechanisms (e.g., through the General Data Protection Regulation or 'GDPR')[7] to a decline in derived demand for data exchange and re-use directly impacting EU MS networks' choices to interconnect? For instance, if we compare these networks to those of non-MS? Meaning, are data protection mechanisms and the promotion of generativity ontologically incompatible? Secondly, are the current data protection mechanisms in place effective, vis-à-vis their set out privacy objectives, in the face of digital market demands? Several researchers have answered these questions in the negative, and this discussion will agree with such a view on the two issues at hand.[8] Firstly, it will be argued that although the GDPR was a clear advancement from its preceding instruments,[9] future demands of data protection in the digital economy will require a clearer and more accurate regulatory framework,[10] that puts scalable data protection mechanisms (rather than overly relying on consent and notice mechanisms), built-in privacy mechanisms (PETs), and industry incentives for generative privacy models at its centre. Secondly, a hybrid model of public and private actors will be argued to be the best fit for developing an updated framework for data protection, away from the duality of 'personal' and 'anonymous' data with high-intensity of positive obligations so as to better seek scalable solutions capable of tackling the reality of the industry and data subjects today. Thirdly, inspiration will be drawn from the AI regulatory framework in the EU, in order to propose regulatory solutions to these two issues of regulatory effectiveness and generativity assurance of data protection by design mechanisms in the future. In tackling these questions, this discussion will seek to ultimately determine arguments for and against the desirability of specific data protection by design mechanisms vis-à-vis generativity of the internet. In short, we must take Ostrom's Law to heart, and understand that 'governance models which work in practice can also work in theory.' [11]

2. The Current EU Data Protection Framework under the GDPR

Initially, data protection rules were codified in EU primary law in 2009, upon the coming into force of the Lisbon Treaty. Under the TFEU, the provision under article 16 specifically guarantees the right to data protection, outlining procedural rules for the legislative tackling of its regulation.[12] Additionally, two provisions can be found in the EU Charter of Fundamental Rights which guarantee the privacy and data

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (GDPR).
[8] European Parliament and Directorate-General for Parliamentary Research Services, *The Impact of the General Data Protection Regulation on Artificial Intelligence* (EU Publications Office 2021); Purtova (n 2); Bendik Bygstad, 'Generative Innovation: A Comparison of Lightweight and Heavyweight IT' (2017) *32 Journal of Information Technology* 180; Ran Zhuo, Bradley Huffaker and Shane Greenstein, 'The Impact of the General Data Protection Regulation on Internet Interconnection' (2021) *45 Telecommunications Policy* 102083.
[9] Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) *4 International Data Privacy Law* 250.
[10] Lee A Bygrave, 'Hardwiring Privacy' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of the Law and Regulation of Technology* (Oxford University Press 2017).
[11] Lee Fennell, 'Ostrom's Law: Property Rights in the Commons' (2011) *5 International Journal of the Commons* 9.
[12] Consolidated Version of the Treaty on the Functioning of the European Union [2007] OJ C 326, art 16.

protection of 'everybody', that is, articles 7 and 8. Both of these are closely intertwined,[13] with their broad reach covering both the retention and processing of data.[14] For the present discussion, a relevant condition under article 8(2) of the Charter is that the processing of data is made on the 'basis of consent or another legitimate legal basis.' In addition, the provision in article 16 TFEU –which reflects the right to data protection codified in article 8 of the Charter–, explicitly states 'everyone' and thus extends the scope of the right to all (natural) persons i.e., not only EU citizens. More importantly, at the core of the present discussion is the instrument of the Regulation (EU) 2016/679 or GDPR, applicable since May 2018. Notably, the legislative process of this instrument was both arduous and subject to lengthy legislative debates.[15] The GDPR is – arguably– a complex model of regulation, with a broad range of conditions for natural persons covered therein e.g., from requiring consent for the 'processing of personal information' to securing portability of data, requiring companies to disclose data breaches within seventy-two hours of 'becoming aware', and appointing Data Protection Officers. An important advancement in the GDPR has been the rejection of the 'age-blind' approach to data subjects of the preceding framework. However, for the present discussion, an emphasised focus will be given to articles 2, 4, 6 and 7 GDPR, as they are of particular relevance.

Firstly, under article 2 GDPR we find the material scope of the instrument i.e., one only applying to the scope of 'personal data' covered under the GDPR. The latter notion of 'personal data' involves that which is either processed by automated or unautomated means and which may or may not be part of a filing system. The GDPR thus does not cover the processing of 'anonymous data' – meaning, this category of data does not trigger the application of the GDPR.[16] Scholars such as Purtova have already pointed out the inviability in the future of a regulatory model based on the duality of personal versus anonymous data, in a world where all data should increasingly be regarded as 'personal' and where scalable protection solutions would be preferable over the current high-intensity model of protection.[17] This is particularly the case where big data are progressively exploited and where identifiability of such data is increasingly feasible, as underpinned both in the Article 29 Working Party guidelines and in recent CJEU case law.[18]

---

[13] Court of Justice of the European Union, C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert*, Court Judgement, 9 November 2010, ECLI:EU:C:2010:662, para 52.
[14] Court of Justice of the European Union, C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, Court Judgement, 8 April 2014, ECLI:EU:C:2014:238, para 29.
[15] The period of revision of the Data Protection framework began in January of 2012, with the GDPR proposal. In October of 2013, the Committee of LIBE of the EP held a vote on the Draft Report of Jan P Albrecht. In March, 2014 the Report of LIBE was adopted by the EP. In June, 2015 the EC agreed on General Approach and in November, 2015 it established its negotiating position. In December, 2015 agreement in trialogue was reached by the EP and the EC. In April, 2016 the EC adopted the EC Position and the LIBEC voted on Recommendation (for second reading), and the EP adopted the GDPR. Finally, in April of 2016 the GDPR was signed.
[16] GDPR, recital 26.
[17] Purtova (n 2); Koops (n 9); Catalina Goanta, 'Big Law, Big Data' (2017) *Law and Method.*
[18] ibid; Article 29 Working Party, *Opinion 4/2007 on the concept of personal data* (20 June 2007); Court of Justice of the European Union, C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, 19 October 2016, ECLI:EU:C:2016:779.

Secondly, under article 6 GDPR conditions for the lawfulness of processing of data are enlisted, including, at least, one of the following: consent; necessity of processing for the performance of a contract; necessity of processing for compliance with a legal obligation to which the Controller is subject; necessity of processing for the protection of the vital interests of the data subject or some other natural person; necessity of processing for the purposes of the legitimate interests pursued by the Controller or by a third party except where such interests are overridden by the interests/fundamental rights and freedoms of the data subject in particular where the data subject is a child. Lastly, under article 4 GDPR we find both the definition for 'personal data' and 'consent' and under article 7 GDPR the conditions for consent are codified. In the following section, a closer look at these provisions will be taken with respect to the first research question on the effectiveness of the consent mechanism under the GDPR.

3. The GDPR Consent Mechanism: Challenges to its Effectiveness & Proposed Solutions

In line with the intended objectives of the lawmakers in the GDPR, consent was clearly defined in the Regulation. The provision in article 4(11) GDPR defines 'consent' of data subjects as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.' The interpretation of the present GDPR definition of consent can be further clarified when compared to the provision in article 2(h) of the preceding European Directive 95/46/EC whereby 'the data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'[19] The inclusion of the terms 'unambiguous indication' and 'clear affirmative action' in the new definition entails that in order for consent to be established, there must be a conscious and positive act so as to assist the relevant Controller to prove that the consent was validly granted.

Now, under article 6(1) GDPR a lawful basis for any type of data processing is required, including the collection, use, and disclosure of personal data. As mentioned above, under articles 6(1)(a) and (b), two of the lawful bases for the processing of non-sensitive personal data are user consent and contracts. Consent may be classified as being one of three types: take-it-or-leave-it, opt-out, and opt-in.[20] Any lawmaker designing a data protection framework such as the GDPR must decide which type of consent is most appropriate for which usage and type of data (albeit here only if data continues to be classified as being either 'sensitive', 'personal' or 'anonymous').

[19] Directive (EU) 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ L 281.
[20] Chris Jay Hoofnagle, 'Designing for Consent' (2018) *7 J. Eur. Consumer & Mkt. L.* 162.

In practice, the GDPR expects companies to request the *use and collection* of personal data via the service's terms and conditions. The lack of actual effectiveness of such lengthy texts is self-explanatory, however, and so will be that of the actual consent of users in the context of this discussion. Where non-sensitive data are concerned, the GDPR also expects firms to ask users to agree via a contract to the processing of such data needed for the performance of the contract. Where sensitive data are concerned, the GDPR does not permit firms to require such agreement from users. In other words, the GDPR limits the 'take-it-or-leave-it' approach for personal data collection and usage to that which is not sensitive and which is needed for the performance of the contract. Alternatively, when consent is the lawful basis for data processing, it must be opt-in. Moreover, where it concerns sensitive data, consent will be explicit.

Although the GDPR seems to find the differentiation of sensitive versus non-sensitive data useful to require opt-out and opt-in consent, or non-explicit and explicit consent, there are clear problems as to how we may limit the boundaries of what we define 'sensitive personal data.' Even more so, the question future regulators should ask is whether data protection frameworks should be based on a duality of personal versus anonymous data, in an era where the monetisation of monitoring is filled with financial incentives for developers to increase data identifiability, and very few ones for either deterring it or decentralising it.[21] Indeed, this paper argues that future regulations of data protection will have to revisit financial incentives for the privacy objectives intended. The current GDPR attempts to prohibit unreasonably discriminatory and coercive financial incentives, but fails to promote more those that would support its ultimate privacy goals in an effective and generative manner in which developers and conglomerates of the industry would likely follow. [22] Not only that, but the scalability of remedies and the appropriate granularity of consumer choices will have to be revised, as the industry evolves.[23] In conclusion, informed consent as the principal means for data protection and privacy cannot be maintained in the future. This is particularly the case if we consider, for instance, behavioural targeting by companies.[24] For these reasons, this paper calls on regulators and lawmakers to instead promote built-in privacy using bottom-top approaches,[25] combining the industry and the public sector to protect data instead and decentralise its processing and storage. Indeed, the use of

[21] Bygrave (n 10); Scott J Shackelford and Rachel Dockery, 'Governing AI' (2020) *30 Cornell Journal of Law and Public Policy* 279.
[22] Here ANT could be useful in this context as a means to analyse the effectiveness of the current data protection model, for it attempts to study the very nature of societies by means of including non-human and non-individual entities as actors. Under an ANT frame, thus, an emphasis would be put on evaluating the actual performativity of governance instruments such as the GDPR. See here Latour (n 3); cf Anthony Amicelle, Claudia Aradau and Julien Jeandesboz, 'Questioning Security Devices: Performativity, Resistance, Politics' (2015) *46 Security Dialogue* 293; Didier Bigo, 'The (In) Securitization Practices of the Three Universes of EU border control: Military/Navy–Border Guards/Police–Database Analysts' (2014) *45 Security Dialogue* 209.
[23] For examples on how this could be achieved for an improved data protection model, for instance in the education sector, see David C Lane and Claire Goode, 'Open For All: The OERu's Next Generation Digital Learning Ecosystem' (2021) *22 The International Review of Research in Open and Distributed Learning* 146; in the health sector, see Rüdiger Rupp and others, 'Das Deutschlandweite, Webbasierte ParaReg-Register zur Lebenslangen Dokumentation von Querschnittgelähmten – Datenmodell, Rechtlich-Ethische Voraussetzungen und Technische Implementierung' (2021) *83 Das Gesundheitswesen* S18.
[24] Frederik Z Borgesius, 'Informed Consent: We Can Do Better to Defend Privacy' (2015*) 13 IEEE Security & Privacy* 103.
[25] Trinh V Doan and others, 'Towards Decentralised Cloud Storage with IPFS: Opportunities, Challenges, and Future Directions' (2022) *Cornell University ArXiv*.

decentralised networks to better accomplish the objectives of emerging privacy regulations is already being looked at by initiatives in Europe, for instance, by GAIA-X.[26]

4. The Changing Face of the Effectiveness of the GDPR Consent Mechanism in the Pandemic-Amplified Demand for a Generative EU Environment

As is well known, the growth of the IoT allows for an exceptional degree of integration of information,[27] giving the chance to cross-match novel and current tech and data (so-called 'interoperability') and to navigate with increasing means and connected users (i.e. 'scalability') via the usage of distributed systems (so-called 'cloud computing').[28] Big data and AI have utterly changed the rules of the game, increasing generative options for both interoperability and integration and giving life to wholly new industry sectors in the name of Foucauldian efficiency. In that context, whilst not a superpower in AI development –such as the PRC or USA–,[29] the European Union has gained a position as an effective centre for data protection and AI regulation.[30] Such a position has also been promoted by the Court of Justice of the EU, for instance, by reaffirming the primacy of the European framework of data protection over those systems offering less protection.[31]

Under that setting, aside from the release of the smartphone back in 2007, the year 2020 was arguably a turning point in the development of internet governance. Though the COVID-19 pandemic's full impact thus far can hardly be assessed at the time of writing of this article given its novelty, the pandemic has certainly forwarded a shift in digital behaviour of companies and users, for instance in the creation of new online habits and trends, the so-called 'one-click' and 'click-collect' shopping, the overall switch to remote working, learning, service and tracking e.g., in the health sector. A fundamental consequence of this turning point is that EU society seems to finally have caught up to an undeniable reality: standards and behaviour of digital industry players need to be more appropriately and realistically aligned with the expectations of our fellow EU private citizens and companies. In other words, they must be aligned with those values, on which the EU legal regime, that 'collective hallucination' that is much more than a set of rules or its players, stands upon.

---

[26] Arnaud Braud and others, 'The Road to European Digital Sovereignty with Gaia-X and IDSA' (2021) *35 IEEE Network* 4.
[27] Alessandro Acquisti, Laura Brandimarte and Jeff Hancock, 'How Privacy's Past May Shape its Future' (2022) *375 Science* 270.
[28] Zed Zulkafli and others, 'User-Driven Design of Decision Support Systems for Polycentric Environmental Resources Management' (2017) *88 Environmental Modelling & Software* 58; Mitsuyoshi Imamura and Kazumasa Omote, 'Toward Achieving Unanimity for Implicit Closings in a Trustless System' in Xingliang Yuan, Wei Bao, Xun Yi, Nguyen Hoang Tran (eds), *Quality, Reliability, Security and Robustness in Heterogeneous Systems* (Springer International Publishing 2021); Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US footsteps?' (2017) *26 Information & Communications Technology Law* 146.
[29] Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (Houghton Mifflin 2018).
[30] European Parliament, *The Impact of the General Data Protection Regulation on Artificial Intelligence* (European Parliament Think Tank 2020); European Parliament and others, *A Comparison between US and EU Data Protection Legislation for Law Enforcement Purposes* (European Parliament 2015); Emmanuel Salami, 'An Analysis of the General Data Protection Regulation (EU) 2016/679' (2017) *SSRN Electronic Journal* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2966210> accessed 3 May 2022.
[31] Court of Justice of the European Union, *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, 6 October 2015, ECLI:EU:C:2015:650.

However, a consistent and prevalent flaw in the GDPR regulatory framework seems to be its basis on the so-called duality of data: 'personal' vs 'non-personal data.' For if we look at who the larger players are, in terms of Application Programming Interfaces ('APIs') and Systems Tool Kits ('STKs'), for instance, they are generally concentrated in a few players. For instance, this is well illustrated in the depiction below mapping the global market and ecosystem of COVID-19 response app development. The depiction below (Figure 1) reflects the importance of securing a generative environment unhampered by inadequate regulatory mechanisms. Therein we see the app development responsiveness across countries during the COVID-19 pandemic, where all app version updates account for release dynamics in response to the pandemic needs of the market. This responsiveness was enabled by ensuring generative conditions provided by platforms were in place, so as to allow for unsolicited innovation.[32]

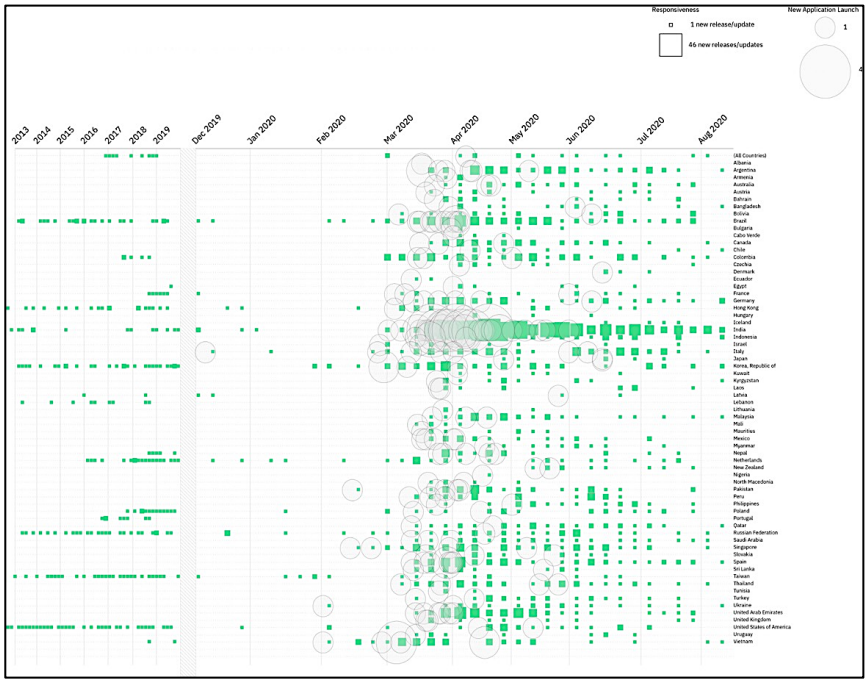

FIGURE 1: Responsivity of COVID-19-related Android app developers by country (from 2013 to August 2020). The circles are the initial releases (i.e., app launches); the squares are any additional releases (i.e., app updates); then scaled by the total number of releases.[33]

As a result, three immediate inferences come to mind. Firstly, that ensuring data protection mechanisms do not hamper the fostering of a generative environment is key to the building of a competitive internal market that is able to adjust to societal needs, such as those faced in the pandemic. Secondly, that the current model of ensuring data cross-matching is only performed with the consent of individual data right owners, will not be the most adequate data protection by design mechanism where it is dictated by a 'personal data' duality model of the GDPR material scope and where the market distribution is cumulated in a small number of players. Thirdly, that the challenges presented by growing AI development and re-/use of data

[32] Michael Dieter and others, 'Pandemic Platform Governance: Mapping the Global Ecosystem of COVID-19 Response Apps' (2021) *10 Internet Policy Review* 1; Zittrain (n 6).
[33] Dieter and others (n 32).

should serve as further incentives for reviewing regulatory solutions to the two issues discussed in the present article: the need to improve the effectiveness of data protection mechanisms whilst still ensuring their generativity vis-à-vis market and societal demands. Several reforms thus seem necessary: a shift from individual consent mechanisms to a data stewardship model, a shift from a dual model of 'personal' and 'anonymous' data model to a scalable model instead of 'personal data', and a framework of risk and harm of data re-/use with a greater focus on its impact and transparency.[34] The question, therefore, is begged: can we find existing alternatives for conceptual and regulatory frameworks and mechanisms in other models out there, which would more appropriately serve as effective and generativity-securing mechanisms for data protection in the long run? The present discussion believes there are, and rather than re-inventing the wheel, it will instead draw from learned regulatory lessons of the digital constitutionalism process experienced by the EU in the past decade. Namely, it will focus on the proposed Artificial Intelligence Regulation ('AI Act')[35] as a key alternative model of reference for the reforms herein recommended.

5. Seeking More Effective & Generative Mechanisms for Data Protection: the AI Act as an Instrument of Legal Portability of Values

There has been an increasingly stark regulatory push for EU digital governance in the last ten years, with policies building on prior legislation (regulating e-Commerce and the information society) and widening its scope to meet rapidly changing market and societal demands. New policies have sought to update distinct legal regimes (e.g., IP law and rules on content moderation and intermediary liability), whilst also creating entirely new regulatory models that truly match technological developments (e.g., regulation of AI technologies through the AI Act, data protection via GDPR). Such digital constitutionalism seeks to build normative frameworks to tackle 'platformisation' and 'datafication',[36] protect EU values and fundamental rights, and check and balance the market imbalances created by actors in the online environment. In that sense, 2022 is on its way to becoming a turning point for European digital governance. The Digital Services Act ('DSA'),[37] Digital Markets Act ('DMA')[38] and AI Act are likely to cause waves beyond EU terrains. Yet, for the EU strategy with regards to data protection to be implemented effectively, an improved coordination of the enforcement mechanisms therein will have to be secured. This discussion will firstly identify the features and mechanisms under the proposed AI Act which could serve as inspiration for an eventual reform

[34] Fred H Cate and Rachel Dockery, 'Artificial Intelligence and Data Protection: Observations on a Growing Conflict' (2018) *J Law Econ Regul* 1.
[35] 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 COM (2021) 206 final ('AI Act').
[36] José Van Dijck, 'Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology' (2014) *12 Surveillance & Society* 197.
[37] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC ('DSA').
[38] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) ('DMA').

of the GDPR. It will argue that there is an untapped potential and symbiosis between the two instruments for generating regulatory solutions in future GDPR reforms when it comes to improving the effectiveness and generativity of its data protection mechanisms in the upcoming decade.

In 2021, the European Commission presented a proposal for an Artificial Intelligence (AI) Regulation, the so-called AI Act. The Commission hoped to address the risks associated with the commercialization and use of AI. The AI Act follows the logic of product safety regulation and is aimed at preventing the realisation of risks. The draft regulation is primarily aimed at 'providers.' In short, under article 3(1)(2) AI Act, these are the producers/developers who bring AI into the market. This draft regulation also applies to others in the chain, such as 'importers',[39] 'distributors',[40] and 'users.'[41] In particular, the framework seeks to ensure that these standard addressees only place and use products on the EU market where they meet the product standards set in, or where they effectively implement, the draft regulation.[42] The present discussion will critically discuss the AI Act, its relationship to existing product safety law and the regulatory inspiration it provides for generating improved alternatives to data protection mechanisms.[43]

The AI Act has three main objectives: firstly, it seeks to ensure that AI systems placed and used in the EU market are safe and observant of EU principles and fundamental rights; secondly, it aims to ensure legal certainty is achieved to further investment and innovation; and thirdly, it hopes to decrease market fragmentation by developing a single market with legitimate, secure and trust-building AI systems.[44] There are three aspects of the AI Act which could be of particular relevance to the data protection mechanisms discussion, in particular when it comes to creating an alternative regulatory framework to the current 'personal data' duality model with high-intensity of positive obligations under the GDPR today.

Firstly, the definition of AI systems under article 3(1) AI Act, seems considerably broad, which means the Regulation will have to apply to a broad spectrum of 'systems', some of which may perhaps not be related to AI at all e.g., certain algorithms that neither use autonomous action nor independent learning. This could pose both difficulties and advantages for future implementation of the Regulation, though at present it is too early to say. However, for the purposes of the data protection discussion, it is generally best that data protection and transfer governance debates do not limit their scope to only personal and non-personal data

[39] AI Act, art 3(1)(6).
[40] ibid, art 3(1)(7).
[41] ibid, art 3(1)(4).
[42] ibid, ch V.
[43] Esther Amayuelas, 'La Responsabilidad de los Intermediarios en Internet ¿Puertos Seguros a Prueba de Futuro?' (2020) *12 Cuadernos de Derecho Transnacional* 808; Giancarlo Frosio, 'Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility' (2017) *SSRN Electronic Journal*; European Commission, *Hosting Intermediary Services and Illegal Content Online: an Analysis of the Scope of Article 14 ECD in Light of Developments in the Online Service Landscape: Final Report* (Publications Office 2019); Aleksandra Kuczerawy, 'From "Notice and Take Down" to "Notice and Stay Down": Risks and Safeguards for Freedom of Expression' in Giancarlo Frosio (ed), *The Oxford Handbook of Intermediary Liability Online* (Oxford University Press 2020).
[44] Explanatory Memorandum to the AI Act, 3.

per se, but rather take a wider spectrum of scalable categories. Therefore, in that context, this broader material scope of the AI Act could provide many advantages both for effectiveness and generativity purposes.[45]

Secondly, another important aspect of the AI Act is its territorial scope. The Regulation would cover providers of AI systems established outside the EU, where the output of the AI system is used in the EU.[46] The clear rationale behind such an ample scope is likely to cover situations where an AI system uses standalone SW which runs somewhere in the cloud in e.g., PRC or US, but is used by 'users' in the EU. Thirdly, the AI Act would be implemented on the internal market basis under Article 114 TFEU, aiming at maximum harmonisation.[47] While it does not harmonise private law remedies for, e.g., consumers, it does apply *in addition to, and on top of,* existing rules and principles on data protection (GDPR), consumer protection (e.g., the Directive 2019/771 and Directive 2019/770) and non-discrimination (EU Charter).[48]

It follows, that the initial significance of this instrument for the purposes of data protection is that by means of the wide material scope (entailed by the broad definition of 'AI system' in the Act), the far-reaching territorial scope (which will cover any provider under the conditions aforementioned, even where they are outside the EU), and the supplementary application of the AI Act on top of existing EU data protection and fundamental rights protection instruments, we have, *prima facie*, a well-laid portable legal device for the export and securement of EU values and principles in the internal market, and perhaps, beyond. This feature has been lacking in the legal instruments of the EU digital legislative strategy thus far, with few exceptions, though this is certainly changing, if we allow ourselves to remain cautiously optimistic given regulatory events of recent years.

Now, if the AI Act could act as a form of regulatory 'portable device' to export onto other digital governance frameworks, what is it that we could export and implement internally in our market and abroad, in the context of data protection? For one, the risk-based approach of the AI Act could surely provide us with inspiration for a more effective mechanism of data protection through a risk and harm framework of data re-/use with a focus on its impact and transparency.[49] This would also align well with the herein highlighted need for a shift from individual consent mechanisms to a data stewardship model and for a shift from a dual model of 'personal' and 'anonymous' data model to a scalable model instead of 'personal data.'[50]

[45] Purtova (n 2); Zittrain (n 6).
[46] AI Act, art 2(1)(c).
[47] Explanatory Memorandum to the AI Act, 6.
[48] ibid 4.
[49] Cate and Dockery (n 34).
[50] Purtova (n 2); Acquisti (n 27); Bygrave (n 10).

6. The Risk-Based Approach of the AI Act: A Utilitarian Alternative for the Improvement of the Data Protection By Design Mechanisms under the GDPR

The AI Act is a risk-based regulatory model, meaning, the obligations imposed on providers and users (and other actors) relative to AI systems depend on the extent to which the marketing, development, or use of AI systems pose a risk. Under the framework of the AI Act, a 'marker' system is established, wherein four risk categories are distinguished: (1) prohibited practices,[51] (2) high risk,[52] (3) transparency risks,[53] and (4) no/minimal risk.[54] Prohibited practices are listed exhaustively and include, for instance, the use of AI tools which 'deploy subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm.'[55] It will be interesting to observe the extent to which such practices are regulated, and to which such content is effectively moderated, in practice, as generally accepted social harms. As for the lower risk categories, the AI Act seeks to encourage their regulation by MS domestically through the promotion of so-called codes of conduct and other soft law instruments.[56]

What this risk-based regulatory model does provide us with, however, is a mixed instrument of soft and hard law, wherein scalable solutions and their impact upon the subjects affected are much more tailored to the specific needs of the technology it seeks to regulate within the internal market. This is something clearly lacking in the data protection regime of the EU to date where we see a model of 'personal data' duality with a high-intensity of positive obligations in place. Yet, today, internet intermediaries bear only partial responsibility for content uploaded by users,[57] especially if the intermediaries host information. This causes practical issues of enforceability. For instance, in a blockchain, the full nodes host content. It is thus clear that the current regulatory model in place is not up to the state of the art. Nor can it catch up in time, it needs to remain flexible and sufficiently agile so as to adjust to market developments. The implications of our inspiration drawn from the AI Act for a revised GDPR are thus that the latter needs to more effectively implement the proposed risk-pronged approach of the AI Act, instead of the purely consent-based mechanism founded on an outdated concept of 'personal' vs 'anonymous' data with a high-intensity of positive duties.

---

[51] AI Act, art 5.
[52] ibid, arts 6-7.
[53] ibid, art 52.
[54] Explanatory Memorandum to the AI Act, 12.
[55] AI Act, art 5(1)(a).
[56] ibid, art 69.
[57] Dirk A Zetzsche, Ross P Buckley and Douglas W Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2018) *U Ill L Rev* 1361.

Firstly, because data protection by design cannot only be imposed legally, where the state of the art tends to be unreliable and ineffective. It requires a combination of a soft and hard law approach, which the AI Act risk-based mechanism adopts.[58] Secondly, because a scalable risk-pronged mechanism of classification promotes that firms re-/using data and automation in their daily content moderation make greater efforts for amplified transparency and disclosure on their usage of tools, as well as the respective implications for data subjects' and users' privacy and access to information.[59] Thirdly, because we need to refrain more from drawing simplifying narratives of data protection law, where the responsibility and subsequent liability are pushed over on to so-called 'algorithms' as an abstract entity where big data analysis is concerned.[60] This also includes narratives where ranking algorithms are capable of making so-called neutral judgments, free of discrimination. This is simply not the case, though as we know, there are remedies available 'providers' can seek. In turn, remedies for 'users' could also be sought from the backend, such as the enhancement of agency of users through choice alternatives of ranking,[61] or a general policy objective of enhancement of transparency on design and performance of such systems and their recommendations. Fourth and lastly, because we have already witnessed what the scenario of ineffective data protection looks like. Defining so-called 'guardrails' for the provision, commercialisation and re-use of data, much like that of AI, based on risks to society, is therefore of importance, and it can no longer be rejected on the basis of economic, financial, nor legal grounds since its impact affects all actors, sectors and connected users of society in the EU. It is also true that today large tech firms cannot be said to be mere 'intermediaries' as under the legal regime of the E-Commerce Directive. It is therefore important that we work together to ensure the market remains generative, whilst adjusting data protection mechanisms to secure their effectiveness. This was observed throughout the pandemic, where platforms even acted as a form of 'regulatory intermediators' by connecting individuals with public services and other authorities through COVID-19 apps.[62] For instance, Google heavily steered such regulatory intermediation via 'specialised modes of editorialisation.'[63] How this role changes over time, however, is up to us: regulators, private sector stakeholders, and connected users. The almost bimodal distribution of players in the market, however, brings us our final ground for reform of the data protection regime, as seen for instance in Figure 2. Only time will tell whether data protection reform, thus, follows suit.

---

[58] Commission and others, *Hosting Intermediary Services and Illegal Content Online: an Analysis of the Scope of Article 14 ECD in Light of Developments in the Online Service Landscape* (Publications Office 2019); Sophie Stalla, 'Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well' in Mariarosaria Taddeo and Luciano Floridi (eds), *The Responsibilities of Online Service Providers* (Springer 2017); Joris van Hoboken and Daphne Keller, 'Design Principles for Intermediary Liability Laws' (*Stanford Cyber Policy Center,* 8 October 2019) <https://cyber.fsi.stanford.edu/publication/design-principles-intermediary-liability-laws> accessed 3 May 2022; Dan Wielsch, 'Private Law Regulation of Digital Intermediaries' (2019) *2 European Review of Private Law* 197; Folkert Wilman, 'The EU's System of Knowledge-Based Liability for Hosting Service Providers in Respect of Illegal User Content – Between the E-Commerce Directive and the Digital Services Act' (2021) *12 JIPITEC* 317.

[59] Aleksandra Kuczerawy, *Intermediary Liability and Freedom of Expression in the EU: From Concepts to Safeguards* (Intersentia 2018); Christophe Geiger and Elena Izyumenko, 'Blocking Orders: Assessing Tensions with Human Rights' in Giancarlo Frosio (ed), *The Oxford Handbook of Intermediary Liability Online* (Oxford University Press, 2020) 566.

[60] Goanta (n 17).

[61] Eleni Kosta, 'Algorithmic State Surveillance: Challenging the Notion of Agency in Human Rights' (2022) *16 Regulation & Governance* 212.

[62] Dieter and others (n 32).

[63] ibid.

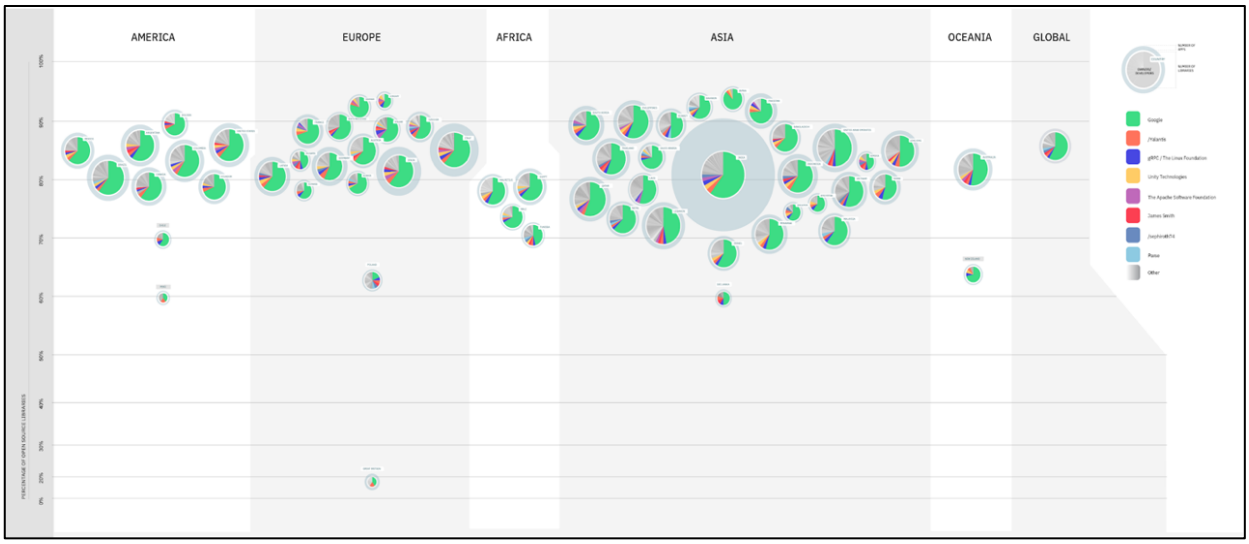

FIGURE 2: 'Developers behind SW libraries embedded in [COVID-19]-related apps by country or region (Android only). Circles (pies) are library developer distributions per country; horizontal axis: continents; vertical axis: % of open-source libraries. Illustration: authors and DensityDesign Lab. By focusing on the ownership of these libraries, we highlight the material conditions of platforms and apps like Google as 'service assemblages' which reveals some of the deeper ways in which pandemic platform governance, and platform power more generally, manifest.'[64]

7. Overview of Conclusions for the Regulatory Outlook of Data Protection Mechanisms

The present article considered the question of how to best regulate the extent and means of data protection in the European context, zooming in particular on the un-/desirability for data protection by design mechanisms vis-à-vis their effectiveness and generativity. It was argued here that although the GDPR was a clear advancement from its preceding instruments, future demands of data protection and generativity in the digital economy will require a clearer and more risk-based regulatory framework. The reformed data protection by design framework should strive to put scalable data protection mechanisms of risk management and data stewardship (rather than overly relying on consent and notice mechanisms), built-in privacy mechanisms (PETs), and industry incentives for generative privacy models at its centre.

Moreover, a hybrid model of public and private stakeholders has been argued to be the best fit for developing the updated framework in the upcoming decade. This includes a shifting away from the duality of 'personal' and 'anonymous' data with high-intensity of positive obligations, implementing instead a risk-based classification system of data similar to that taken in the AI Act regulatory approach, to better seek scalable solutions capable of tackling the reality of the industry and data subjects today. Lastly, market initiatives seeking to promote decentralised cloud services and data stewardship models should be much more incentivized in the market by lawmakers and regulators alike. Public sector bodies should avoid the conclusion of agreements creating exclusive rights for the re-use of certain data, so as to make data more available to

[64] ibid.

SMEs and start-ups. Not only that, but a reformed framework should set up pools of data on a voluntary registration scheme of data altruism organisations. These initiatives would help exploit the potential in the use of data made available voluntarily by informed consent or general interest, such as scientific research, healthcare, combating climate change or improving mobility. Indeed, these measures may also potentially provide simple infrastructure solutions on the internet layer that could ultimately both improve market generativity for tech firms as well as allow data subjects to gain more effective control over their data. In short, in pursuing the herein proposed solutions vis-à-vis present and future challenges for the effectiveness and generativity of data protection mechanisms, we will have effectively taken Ostrom's Law to heart and ultimately grasped that 'governance models which work in practice can also work in theory.' [65]

[65] Fennell (n 11).

Case Note on *Zoltan Varga v Slovakia*

Ioannis Takolas[1] *& Dimitrios Liasis*[2]

Abstract

This case deals with the issue of covert surveillance conducted by the Slovak Intelligence Service. The European Court of Human Rights (ECtHR) examined whether the implementation of the national legislation with regard to secret surveillance complied with Article 8 of the European Convention on Human Rights (ECHR).[3] The following analysis will scrutinise the implementation of the *Huvig* legality test by the ECtHR, which was established in previous case law. This commentary aims to assess the compliance of surveillance legislation with this fundamental right and to identify whether any new elements were introduced to strengthen the right to privacy.

[1] Ioannis Takolas is currently an LLM student in 'Law and Technology' at Tilburg University. As an Erasmus student at the University of Liège, he explored the challenges deriving from the emergence of AI and the evolution of human rights protection within the EU legal order. Subsequently, he worked as an Assistant Researcher in the Law and Technology Group of Ghent University conducting a mapping exercise regarding journalistic freedom of expression among various countries in collaboration with the Legal Clinic of Ghent University. Nowadays, as an LLM student, he researches how to reconcile modern digitised societal models with substantial human rights protection.

[2] Dimitrios Liasis is a European Qualified Lawyer. He has always been fascinated by emerging technologies and how they can revolutionise and disrupt the legal system. He has graduated from the LLM in 'Law and Technology' from Tilburg University. Through his Thesis with regard to the patent rights to the inventions that AI generates, he has accumulated valuable knowledge about AI and Blockchain Technology. During his postgraduate degree, he developed his technological affinity by completing specialisation courses in programming and he is currently working as a Programmer invested to combine his academic and technical insight.

[3] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended by Protocols Nos. 11 and 14) (ECHR) [1950].

1. Facts

The case deals with individual covert surveillance. The applicant was subjected to a surveillance operation by virtue of three warrants[4] by the Regional Competent Court at the request of the Slovak Intelligence Agency (hereafter SIS). Upon the applicant's complaints, Slovakia's Constitutional Court declared the annulment of the above-mentioned warrants.[5] In the meantime, material obtained from the surveillance, resulting from the implementation of the three warrants, was leaked.[6] The applicant sought domestic remedies to achieve the destruction of this material. The Constitutional Court asserted that the destruction of the material lies in the competence of the Regional Court, which authorised the surveillance. In turn, the Regional Court stated that it was incompetent to order the deletion of the material and that only the SIS may rule on this matter. Neither the Constitutional nor the Regional Court engaged in judicial oversight during the implementation of the warrants and the actions of SIS.[7] Moreover, the applicant attempted to achieve the deletion of the material through an unsuccessful administrative procedure.[8] Due to the inadequacy of legal remedies at the domestic level deriving from the annulment of the warrants, he sought redress before the ECtHR.

2. Questions to the Court

The question referred to the court was whether the implementation of the three warrants and the retention of the produced material breached the applicant's right to private life.[9] The Court found a violation of Article 8 based on the following analysis.

3. Legal analysis

3.1. Admissibility

In examining the admissibility of the privacy violation claim, the Court commenced by assessing whether the applicant shall be granted victim status. In this vein, it is notable that traditionally, *in abstracto* claims would be declared inadmissible by the Court.[10] It was only in the 1970s when the unique nature of surveillance technologies caused the ECtHR to resolve the tension between the applicants' inability to substantiate a privacy violation claim, on the one hand, and the frequent absence of any information upon the implementation of covert surveillance techniques. Actually, when delivering the *Klass and Others v Germany* judgement[11] the Court moved beyond the personal harm requirement and assessed the surveillance legal

[4] Zoltán Varga v Slovakia App nos 58361/12 and 2 others (ECtHR, 20 July 2021), paras 6-9.
[5] ibid [31-47].
[6] ibid [18].
[7] ibid [14-15, 45-46].
[8] ibid [40-41].
[9] Article 8 ECHR.
[10] Bart van der Sloot, 'Is the Human Rights Framework Still fir for the Big Dara Era? A Discussion of the ECtHR's Case-Law on Privacy Violations Arising from Surveillance Activities' in Serge Gutwirth, Ronald Leenes, Paul de Hert (eds), Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection (Springer 2016), 411, <https://www.ivir.nl/publicaties/download/1701.pdf > accessed 2 February 2022, page 6.
[11] *Klass and Others v Germany* (ECtHR, 6 September 1978).

framework to accept an *in abstracto* claim for the first time in its jurisdictional history.[12] Furthermore, in the recent *Zakharov* case, the ECtHR made a bold step by consolidating this approach. In fact, it established that 'an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied…'.[13] On this basis, the analysis regarding the victim status in the *Zoltan* case did not revolve around the concrete effect of the impugned policy on the applicant. In contrast, the focus was placed on whether the essence of the applicant's claims was addressed by the Regional Court's decision, which upheld his complaints.[14] Upon providing a negative answer to this question, the Court concluded by granting victim status to the applicant.[15]

Additionally, the *Klass* decision alongside its recent successor, the *Zakharov* ruling, is of great importance with regard to the merits of the *Zoltan* case. More specifically, the Klass case established the framework for the regulation of surveillance operations. In fact, it was the first time for the Court to consider the implementation of secret surveillance methods by public authorities 'necessary in a democratic society' to preserve national security and prevent disorder or crime.[16] In this manner, it essentially set the framework for the regulation of surveillance practices within the Council of Europe (CoE).[17] [18]

Focusing on the *Zoltan* judgement, the Court dealt with the alleged privacy infringement following its jurisprudence; it initially confirmed that secret surveillance measures fall within the scope of Article 8 ECHR.[19] Moreover, in assessing the existence of interference, the Court highlighted that the applicant was subjected to surveillance and that the produced material was retained by the SIS and the Regional Court. It therefore concluded that the applied practices constituted an interference with the applicant's privacy.[20]

3.2. Legality Test

Having established the interference, the Court adopted the *Huvig* legality test and proceeded with examining the justification of the interference based on Article 8(2) of the ECHR.[21] More precisely, this provision introduces three cumulative conditions for the justification of interference with the respective right.[22] For the first requirement, the ECtHR stated that a surveillance measure must demonstrate legality. Based on this and

---

[12] ibid, p 10.
[13] *Roman Zakharov v Russia* (ECtHR, 4 December 2015) para 171.
[14] *Zoltán* judgement [108-110].
[15] ibid [111].
[16] *Klass* judgement [48].
[17] Paul De Hert and Gianclaudio Malgieri, 'Article 8 ECHR compliant and foreseeable surveillance: the ECtHR's expanded legality requirement copied by the CJEU. A discussion of surveillance case-law' (2020) 6 (21) Brussels Privacy Hub, Working Paper <https://brusselsprivacyhub.eu/publications/wp621.html> accessed 15 September 2021;
[18] *Klass* judgement [48].
[19] *Zoltan* judgement [95].
[20] *Zoltán* judgement [145-149].
Klass judgement [149].
[21] *Zoltán* judgement [150].
[22] Article 8 ECHR, The impugned measure "shall be in accordance with the law, pursue a legitimate aim and be necessary in a democratic society."

in delivering the *Huvig* ruling the Court identified four legality requirements;[23] initially, as regards the material requirement of legality, the impugned measure should have some basis in domestic law. Simply stated, the law shall be perceived in its substantive sense to encompass both written formal laws and lower rank enactments,unwritten law. Turning to the accessibility requirement of legality, the law also refers to the quality of the law in question; in fact, the law shall be accessible to the person concerned. Towards the foreseeability requirement of legality, the law must enable the person concerned to foresee its consequences for him. Lastly, focusing on the rule of law requirement of legality, the whole domestic arrangement should be compatible with the rule of law. [24] The ECtHR shaped this approach in response to the constantly increasing complexity of available surveillance technologies in 1990.

Nonetheless, the *Huvig*[25] and the *Malone*[26] cases' contribution to the ECtHR's surveillance jurisprudence extends even further, given that the analysis of the legality requirement paved the way for the foreseeability criteria.[27] Actually, in the examination of a law providing for telephone tapping, the ECtHR elaborated on the conditions on foreseeability. More specifically, the law shall clearly define the categories of individuals liable to be monitored, the nature of the offences likely to trigger surveillance measures and the temporal constraints of such measures. Moreover, the provision shall clarify the procedure for the storage of the resulting information, the precautions for the communication of the data to judges and the defence and finally the circumstances for the deletion of such information.[28] In other words, the Court outlined six requirements under which domestic laws can be adequately foreseeable and compliant with the ECHR legality principle.[29] [30]

After delineating the theoretical background of the *Zoltan* case, the Court advanced to test the legality of the surveillance procedure against the *Huvig* legality test. In this context, the *Zoltan* judgement established that various critical aspects of the procedure for storing data are subjected to an internal regulation by the SIS Director. However, its content could be accessed neither by the person concerned nor by the Court that issued the warrants due to classification. In fact, the ECtHR highlighted that the SIS was not subject to any means of supervision when acting on the basis of the issued warrants.[31] Therefore, such an inability to reach and contest the surveillance regulatory regime amounts to a clear lack of accessibility.[32]

---

[23] De Hert and Malgieri (n 16), p. 8-9.
[24] *Huvig v France* App no 11105/84 (ECtHR, 24 April 1990) para 26.
[25] Huvig judgement.
[26] *Malone v the United Kingdom* App no. 8691/79 (ECtHR, 2 August 1984) para 67.
[27] De Hert and Malgieri (n 16), 304 - 318. "laws need be foreseeable, not as to the likelihood that the authorities may interfere with the people's right to privacy but, as to "the circumstances in which and the conditions on which public authorities are empowered to resort" to such interference. Malone's legality test required legal provisions be accessible, foreseeable and precise in the sense of sufficiently indicating "the scope and manner of exercise of the discretion conferred on the relevant authorities". Such a test demanded detailedness referring to the why and the how, the overall organisation of the interference (in that case, surveillance).".
[28] De Hert and Malgieri (n 16), p. 9.
[29] De Hert and Malgieri (n 16).
[30] Christos Giakoumopoulos and Giovanni Buttarelli and Michael O'Flaherty, Handbook on European data protection law (1st eds, Luxembourg: Publications Office of the European Union. 2018).
[31] ibid [167-168].
[32] ibid [169].

Regarding the material requirement of the legality principle, the Court observed that the implementation of the assessed warrants relied on the provisions of the PP Act.[33] The latter governed the primary material resulting from the implementation of the issues warrants.[34] These provisions required the warrants to be of a judicial origin, which is also satisfied in the case under discussion. In this respect, the Court found that since the examined measure clearly demonstrates a basis in domestic law, it also meets the material legality requirement.

3.2.1. Foreseeability Test

Adhering to the *Huvig* legality criteria,[35] the ECtHR then carried out the foreseeability assessment. In this regard, the ECtHR in its *Sunday Times v UK* decision determined that a citizen 'must be able - if need be, with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences that a given action may entail'.[36] Concerning the first and the second *Huvig* criteria, 'the categories of people liable to be monitored' and 'the nature of the offences that might give rise to surveillance', it is apparent that the ECtHR did not engage in further analysis and proceeded to examine the remaining aspects of foreseeability. This omission might insinuate that the ECtHR implicitly accepts the Slovakian law as sufficiently clear.

As for the duration of the surveillance, the ECtHR acknowledged that the surveillance was lacking clear and specific rules in terms of time frame, and therefore did not demonstrate adequate foreseeability regarding the duration of the surveillance. In the ECtHR's view, this constituted a major flaw of the surveillance since it essentially provided for indefinite surveillance. According to the Court, the ambiguity concerning the time frame of the surveillance rendered the warrants 'unjustified and unlawful'.[37]

Testing the procedural foreseeability, the Court went one step further and examined whether the implementation of the law by the Judiciary and the SIS was in accordance with the law, and the analysis was not limited to the examination of the statute. The Court considered that the warrants were issued by the Regional Court, whereas the Executive decided on its own accord about the TMGI (technical means of gathering intelligence).[38] In addition, their duration demonstrated neither a clear time frame nor judicial oversight. These factors left room for arbitrariness by the Executive.[39] The ECtHR stated that the name of the judge who authorised the surveillance was not mentioned within the warrants. This resulted in a lack of due process because it prevented the applicant from verifying whether the warrants had been issued by a legitimate judge and subsequently from seeking redress.[40] In this respect, the Court reiterated that the SIS did

[33] Privacy Protection Act(Law. no. 166/2003).
[34] ibid [153].
[35] *Huvig* judgement.
[36] The Sunday Times v United Kingdom (ECtHR 26 April 1979), para 49.
[37] *Zoltan* judgement [33, 156].
[38] *Zoltan* judgement [28]. TMGI refers to the "use of technical means of gathering intelligence ("TMGI") to carry out that supervision.".
[39] ibid [151].
[40] ibid [33, 55, 153].

not provide specific reasons for requesting the application of TMGI.[41] These elements cast serious doubt on the 'practical foreseeability' in terms of procedure and delineate a case 'of an intelligence agency that itself drafts the warrants authorising its interference…',[42] which in essence enables the SIS to decide and implement warrants in an unrestrained manner.[43]

As for the next foreseeability requirement, i.e., the precautions regarding the communication of data, the ECtHR did not engage in a rigorous assessment of whether there are adequate precautions in place. Nevertheless, the ECtHR acknowledged that the data collected from the surveillance was leaked on the Web and used in unrelated criminal investigations by the authorities.[44] This could indicate the inadequacy of existing precautions in practice. However, the ECtHR did not delve deeper and proceeded with the examination of other foreseeability requirements.

Moreover, foreseeability concerning the circumstances of the retained data's destruction of the obtained data was tested by the ECtHR. Scrutinising the legal regime which governed the destruction, the Court concluded that domestic law did not set the conditions for the destruction of the stored data.[45] In lieu, the SIS Act mandated that such data should be made inaccessible to everyone, including the judge authorising the surveillance. The latter provision raised grave concerns; when seeking the destruction of the retained material, the applicant faced a double hurdle. Firstly, the classification of the data prevented him from proving the storage of data; in reality, unawareness of the existence of the stored data impeded the applicant from gaining knowledge of the data's content and thus, the destruction of the stored material was rendered impossible.[46] Secondly, the vicious jurisdictional cycle between the Regional and the Constitutional Court deprived the applicant of an effective judicial remedy, given that both courts declined competence to order the destruction of the retained data. Consequently, it was only the Executive that could order its deletion. This situation allowed room for arbitrariness.[47] The ECtHR considered this a major flaw and reiterated the *Klass* reasoning that in cases of telephone tapping, an effective legal remedy shall entail the destruction of the retained information.[48]

3.2.2. Impugned Measures and the Rule of Law

The Court also emphasised the lack of judicial oversight of the surveillance procedure. According to the ECtHR's jurisprudence, in cases of interference, the person being surveilled shall be provided with safeguards against unjustified interference, such as the judicial control of the surveillance procedure and the notification

[41] ibid [33].
[42] ibid [156].
[43] ibid [1,5,6].
[44] ibid [18-21].
[45] ibid [158].
[46] ibid [151].
[47] ibid [151, 161-171].
[48] *Klass* judgement [71].

duty.[49] These safeguards are inextricably connected with the Rule of Law and the right to an effective legal remedy.[50] In the present case, with regard to the supervision of the surveillance procedure, the ECtHR focused on the matter of judicial oversight and recognised that the Slovakian law provided such an obligation on behalf of the issuing judge.[51] However, the ECtHR did not limit its assessment to the statutory provisions, but examined the practical implementation of the law as well; the ECtHR thus noted that both the Regional and the Constitutional Court adopted a passive stance during the surveillance. In fact, they authorised the SIS to draft the TMGI and set the time frame of the surveillance, without intervening at any stage of the procedure.[52] Consequently, the Court concluded that the judicial control was non-existent, despite the statutory provision.

Notification-wise, both the *Digital Rights Ireland* [53] and the *Roman Zakharov v. Russia* cases[54] recognised that the surveilled must be notified of the surveillance, 'as soon as the notification does not jeopardise the purpose of the surveillance'.[55] 'Emphasis was put on the notification duty in the *Tele2 Sverige* case, as well.[56] In *Tele2*, the CJEU adjudicated that notification is of prime importance, given that it enables individuals to seek judicial redress. According to the CJEU, notification can serve as an effective safeguard against unjustified interference. This means that notifying the surveilled individual that they are subject to a covert procedure can help minimise the degree of interference with the fundamental right to privacy in the sense that the interference is rendered justified.[57] A similar approach was also adopted in *Digital Rights Ireland*.[58] Specifically, the CJEU stated that the data retention constituted a 'wide-ranging' interference because it was not justified by the duty of the authorities to notify the person under covert surveillance. In this context, the significance of the notification requirement is indisputable, as notification is also inextricably connected with the idea of the Rule of Law. The idea of the Rule of Law can only be realised in case the individuals can identify they are subject to surveillance. Only on this condition can they seek judicial redress against the surveillance procedure.[59] Hence, it is evident that notification is a necessary requirement for the subsequent exercise of the right to effective legal remedy.[60] In fact, lack of notification means that the individuals under surveillance most likely do not know that they are being monitored. Unaware of the surveillance, these

[49] De Hert and Malgieri (n 16).
[50] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended by Protocols Nos. 11 and 14) (ECHR) [1950], art 13.
[51] *Zoltan* judgement [158].
[52] ibid [151, 162].
[53] *Digital Rights Ireland and Other* (ECtHR 8 April 2014).
[54] De Hert and Malgieri (n 16). "In the 2014 Digital Rights Ireland judgement, the CJEU found data retention 'a particularly serious interference' because it is 'wide-ranging' and is not accompanied with a notification duty to notify, which is 'likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance' (Digital Rights Ireland, §37). Notification to individuals".
[55] *Zakharov* judgement [287].
[56] *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others 21* (CJEU, December 2016).
[57] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended by Protocols Nos. 11 and 14) (ECHR) [1950] art 8.
[58] De Hert and Malgieri (n 16).
[59] *Tele2 Sverige* judgement.
[60] Article 13 ECHR.

individuals will not seek judicial redress. As a consequence,the right to an effective legal remedy will not be exercised.

In the case at hand, the Court did not reach a clear conclusion on this matter. However, the Court implicitly referred to a violation of the right of the applicant to be notified. For further clarity, the ECtHR highlighted the applicant's right to be informed about the retained material collected from the surveillance. Additionally, it marked that this right is a prerequisite for an effective legal remedy, as mentioned above.[61] The notification was justified based on the following factors. Firstly, the warrant was annulled, but the applicant was still incapable of accessing the material due to classification. Secondly, the procedure was considered unlawful and therefore, no legitimate interest was to be jeopardised by notifying the surveilled. As a result, the applicant should have been notified of the entire surveillance procedure and should consequently gained access to the retained material. However, the Court in the present case was reluctant to clearly state that a notification duty shall be fulfilled by the national authorities.

4. Conclusion

To sum up, the contribution of this judgement to the cohesion and the development of ECtHR jurisprudence is considered invaluable. Firstly, it adheres to the theoretical construct shaped by previous cases and engages in a rigorous analysis of the *Huvig* criteria. This approach may be attributed to the fact that monitoring all activities within an apartment that constitutes a private residence amounts to a major privacy interference in comparison with the telephone tapping techniques addressed in the *Huvig* decision. Moreover, the present case enhances the *Huvig* test by applying it on a practical level. This development indicates that the Court genuinely sought to examine the foreseeability of the challenged surveillance measure, rather than limiting its assessment to theoretical tests. Finally, the ruling clarifies the significance of the right to privacy as a requirement for other fundamental rights, such as the right to an effective legal remedy.[62] In particular, an individual's inability to access information resulting from surveillance measures against them does not allow for identification of the issuing authority or the violation; it thus prevents the exercise of the right to seek an effective legal remedy. However, despite recognising this problematic situation, the ECtHR did not clearly state that requiring national authorities to notify the surveilled of the implemented surveillance methods may resolve this issue.

As a concluding point of criticism, the following issue shall be taken into consideration: in terms of systematic coherence, this ruling is of great value since it reverently relied on the conceptual constructs shaped within the ECtHR's case-law. However, the Court was contained within the artificial border of the three-step test; in fact, it started with the analysis of the legality requirement and concluded twice that the impugned

[61] *Zoltan* judgement [162, 169].
[62] Article 13 ECHR.

practices were not in accordance with the law.[63] Nonetheless, it proceeded to determine that, on the basis of this finding, 'it is not necessary to examine whether the other requirements of Article 8(2) ECHR were complied with'.[64] Therefore, it missed the opportunity to utilise an innovation introduced in the *Zakharov* case, the so-called combined approach. More specifically, in this cornerstone ruling, the Court decided to jointly assess elements of the legality principle and the necessity requirement.[65] In this manner, it would avoid examining the necessary safeguards both as an aspect of legality and as a foreseeability element. However, by restricting the scope of the analysis to the legality test, the Court did not seize the opportunity to proceed to a comprehensive and substantial analysis of the surveillance regime in the *Zoltan* case.[66] This would actually maximise the contribution of the ruling to the development and the cohesion of surveillance case-law.

Taking the above into consideration, such a judgement should overall be seen as a desirable jurisdictional step. However, had the ECtHR adopted a bolder stance toward the recurring jurisdictional crossroads, it would have further enhanced the ability of the CoE legal framework to effectively safeguard the privacy of European citizens against emerging disruptive technologies. The Court would, in this sense, deliver both a message that the implementation of novel surveillance methods shall comply with the high standards shaped through its case-law and a promise for substantial privacy protection within the European legal order.

[63] *Zoltan* judgement [162, 171].
[64] ibid [172].
[65] *Zakharov* judgement, para 237.
[66] Eleni Kosta, 'Surveilling masses and unveiling human rights – Uneasy choices for the Strasbourg Court' Inaugural address for the Chain on Technology Law and Human Rights at Tilburg University [2017] <https://ssrn.com/abstract=3167723> accessed 2 February 2022.

THE RIGHT TO BE FORGOTTEN:

Comparative Analysis of Policies That Have Been Developed with Respect to the Right to Be Forgotten Online at EU and US Level

Simona Urbaničová[1]

Abstract

During the last few decades, a new 'digital world' has been created alongside the 'real' one. Even the policies concerning the right to privacy that have been developed in the 'real' world are sometimes exposed to problems. Next to gaps and imperfections of the right to privacy in the 'real world', a completely new concept of the right to privacy in the 'digital' world has been created. The internet has become a searchable database for content of any kind that had already been uploaded there. Moreover, the internet is considered to have 'perpetual memory', which is incomparable with human memory. Therefore, it is practically impossible to escape this digital memory of the internet. As a result, individuals are threatened to be trapped in their digital past. Because of this relatively recent phenomenon, there has been an urge to create a legal concept of the digital right to privacy whereby the internet population should be protected. The right to be forgotten has recently also become part of this concept. The purpose of this paper is to comparatively analyse the policies that have been developed concerning the right to be forgotten in the EU and the US.

[1] Simona Urbaničová comes from Slovakia and is a full-time law student. In 2021, she graduated with LL.B. from Maastricht University (the Netherlands). During the academic year of 2020/21, she undertook a position of the Director for Advocacy at ELSA the Netherlands and took part in other ELSA projects, such as ELSA European Human Rights Moot Court Competition and ELSA Legal Research Group.
She is currently pursuing LL.M. (double degree) at KU Leuven (Belgium) and University of Zürich (Switzerland). Her interests lie in European public law, policy-making, public administration and governance.

1. Introduction

During the last few decades, a new 'digital world' has been created alongside the 'real' one. Even the policies concerning the right to privacy that have been developed in the 'real world' are sometimes exposed to problems. Next to gaps and imperfections of the right to privacy in the 'real' world, a completely new concept of the right to privacy in the 'digital' world has been created. The worldwide internet population is estimated to be 2.1 billion people. More precisely, the internet population in North America is over 274 million people, while in Europe it is over 519 million people.[2] A continuously increasing number of individuals join this online community, for instance, by simply creating social media accounts where they upload various content, most of which concerns their private life. Every social media user, therefore, creates the so-called digital 'trace' or footprint.[3] However, what if part of this content is embarrassing or inappropriate? Should one mistake impact the rest of a person's life? Should a person's digital footprint be permanent and indelible?

The internet has become a searchable database[4] for content of any kind that had already been uploaded there. Moreover, the internet is considered to have 'perpetual memory',[5] which is incomparable with human memory. According to the internet law scholar Victor Mayer Schönberger, it is practically impossible to escape the digital memory of the internet.[6] As a result, individuals are threatened to be trapped in their digital past.[7] Because of this relatively recent phenomenon, there has been an urge to create a legal concept of the digital right to privacy whereby the internet population should be protected. The right to be forgotten has recently also become part of this concept. However, it should be noted that the right to be forgotten is a rather recent development applicable only in a few jurisdictions, especially the European ones.

For the purposes of this paper, the general meaning of the concept of the right to be forgotten should be clarified. This specific right is ascribed to individuals to have online personal data removed or the access to such data restricted while the rights against search engines are also incorporated in this concept.[8] The aim of this paper is to comparatively analyse the policies that have been developed with regard to the right to be forgotten in the EU and the US.

---

[2] Meg Leta Jones, *Ctrl + Z: The Right to Be Forgotten* (NYU Press 2016) 3.
[3] D Dörr and R. L. Weaver (Eds.), *The Right to Privacy in the Light of Media Convergence: Perspectives from Three Continents* (De Gruyter 2012) 324.
[4] Meg Leta Jones, *Ctrl + Z: The Right to Be Forgotten* (NYU Press 2016) 5.
[5] ibid, 16.
[6] ibid, 6.
[7] D Lindsay, '*Emerging Challenges in Privacy Law: The 'Right to Be Forgotten' in European Data Protection Law'* (Cambridge University Press 2014) 294.
[8] D Lindsay, *'The "Right to Be Forgotten" by Search Engines under Data Privacy Law: A Legal and Policy Analysis of the Costeja Decision'* in A T Kenyon (Ed.), '*Comparative Defamation and Privacy Law'* (Cambridge University Press 2016) 201.

2. The EU policies regarding the right to be forgotten online

2.1. The historical development of the right to be forgotten

Data protection laws started developing in the early 1980s. Two main international instruments are considered to lay down the origins of data protection laws, namely the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Council of Europe's Convention on Data Protection.[9] A number of crucial principles were incorporated in the above-mentioned instruments, such as the use limitation principle, the individual participation principle and the data quality principle. Nevertheless, an express right to be forgotten was still missing, due to the emphasis put on the importance of access to personal data by data controllers.[10]

In 1995, the Data Protection Directive ('1995 DP Directive') was adopted in the EU, which extended the scope of pre-existing instruments and made some significant changes regarding data collection and processing.[11] However, neither the right to erasure nor data expiry limits were introduced.[12]

In 2009, a significant initiative towards the introduction of the right to be forgotten came from the European Commissioner for Justice, Fundamental Rights and Citizenship - Viviane Reding. The proposal for the new Data Protection Regulation ('DP Regulation') was released on 25 January 2012. The DP Regulation aimed to replace the 1995 DP Directive and introduced 'the right to be forgotten and to erasure' in its Article 17. This can be regarded as the first explicit legislative right to be forgotten whereby the erasure of the personal data held by data controllers can be enforced by data subjects.[13]

2.2. *Google Spain, SL, Google Inc v Agencia Española de Protección de Datos*

In 2014, the European Court of Justice ('ECJ') heard a case and created a contemporary precedent on the issue of the right of deletion of data.[14] Facts of the case are as follows: In 2010, Mr. Costeja González filed, together with the *Agencia Española de Protección de Datos* ('AEPD'), a complaint against the daily newspaper La Vanguardia, as well as Google Spain and Google Inc. The issue in this case was that when typed into the 'Google Search', Mr. Costeja Gonzalez's name was automatically linked to two pages of La Vanguardia.[15] These two pages had been published in 1998, but were still available online years after the publishing. The

[9] D Dörr and R. L. Weaver (Eds.), *The Right to Privacy in the Light of Media Convergence: Perspectives from Three Continents* (De Gruyter 2012) 334.
[10] ibid.
[11] ibid, 337.
[12] ibid, 336.
[13] Meg Leta Jones, *Ctrl + Z: The Right to Be Forgotten* (NYU Press 2016) 10.
[14] T Macaulay, 'What Is the Right to Be Forgotten and Where Did It Come from?' (Techworld, 14 September 2017) <https://www.techworld.com/data/could-right-be-forgotten-put-people-back-in-control-of-their-data-3663849/> accessed 6 April 2019.
[15] Case C-131/12 *Google Spain, SL, Google Inc v Agencia Española de Protección de Datos* (ECJ 13 May 2014).

problem was the content of the published pages which announced that Mr. Costeja Gonzalez's property had been forcefully sold in order to recover social security debts.[16]

In his complaint, Mr. Costeja González made two requests. First, La Vanguardia shall either delete or adjust the relevant pages so that his data would not be visible anymore. Secondly, Google shall ensure that his personal data will no longer be linked to La Vanguardia.

The complaint against the daily newspaper was dismissed since the publication of Mr. Costeja Gonzalez's personal data was justified. However, the complaint against Google Spain and Google Inc was upheld by the Spanish court.[17] Consequently, the Spanish court referred three questions to the ECJ for a preliminary ruling. The first question was based on the dilemma of whether search engines fall within the territorial scope of the DP Directive. The second question concerned the material scope of the DP Directive.[18] The last question asked, in essence, whether the DP Directive should be interpreted in a way that individuals can directly request the search engines, like Google, to delete their personal data since they do not wish that specific data to be published online.[19]

The ECJ ruled that Google was obligated to withdraw the data from its indexes.[20] More precisely, the ECJ stated that the aim of the DP Directive is to protect fundamental rights, namely the right to privacy, and therefore, interpreted the DP Directive in favour of Mr. Costeja González.[21] The reasoning was as follows: the search engines are responsible for spreading the personal data and are obligated to delete specific data if it 'is liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense'.[22] This also concerns the cases where a data subject does not wish to be known to third parties.[23]

Not only is this judgement considered to affirm the existence of the right to be forgotten,[24] but it is considered to be enforceable as well.[25] It is important to note that even though this judgement is a significant improvement to privacy rights online, it is also considered as conflicting with other fundamental rights, such as the right to freedom of expression or the right to access to information.[26] Some organisations, such as the

---

16 T Macaulay, 'What Is the Right to Be Forgotten and Where Did It Come from?' (Techworld, 14 September 2017) <https://www.techworld.com/data/could-right-be-forgotten-put-people-back-in-control-of-their-data-3663849/> accessed 6 April 2019.
17 Case C-131/12 *Google Spain, SL, Google Inc v Agencia Española de Protección de Datos* (ECJ 13 May 2014).
18 E Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgement in Case C-131/12, *Google Spain v Agencia Espanola de Proteccion de Datos*' (2014) 14 *HRLR* 761, 764.
19 ibid, 765.
20 T Macaulay, 'What Is the Right to Be Forgotten and Where Did It Come from?' (Techworld, 14 September 2017) <https://www.techworld.com/data/could-right-be-forgotten-put-people-back-in-control-of-their-data-3663849/> accessed 6 April 2019.
21 Meg Leta Jones, *Ctrl + Z: The Right to Be Forgotten* (NYU Press 2016) 10.
22 Case C-131/12 *Google Spain, SL, Google Inc v Agencia Española de Protección de Datos* (ECJ 13 May 2014).
23 E Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgement in Case C-131/12, *Google Spain v Agencia Espanola de Proteccion de Datos*' (2014) 14 *HRLR* 761, 763.
24 ibid, 761.
25 Meg Leta Jones, *Ctrl + Z: The Right to Be Forgotten* (NYU Press 2016) 10.
26 E Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgement in Case C-131/12, *Google Spain v Agencia Espanola de Proteccion de Datos*' (2014) 14 HRLR 761, 762.

European Digital Rights, criticise the ruling, stating that the right to be forgotten outweighs the freedom of expression.[27] Overall, together with other developments, this judgment has created a global controversy.[28]

2.3. Article 17 of the General Data Protection Regulation

The General Data Protection Regulation ('GDPR') was proposed in 2012, adopted in 2016 and implemented in 2018. As the judgement of the ECJ in 2014 set a precedent for the right to be forgotten, this concept was also introduced in Article 17 of the GDPR under the heading 'right to erasure'.[29] Unlike the DP Directive, the GDPR directly applies to all Member States.[30]

Article 17(1) of the GDPR lists six alternative circumstances under which one can claim and enforce the right to be forgotten. They are the following: (a) where the personal data are no longer necessary; (b) where the data subject withdraws their consent; (c) where the data subject objects to the processing and, only applicable to an objection made under Article 21(1) of the GDPR, there are no overriding legitimate grounds for the processing; (d) where the personal data have been unlawfully processed; (e) where the controller is subject to a legal obligation under EU law or national law of a Member State; or (f) where the personal data have been collected in relation to the offer of information society services.[31] It is clear that the right to be forgotten under Article 17(1) of the GDPR has a broad scope, encompassing a great variety of situations in which the right to be forgotten can be invoked.

Article 17(3) of the GDPR, on the other hand, outlines limitations, more precisely situations where different interests or rights prevail over the right to be forgotten. The right to be forgotten is not applicable to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation under EU law or national law of a Member State to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health; (d) for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes; or (e) for the establishment, exercise or defence of legal claims.[32]

---

[27] Herke Kranenborg, 'Google and the Right to Be Forgotten Case Notes' (2015) 1 *EDPL* 70, 74.
[28] D Lindsay, *'The "Right to Be Forgotten" by Search Engines under Data Privacy Law: A Legal and Policy Analysis of the Costeja Decision'* in A T Kenyon (Ed.), '*Comparative Defamation and Privacy Law*' (Cambridge University Press 2016) 221.
[29] —, 'Everything You Need to Know about the "Right to Be Forgotten"' (GDPR.eu, 5 November 2018) <https://gdpr.eu/right-to-be-forgotten/> accessed 27 March 2019.
[30] D Lindsay, '*Emerging Challenges in Privacy Law: The 'Right to Be Forgotten' in European Data Protection Law'* (Cambridge University Press 2014) 290.
[31] Article 17(1)(a)-(f) of the GDPR.
[32] Article 17(3)(a)-(e) of the GDPR.

In case Article 17(1) of the GDPR is invoked and none of the exceptions under Article 17(3) of the GDPR apply, data must be erased in a way which makes it difficult to restore it without excessive effort. In addition, recipients of the erased data should be notified.[33]

3. The US policies regarding the right to be forgotten online

3.1. The First Amendment of the US Constitution

The US is considered to be an anomaly when it comes to the regulation of privacy rights.[34] Unlike in the EU, there is no uniform approach to data privacy regulation in general and this is mainly due to the core function of the First Amendment of the US Constitution. It lists fundamental rights that prevail over other rights, namely freedoms of religion, expression, assembly and the right to petition.[35] The wording is as follows:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.[36]

The relevant part of the First Amendment for the purpose of this paper is the statement that Congress shall not restrict the freedom of speech or the press.[37] The US Constitution does not provide for the right to information privacy, however, the Supreme Court formed the concept of the right to privacy in 1965 in *Griswold v. Connecticut*.[38] It is difficult not to notice that there is an obvious conflict between the constitutional superior right to expression and the right to privacy created by the Supreme Court.[39]

3.2. Functional Equivalents to the Right to Be Forgotten

Even though there is no concept of the right to be forgotten in the US, there are some functional equivalents. Individuals can utilise four legal mechanisms in case they want to limit the availability or reduce their personal data that is already uploaded on the internet. These legal mechanisms are as follows: intellectual property limitations, contractual obligations, defamation and privacy torts. The first category, regulated by the Digital Millennium Copyright Act, is rather limited since it is only applicable to the removal of copyright-protected material.[40] The scope of application of the private torts is rather narrow as well since they address only four situations, namely: (a) intrusion upon seclusion; (b) private information disclosed publicly; (c)

---

[33] Articles 17(2) and 19 of the GDPR.
[34] Meg Leta Jones, *Ctrl + Z: The Right to Be Forgotten* (NYU Press 2016) 10.
[35] —, 'First Amendment' (Legal Information Institute, 5 February 2010) <https://www.law.cornell.edu/constitution/first_amendment> accessed 7 April 2019.
[36] US Constitution, First Amendment.
[37] ibid.
[38] *Griswold v. Connecticut*, 381 U.S. 479 [1965].
[39] Meg Leta Jones, *Ctrl + Z: The Right to Be Forgotten* (NYU Press 2016) 56.
[40] ibid, 57.

misappropriation of name; and (d) false light.[41] Although these legal mechanisms exist, claimants are significantly restricted by the freedom of speech and moreover, the interest of the public prevails over the individual interest.[42] The right to be forgotten applies to data that is irrelevant, defective, outdated, etc. Data controllers, including search engines, such as Google, are not obligated to remove or limit such information in the US since they are granted protection and immunity under Section 230 of the Communication Decency Act.[43] The publishers or data controllers cannot be held liable for what others posted.[44]

3.3. The State of California and the State of New York as Two Pioneers

There are two US States that came the closest to the concept of the right to be forgotten. Firstly, the legislation regarding regrettable content was implemented in 2015 in the State of California, namely Privacy Rights for California Minors in the Digital World. However, it must be noted that it is only applicable to children under 18 years old, and only content that can be accessed by the public, not privately held content, can be removed upon request made by a minor.[45] Furthermore, this legislation is only applicable to the content uploaded by a minor themselves and not by third parties.[46] This Californian law should be regarded as an exception to the norm, since US law is rather reluctant to remove truthful information from the internet. Such removal can often be seen as unconstitutional and as a violation of the First Amendment of the US Constitution.[47]

Secondly, since 2017, efforts have been made to pass Bill A05323.[48] This bill was introduced by the New York State Senator and Assemblyman David Weprin, and its aim is to establish the right to be forgotten. Search engines, but also other publishers, would be obligated to remove any 'inaccurate, irrelevant, inadequate or excessive' personal information.[49] The content and the whole concept of this bill have been heavily influenced by the European concept of the right to be forgotten. It is especially obvious when one considers that the bill also lists cases that limit the right to be forgotten - a feature very much resembling Article 17(3) of the GDPR.[50]

3.4. Other Unsuccessful Attempts and Impediments to the Right to Be Forgotten on Federal Level

The US adopted special protection for children online via the 1988 Children's Privacy Protection Act, however, no right to be forgotten is implemented therein. There was an additional effort made, namely the proposal of the Do Not Track Children amendments to the Children's Privacy Protection Act of 1988.

---

41 ibid, 57.
42 ibid, 59.
43 L Bode and Meg Leta Jones, 'Do Americans Want a Right to Be Forgotten? Estimating Public Support for Digital Erasure Legislation' (2018) 10 *Policy & Internet* 244, 247.
44 A Gajda, 'Privacy, Press, and the Right to Be Forgotten in the United States' (2018) 93 *Washington Law Review* 201, 256.
45 L Bode and Meg Leta Jones, 'Do Americans Want a Right to Be Forgotten? Estimating Public Support for Digital Erasure Legislation' (2018) 10 *Policy & Internet* 244, 248.
46 Meg Leta Jones, *Ctrl + Z: The Right to Be Forgotten* (NYU Press 2016) 68.
47 ibid, 68.
48 Full text of Bill A05323 can be accessed via https://legiscan.com/NY/bill/A05323/2017.
49 Section 1 of Bill A05323.
50 L Bode and Meg Leta Jones, 'Do Americans Want a Right to Be Forgotten? Estimating Public Support for Digital Erasure Legislation' (2018) 10 *Policy & Internet* 244, 247.

Nonetheless, the proposal did not find sufficient support and was, therefore, unsuccessful. The main idea of these amendments was to oblige data controllers to provide minors with the mechanisms to erase their personal information that is publicly accessible.[51]

When it comes to the US system, a rather important factor is also the absence of a designated data protection agency. Most privacy policy making is in the hands of the Federal Trade Commission. The scope of its competencies is, however, limited.[52]

To conclude, individuals in the US currently have very little legal support and very few and limited possibilities to erase their old and/or unwanted information from the digital world.[53]

4. Comparative analysis of the EU and US concepts of the right to be forgotten

From the previous sections, which described the legal instruments concerning the right to be forgotten in the EU and the US respectively, it became clear that both jurisdictions have widely differing attitudes towards the right to be forgotten.[54] One of the possible explanations is that the EU and the US both have different historical, cultural and, most importantly, legal backgrounds. As a result, their attitudes towards the controversial right to be forgotten were ultimately shaped in a very different way.[55]

EU law has recognised and subsequently implemented the right to be forgotten in the form of Article 17 of the GDPR. The right provides persons in the EU with a possibility of erasure of their personal data from search engines and various databases.[56] This clearly shows that the main aim of the EU framework is to safeguard the dignity of individuals rather than to protect against governmental intrusions.

In contrast, US law clearly ensures the reasonable protection of personal data, however, the scope of that protection falls short of the EU.[57] When it comes to the right to be forgotten as such, the US federal legislature is very reluctant to implement such a right in its full application. Nevertheless, some, although very few, characteristics of this right are implemented in US law. Only this limited version of the right to be forgotten is compatible with the US Constitution, more precisely with the First Amendment. The right to have voluntarily uploaded data erased is very much in compliance with the First Amendment.[58] Unlike in the EU, the freedom of expression - a fundamental value of the US - prevails over privacy and therefore, over the

[51] ibid, 248.
[52] L Bode, 'Ready to Forget: American Attitudes toward the Right to Be Forgotten' (2017) 33 *The Information Society* 76, 77.
[53] Meg Leta Jones, *Ctrl + Z: The Right to Be Forgotten* (NYU Press 2016) 67.
[54] S C Bennett, 'The Right to Be Forgotten: Reconciling EU and US Perspectives' (2012) 30 *Berkeley Journal of International Law* 161, 168.
[55] I Stupariu, 'Defining the Right to be Forgotten: A Comparative Analysis between the EU and the US' (2015) *Central European University* 27.
[56] R K Walker, 'The Right to Be Forgotten' 64 *Hastings Law Journal* 257, 261.
[57] ibid, 270.
[58] ibid, 261.

right to be forgotten.[59] This does not mean that EU law does not respect the freedoms of expression and the press and does not regard them as fundamental values. However, the EU aims to balance the interests of both the freedom of expression and the right to privacy.[60] The implementation of the right to be forgotten can be seen as one of the balancing mechanisms, although in the eyes of US lawmakers it is often seen as suppression of the freedom of expression. There is general scepticism towards the adoption of the right to be forgotten in the US, with some even claiming that it is simply impossible for such a right to exist in a country with values such as those of the US.[61] However, there are some elements of US privacy law that can be reconciled with the EU concept of the right to be forgotten.[62] As already elaborated on in the previous section, there are some functional equivalents to the right to be forgotten in the US. What needs to be stressed is that these functional equivalents are not able to appropriately cope with personal data and privacy issues online, which consequently means that there is a significant legal lacuna.[63] In the EU, these issues, which in the US fall into such a legal lacuna, are mainly covered by the GDPR.

The difference in the traditions of both jurisdictions can also be seen in the way in which the courts deal with the issue. In contrast to the US, European courts are more willing to restrict the freedom of speech if that is necessary to protect the rights of an individual, especially one's right to dignity. Therefore, less focus is put on the protection of the freedom of expression from government intervention.[64] In the US, on the contrary, most of these kinds of cases would be overruled by the First Amendment.[65]

5. Conclusion

To conclude, the attitude towards the right to be forgotten largely depends on the country's historical, legal and cultural background as well as the overall privacy policy. This issue can be accurately described as a spectrum with two poles, one pole representing the dignity of an individual and the second pole representing liberty. While EU law is more inclined towards the former pole, the basis of US federal law is the latter one.[66] The EU intervenes in order to protect the privacy and dignity of an individual, while in the US, public and states' interests are regarded as having the highest priority. Therefore, it is understandable why the EU concept of the right to be forgotten in its full application is not implemented in US federal law and why this

[59] S C Bennett, 'The Right to Be Forgotten: Reconciling EU and US Perspectives' (2012) 30 *Berkeley Journal of International Law* 161, 169.
[60] ibid, 173.
[61] Such an argument is proposed by, for example, Timothy Ryan in *The Right to Be Forgotten: Questioning the Nature of Online Privacy* (2011); Jennifer L. Saunders in *Across Jurisdictions and Web Domains, Questions of Privacy and Online Anonymity Persist* (2011); or L. Gordon Crovitz in *Forget Any "Right to be Forgotten"* (2010).
[62] ibid, 167.
[63] R K Walker, 'The Right to Be Forgotten' 64 *Hastings Law Journal* 257, 269.
[64] ibid, 270.
[65] S C Bennett, 'The Right to Be Forgotten: Reconciling EU and US Perspectives' (2012) 30 *Berkeley Journal of International Law* 161, 168.
[66] R K Walker, 'The Right to Be Forgotten' 64 *Hastings Law Journal* 257, 271.

concept would even be regarded as unconstitutional in the US.[67] These diverging approaches result in a visible conflict between these two jurisdictions regarding the issue.

However, one cannot refute the fact that the EU developments regarding personal data and privacy protection have had a significant global influence, likely meaning that uniform standards will soon be needed. Therefore, the discussion between the EU and the US will gradually become inevitable since both jurisdictions will need to agree at least upon minimal personal data protection standards. This gradual harmonisation will most likely influence the difference in the attitudes towards the right to be forgotten and this difference may become less and less significant in the end.

[67] ibid.

COMBATING PANDEMICS:

Effect of South Korea and The Netherlands' Data Privacy Laws on Development of COVID-19 Tracing Apps

Sahel Bahman[1]

Abstract

Over the past years countries have taken several measures to combat the COVID-19 pandemic. One of these measures was the creation of COVID-19 Tracing Apps, intended to trace positive cases and their contacts. Ultimately this has given rise to questions of balancing the health of individuals and their privacy rights. A variety of approaches have been taken by different jurisdictions when creating such apps due to the differing privacy laws. This paper discusses the privacy laws of South Korea and the Netherlands, ultimately portraying how each State balances health and privacy rights respectively.

[1] Sahel Bahman is a LLB student completing the European Law School programme at Maastricht University. She is currently a student tutor at Maastricht University, tutoring the course Introduction to International and European Law. Her legal interests are in the fields of Law and Technology, and in the upcoming academic year she is pursuing the Advanced Master program in Intellectual Property Law and Knowledge Management (LLM).

1. Introduction

The ongoing COVID-19 pandemic, and its spread between and within countries, has revealed a potential for the use of modern privacy laws in public health policy. For countries and health systems alike, the most effective way to understand the severity and prevalence of COVID-19 would be to track positive cases; trace contacts and places PCR-positive cases might have visited or seen. This makes sense, given the exponential nature of viral contamination.[2] However, given the current Information Age, digital data has exposed people to illicit and illegal activities such as fraud, identity theft, or even malign hacking to obtain personal information.[3] Therefore, especially in liberal democracies, data protection laws have been approved and are enforced as they seek to protect the rights of citizens within such democracies.[4] An example of such a democracy is the Netherlands which, as a result of privacy laws such as the European Union's General Data Protection Regulation (GDPR), did not release a tracking and tracing COVID-19 app until the 8 October 2020, almost seven months after initial measures were taken by the government. On the other hand, a COVID-19 app was available in South Korea since March 2020. This is largely due to the amendments South Korea made to their Infectious Disease Prevention and Control Act (IDPCA), World Health Organization, following the MERS epidemic and to their privacy laws in January of 2020. In case of a serious outbreak of a disease, these amendments allowed the government to have more access to data by overriding several privacy laws, including the Personal Information Protection Act 2011 (PIPA). This allowed South Korea to take swift action far sooner during the initial stages of the COVID-19 pandemic, which will be elaborated upon within this paper.[5]

As such, through a comparative methodology, this paper will answer the research question: what are the differences between South Korea and the Netherlands' data privacy laws and how did these affect the development of apps tracking and tracing positive COVID-19 cases? Firstly, it is important to distinguish between tracking and tracing apps. Tracking refers to gaining insights in real time hence, a tracking app will be able to detect a person's current location and the places they have been.[6] On the other hand, tracing is done in retrospect. Tracing apps detect encounters between people through Bluetooth or location and based on the strength of radio signals it is able to detect the distance between people and trace the proximity.[7]

---

[2] World Health Organization, *WHO Director-General's opening remarks at the media briefing on COVID-19* (who.int, 2020) <https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---16-march-2020%20last%20visited%2002/11/2020> accessed 24 March 2022.

[3] Kurt M. Saunders and Bruce Zucker, Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act, 8(3) Article 5, 1999 , *Cornell Journal of Law and Public Policy,* 667-675.

[4] Kevin D. Haggerty and Minas Samatas, *Surveillance and Democracy* (1st Edition, New York; Routledge-Cavendish, 2010) 10, 34.

[5] Sangchul Park and Gina Jeehyun Choic and Haksoo Ko, 'Information Technology-Based Tracing Strategy in Response to COVID-19 in South Korea – Privacy Controversies', Vol. 323, No. 21, June 2020, *The Journal of the American Medical Association;* Chris H. Kang, Sun Hee Kim and Doil Son, *South Korea: Korea Introduces Major Amendment to Data Privayc Laws* (mondaq.com, 2020). <https://www.mondaq.com/privacy-protection/898830/korea-introduces-major-amendments-to-data-privacy-laws> last accessed 19 May 2022.

[6] Björn Greif*, Corona App: What's the Difference between Tracking and Tracing?*, (Cliqz.com, 2020) <https://cliqz.com/en/magazine/corona-app-whats-the-difference-between-tracking-and-tracing> last accessed 19 May 2022.

[7] ibid.

This research paper will start by presenting the contextual information regarding COVID-19 in the Netherlands and South Korea, respectively. Then, the focus will be on a comparison between South Korea's data privacy laws as well as the IDPCA and the Netherlands' data privacy laws, in order to evaluate the effect of legislation on the development of tracking and tracing apps for PCR-positive cases.

2. Covid-19 in South Korea and the Netherlands

South Korea was one of the first countries to be affected by COVID-19, the first case being reported on 20 January 2020. South Korea's initial response to prevent the spread was to impose a special entry procedure which included an entry ban on travellers from high-risk nations and requiring all travellers entering the nation to download a "Self-Diagnosis App" to monitor the development of symptoms. Moreover, 14-day quarantine became mandatory as of 1 April.[8] However, to avoid harsh lockdowns and a complete ban on travel, South Korea adopted a test, trace and treat strategy to control the spread, implemented by April 2020. As a consequence of amended laws following the 2015 MERS outbreak, the government was prepared to deal with an infectious disease.[9] [10]

Conversely, the Netherlands' initial approach to COVID-19 was more moderate, embracing the concept of herd immunity. This was attained through a targeted lockdown which only closed down businesses requiring close contact, whilst leaving open other businesses.[11] The first confirmed case was on February 27, 2020. On 12 March, more measures were introduced to control the spread of COVID-19, including mere encouragements to the Dutch population to social distance, work from home, and the cancellation of gatherings exceeding 100 people. In contrast to South Korea, the Netherlands' initial response was dependent on society to take the initiative and responsibility to control the spread. Although the measures became stricter later, it is important to note the differences in the initial responses to COVID-19 because this is reflective of the flexibility of each jurisdiction's legislation, as will be subsequently discussed in relation to COVID-19 apps.[12]

Both South Korea and the Netherlands are civil law jurisdictions, with South Korea's data privacy laws being compared to the GDPR as used in the Netherlands.[13] However, each jurisdiction has taken a

[8] Coronavirus Disease-19, Republic of Korea, *Korean government's response system (as of February 25, 2020)*, (ncov.mohw.go.kr, 2020) <http://ncov.mohw.go.kr/en/baroView.do?brdId=11&brdGubun=111&dataGubun=&ncvContSeq=&contSeq=&board_id=> last accessed 19 May 2022.
[9] Sangchul Park and Gina Jeehyun Choic and Haksoo Ko (n 4), p. 2129
[10] Ministry of Economy and Finance, *Tackling COVID-19 Health Quaranting and Economic Measures: Korean Experience. Ministry of Economy and Finance of Korea*, (moef.go.kr, 2020)
<https://english.moef.go.kr/pc/selectTbPressCenterDtl.do?boardCd=N0001&seq=4868> last accessed 19 May 2022, 9-14.
[11] Anna Holligan, *Coronavirus: Why Dutch lockdown may be a high-risk strategy*, (BBC News, 2020)
<https://www.bbc.com/news/world-europe-52135814> last accessed 19 May 2022.
[12] The Government of Netherlands *Factsheet: Coronavirus: How Does Contact Tracing Work?,* 18 August 2020.
[13] Chris H. Kang, Sun Hee Kim and Doil Son (n 5).

different approach responding to COVID-19, which is apparent in their data privacy laws and subsequently the process of developing COVID-19 apps.

3. South Korea

3.1. Privacy Law

It is vital to elaborate on the privacy laws in South Korea to then later portray how these were overridden during the COVID-19 pandemic. One of these was the Personal Information Protection Act (PIPA) which entails South Korea's data protection law. Article 1 PIPA states the purpose of the act is to further realise the dignity and value of the individuals by protecting their privacy through prohibiting the unauthorised collection, leak, abuse or misuse of personal information. Personal information is defined in Article 2(1) as information pertaining to any living person that makes it possible to identify such an individual by their name and resident registration number, image, etc. Article 15(1)(1) prohibits the collection, use and disclosure of personal data without prior consent of the individual whose data is involved. However, in January 2020 the Korean National Assembly passed amendments to the PIPA including the addition of a provision to Articles 15 and 17.[14] Article 15(3) and Article 17(4) now allow a personal data controller to use, release and provide personal data and information without consent of a data subject insofar as it is in line with the purpose it was collected for, and measures are taken to secure the encryption.

South Korea's Act on The Protection, Use, Etc. of Location Information further substantiates privacy rights of individuals by aiming to protect privacy from leakage, abuse and misuse of location information.[15] Article 2(1) defines location information as 'information about a place where a portable object or an individual exists or has existed at a certain time, which is collected by the use of telecommunication equipment facilities […]'. Furthermore, Article 2(2) defines personal location information as location information of a specific person. Article 15 is the provision pertaining to the prohibition of collection of location information. Article 15(1) prohibits the collection, use, or provision of location information of an individual or mobile object without the consent of the individual or owner of the mobile object. Therefore, South Korean legislation contains safeguards to ensure protection of location data; however, the extent to which these are adhered to during a health emergency will be discussed throughout this paper.

After the 2015 MERs outbreak in South Korea, the IDPCA was amended to ensure that in case of a health emergency, personal data could be collected to allow for efficient response for controlling the disease. These amendments allowed for public agencies, specifically the Korea Centres for Disease Control and Prevention (KCDC), to collect and share seven categories of data of (suspected to be) infected individuals

[14] ibid.
[15] South Korea's Act on the Protection, Use, Etc. of Location Information, art 1.

with the central, municipal or local governments, national health insurance agencies and healthcare professionals.[16]

The IDPCA aims to control infectious diseases through necessary means in order to maintain citizen's health.[17]Article 2(1) IDPCA provides a series of definitions of an infectious disease. COVID-19 would be categorised as a Group 5 'infectious disease under surveillance by the World Health Organization (WHO)'. This is further defined by Article 2(8) IDPCA stating that such an infection means that it was designated to be subject to surveillance by the WHO to prepare for an international public health emergency, as announced by the Minister of Health and Welfare. In March 2020, the WHO Director-General announced that COVID-19 is characterised as a pandemic, thereby falling under the aforementioned definition.[18]

3.2. Tracking and Tracing

South Korea's approach to controlling the pandemic is a "Test, Trace, Treat"[19] approach. Tracing methods will be elaborated upon in this section in order to assess how the IDPCA allowed for the setting aside of data privacy laws during the pandemic.

Contact tracing is conducted through an app which identifies the movements of confirmed patients through location data.[20] This allows for authorities to ensure these patients are complying with self-isolation as well as allowing for the tracing of who the patients were in contact with and consequently may have infected.[21] Prior to this, the KCDC investigators had to request data such as credit card transaction history of confirmed patients from police investigators which required a waiting period, and thus took longer. The current system allows for various data to be analysed immediately and given to health investigators.[22]

The IDPCA requires the release of virus carrier travel logs. Article 34-2(1) IDPCA states that citizens should be provided with detailed information about patients with infectious disease. This includes their

---

16 Sangchul Park and Gina Jeehyun Choic and Haksoo Ko (n 4), 2129.
17 Infectious Disease Prevention and Control Act as translated in: Korea Law Translation Center; Infectious Disease Control and Prevention Act 2015 [English]
<https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=172762&viewCls=engLsInfoR&urlMode=engLsInfoR&chrClsCd=010203#0000> last accessed 19 May 2022.
18 World Health Organization, *WHO Director-General's opening remarks at the media briefing on COVID-19* (who.int, 2020)
<https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020> last accessed 19 May 2022.
19 Ministry of Economy and Finance (n 10).
20 ibid, 13.
21 Ministry of Foreign Affairs Korea, *한국의 코로나19 대응: 코로나 바이러스 추적 Korea's Response to COVID-19: How it Tracks Down the Coronavirus* (moda.go.kr, 31 May 2020)
<https://www.mofa.go.kr/eng/brd/m_22744/view.do?seq=6&srchFr=&amp%3bsrchTo=&amp%3bsrchWord=&amp%3bsrchTp=&amp%3bmulti_itm_seq=0&amp%3bitm_seq_1=0&amp%3bitm_seq_2=0&amp%3bcompany_cd=&amp%3bcompany_nm=&page=1&titleNm=> last accessed 19 May 2022; Ministry of Economy and Finance (n10), 13.
22 Sarah Wray, *South Korea to step-up online coronavirus tracking* (SmartCitiesWorld, 2020)
<https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109> last accessed 19 May 2022.

movements and contacts once the alert levels are at "precautions" or above. Therefore, in the case of COVID-19, it is explicitly required by the IDPCA that the population should be informed if they have been in contact with a PCR-positive person.

Article 34-2(1) IDCPA requires the release of detailed information to citizens in order to acquaint them with the measures taken for preventing the infectious disease. The KCDC published guidelines stating the period of disclosure of data is from one day before symptoms began to the date of quarantine. If there were no symptoms then location information will be disclosed from one day prior to the date of quarantine; hence, providing protection to personal data by limiting the period of time which data can be collected from. Additionally, the KCDC emphasized that personally identifiable information must be excluded in order to guarantee that there would be no violation of Article 15(1)(1) PIPA. Moreover, data must be deleted 14 days from the last contact and the data is anonymised by converting personal information regarding location like address into random long strings of four characters.[23] To further guarantee protection of personal information data as specified under Article 15(1)(1) PIPA, the data is anonymised, and its collection is limited in duration and scope. If a person has been in contact with a Covid-positive individual, they will receive a notification from the app which informs them that they may have been infected, as required by Article 34-2(1) IDPCA. Hence, anonymity of the patient is maintained while still allowing for the possibly infected person to get tested and treated.[24]

The provision to request to provide information is laid down in Article 76-2 IDPCA. Article 76-2(1) IDPCA states that the Minister of Health and Welfare or the Director of the KCDC may, if necessary to prevent the spread of infectious diseases, ask central administrative agencies, heads of local government, medical institutions, pharmacies, corporations and individuals to provide information of patients with infectious diseases and those likely to be infected. Hence, for the purposes of preventing the spread of an infectious disease such as COVID-19, the Act allows for public agencies to collect the information of patients as well as individuals who may get infected as a result of contact with infected persons. One of the types of information that can be collected is outlined in Article 76-2(1)(2) IDPCA: personal information including names, resident registration numbers, addresses and telephone numbers. As previously stated, Article 15(1)(1) PIPA prohibits collecting individuals' personal information without their consent; however, in case of a health emergency, like COVID-19, the IDPCA allows for the PIPA to be overridden.

With regards to location information, Article 76-2(2) IDPCA states that if it is necessary for the prevention of infectious diseases and their spread, the Minister of Health and Welfare may request the National Police Agency, regional police agency and police stations to provide location of information of

[23] Gyuwon Jung, Hyunsoo Lee, Auk Kim and Uichin Lee, Too Much Information: Assessing Privacy Risks of Contact Trase Data Disclosure on People With COVID-19 in South Korea, 2020, *Frontiers in Public Health* <https://www.frontiersin.org/articles/10.3389/fpubh.2020.00305/full> last accessed 10 October 2020.
[24] Ministry of Economy and Finance (n10), 13; Ministry of Foreign Affairs Korea (n 21).

patients with the infectious disease and persons who are likely to be infected by an infectious disease. This provision explicitly allows for this information to be collected notwithstanding Article 15 of the Act on the Protection, Use, etc. of Location Information. Article 15 had been amended in December 2015, illustrating how the IDPCA was revised to allow for overriding of privacy laws in favour of public health. Consequently, this allows for tracing apps to be developed at a faster rate because adherence to privacy laws was not a strict requirement.

4. Netherlands

4.1. Privacy Law

In contrast to South Korea, which follows its own data privacy Acts, the Netherlands' data privacy law is based on the GDPR. EU regulations have direct effect across all EU Member States, thus, requiring each jurisdiction to comply with the regulation.[25] Based on Article 93 Dutch Civil Code (BW), the Netherlands is a monist country meaning international law becomes part of its domestic legal order, hence it is directly applicable in the same manner domestic law would be. The Netherlands' privacy law must first be discussed prior to elaborating on its effect on the development of COVID-19 apps.

Article 1 GDPR states the objectives of the regulation, including protection of natural persons with regard to processing of personal data. Additionally, it regulates rules relating to the free movement of personal data and protects fundamental rights and freedoms of natural persons, specifically their right to the protection of personal data. Article 4(1) GDPR defines personal data as any information relating to an identified or identifiable natural person. It further defines an identifiable natural person as one who can either directly or indirectly be identified through identifiers such as a name or location data. Article 4 GDPR's definition of personal data is comparable to Article 2(1) of South Korea's PIPA's definition of personal information.

Comparably to South Korea's PIPA, Article 6(1)(a) GDPR states that processing is only lawful if the data subject has given consent to the processing of his or her data. Furthermore, processing is also lawful if it is necessary for the performance of a task carried out in the public interest, in accordance with article 6(1)(e) GDPR. Additionally, Article 9(1) GDPR prohibits processing of personal data concerning health. The only exceptions to this are provided for in Article 9(2); subsection 1 specifies that paragraph 1 does not apply if the data subject has given explicit consent to the processing of those personal data.

Article 17 GDPR provides for the right to erasure or right to be forgotten, comparable to South Korea KCDC's guidelines to delete data 14 days after final contact. The data subject has the right of erasure of personal data concerning him or her without undue delay and the controller must erase the personal data

[25] Consolidated version of the *Treaty on the Functioning of the European Union,* 2016, OJ 2020, art 288.

also without undue delay. Therefore, in both jurisdictions a similar protection of the data subject is provided regarding storing of data. The conditions for consent are laid down in Articles 4(11) and 7 GDPR, specifically that it must be 'freely given, specific, informed and unambiguous.' Pursuant to the latter provision, the request for consent must also be 'clearly distinguishable from other matters' and presented in 'clear and plain language.'

In summary, the Netherlands' privacy laws share similarities to South Korea on the surface; however, differences arise regarding the flexibility, which will be discussed in the following sections.

4.2. Tracking and Tracing

Pursuant to Article 21 GDPR, the data subject has the right to object at any time to the processing of personal data that concerns him or her, based on Article 6(1)(e). This provision highlights a contrast between the Netherlands and South Korea. South Korea allows for overriding of the consent requirement with regards to collection of personal data and lacks the right to refuse profiling. Contrastingly, in the Netherlands, in accordance with the GDPR, without the consent of the data subject, collection of personal data is not possible. As a result, this emphasises the requirement for user anonymity within the COVID app in the Netherlands.

Article 68(1) GDPR establishes the European Data Protection Board (EDPB) as a body of the EU with legal personality. The EDPB released a statement regarding processing e-communication data, stating that (location) tracking is only allowed if it is anonymous or conducted with consent of the subject.[26] Therefore, anonymity is a crucial requirement. As a result, all COVID-19 app prototypes presented to the Dutch government had to meet anonymity requirements. However, in April, the State Attorney conducted a privacy analysis on seven prototypes of COVID-19 apps which he concluded did not guarantee complete anonymity and were thus rejected.[27] This problem continued into August when the Dutch privacy watchdog, Autoriteit Persoonsgegevens, stated that the privacy of users of the COVID-19 app was still not sufficiently guaranteed.[28] Here, the Netherlands' contrast with South Korea is evident. South Korea's laws allowed for overriding of data privacy laws in case of a health emergency, whereas the Netherlands, as an EU Member State, is obliged to adhere to the GDPR, hence restricting its ability to create such apps at a faster rate.

---

[26] Andrea Jelinek*, Statement on the processing of personal data in the context of the COVID-19 outbreak*, (European Data Protection Board, 2020_<https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf>_last accessed 6 September 2020.

[27] Gerrit-Jan Zwenne and Marte van Graafeiland, *Openbare samenvatting privacyanalyses bron- en contactonderzoekapps* (Pels Rijcken, 2020) <https://www.rijksoverheid.nl/onderwerpen/coronavirus-app/documenten/publicaties/2020/04/19/samenvatting-privacy-analyse-contactonderzoeksapps> last accessed 6 September 2020, 3.

[28] Autoriteit Persoonsgegevens, *DPA: Privacy of coronavirus app users not yet sufficiently guaranteed,* (Autoriteit Persoonsgegevens, 2020) <https://autoriteitpersoonsgegevens.nl/en/news/dpa-privacy-coronavirus-app-users-not-yet-sufficiently-guaranteed> last visited 10 October 2020.

Prior to the development of the current COVID-19 app, if a person tested positive the Municipal Health Service (GGD) would contact them and question who the person has been in contact with. A list of contacts would be made including, household members, close contacts, and contacts who were in the same space as the infected person.[29] Although this method still allowed for contacts to be identified and tested, it still left room for error. It was highly dependent on the patient's memory and according to psychological studies of Bartlett et al. 1932, a person's memory is never completely reliable and can be prone to reconstruction.[30] Therefore, the establishment of the Bluetooth based contact tracing app will allow for a more efficient method to identify and alert close contacts of positive cases, without risking interference with data privacy.

As of October 2020, The Netherlands' COVID app, CoronaMelder, is available for download and can be installed and used voluntarily. CoronaMelder is an app which will alert a user if they have been in close proximity, for more than 15 minutes, to someone who has tested PCR-positive. The tracing app uses Bluetooth and detects how close someone is based on how strong the Bluetooth signal is. No location data is used by the app hence, ensuring location data privacy of the user.[31] Similarly to South Korea's COVID app, CoronaMelder exchanges random codes with other phones and therefore, does not exchange any personal or location information of the user[32]. Consequently, the current app ensures complete anonymity of the user thus, maintaining the privacy of the user and ultimately not requiring any form of consent as no personal data is obtained. Subsequently, there is complete adherence to the GDPR by the Netherlands.

5. Comparative Overview

An important contrast to be noted is the fact that the tracing app in the Netherlands uses Bluetooth in order to inform those who have been in contact with patients whereas in South Korea the app uses location data. Although it is anonymised in both countries when informing the contacts, in South Korea authorities can easily access a person's location data, whereas in the Netherlands it is merely based on Bluetooth signals, hence providing more extensive protection of privacy and anonymity. Therefore, although South Korea developed the COVID-19 app at a faster pace, the Netherlands was able to ensure more protection of data privacy.

Moreover, regarding the pace of development of a tracing app, South Korean legislation reduces limitations provided by privacy laws which allowed the authorities to provide a tracing app to their citizens seven months earlier than the Netherlands. An example of such legislation in South Korea is the

[29] Government of The Netherlands (n12).
[30] Frederic Bartlett, *Remembering: A study in experimental and social psychology.* (Cambridge, UK: Cambridge University Press, 1932), 203 & 213.
[31] CoronaMedler, *Stop the spread of the coronavirus, download CoronaMedler*, (CoronaMedler, s.d..) <https://coronamelder.nl/en> last accessed 19 May 2022.
[32] ibid, button FAQ, button 'What about my privacy?'.

aforementioned Article 34-2 IDPCA, stating that the Minister of Health and Welfare must disclose various items of information required for preventing the spread of the infectious disease, including information regarding contacts of patients. On the other hand, the Netherlands has no such law as it must adhere to the laws of the EU which require consent, and if not acquired, anonymity must be ensured regarding processing and sharing of personal data. Therefore, the fact that South Korea is able to override their data privacy laws whilst the Netherlands must adhere to data privacy laws even during a health emergency, allowed for South Korea to have a simpler process of implementing a tracing app to trace contacts of PCR-positive cases, in comparison to the Netherlands who had to ensure absolute anonymity of patients and their contacts before such an app could be created.

These differences may exist as a result of different priorities between the jurisdictions. In South Korea, the MERS outbreak resulted in the authorities prioritising public health over privacy in order to ensure the control of the spread of an infectious disease, as reflected in their amendments to allow the overriding of privacy law. On the other hand, the Netherlands, or more specifically the EU, seems to prioritise personal privacy which may be a result of the dangers that come with the Information Age or it may be due to the country not experiencing an infectious disease in its recent years to the extent that South Korea did.[33] This is reflected in the difference between the extent of data privacy protection in each country regarding the app, as South Korea uses location data whilst the Netherlands uses Bluetooth data. Hence, the Netherlands offers more data privacy protection, at the loss of having the app produced almost seven months later than South Korea's. The WHO's director-general has stated the positive impact that tracing apps have by allowing efficient contact tracing which is one of the 'backbone[s] of the [COVID-19] response'.[34] Therefore, the attempt to balance public health and data privacy may cause hindrance to the COVID-19 response and ultimately tip such a balance to favour data privacy. Consequently, the question that has arisen to legal systems across the world, as a result of the COVID-19 pandemic, is what must be prioritised and whether in the future new approaches must be taken regarding data privacy. Countries which have had worse conditions may choose to shift their focus from a balance between public health and data privacy to prioritising public health whilst others may attempt to maintain the balance, which ultimately prioritises data privacy.[35]

[33] History.com Editors, *Pandemics That Changed History,* (History.com, 2020) <https://www.history.com/topics/middle-ages/pandemics-timeline> last accessed 19 May 2022.
[34] World Health Organization (n 1).
[35] Alfred Ng, *Coronavirus pandemic changes how your privacy is protected*, (Cnet, 2020) <https://www.cnet.com/health/coronavirus-pandemic-changes-how-your-privacy-is-protected/> last accessed 19 May 2022.

6. Conclusion

In summary, South Korea and the Netherlands share some similarities in their legislation regarding data privacy. This includes the applicable privacy laws of both countries, which emphasise the importance of consent before access to data is granted, as portrayed in Article 15(1)1 PIPA and in Article 6(1)(a) GDPR, respectively. However, a significant difference still exists regarding the possibility of revoking previously given consent. The Netherlands allows for data subjects to object to the processing of personal data concerning them personally at any point. In contrast in South Korea, there is no comparable provision in any of the relevant data privacy legislation. As a result, the relevant authorities in South Korea can continuously process individuals' data once initial consent has been provided, unlike in the Netherlands where authorities must take into account revocation of consent. Consequently, the processing of data in South Korea can be facilitated by the authorities at a faster pace, as there are no issues which may potentially arise from revocation of consent. Therefore, despite its similarities, differences do arise in each jurisdiction which ultimately affected the pace of COVID-19 app development.

To conclude, the abovementioned differences between South Korea and the Netherlands in this paper are: revocation of consent, the flexibility of privacy laws, and the impact this had on the development of the apps. The most significant difference is the flexibility of privacy laws, meaning that South Korea did not have to adhere to as many limitations in the grey area where public health and privacy intersect. This allowed the South Korean authorities to develop and implement a tracing app during the early stages of the spread of the disease. The Netherlands on the other hand is required to adhere to the data privacy laws provided by the EU and consequently had to develop several prototypes before the final app could ensure complete compliance with legal requirements. Therefore, the differences between each jurisdiction resulted in track and trace apps for COVID-19 to be developed at a considerably different pace.

AI, LAW ENFORCEMENT AND PRIVACY:
Does the GDPR Sufficiently Regulate for Automated Decisions Based on Predictive Policing Profiling?

Laura Higgins Mulcahy[1]

Abstract

Predictive policing is defined as 'any policing strategy or tactic that develops and uses information and advanced analysis to inform forward-thinking crime prevention'.[2] These activities, incorporated with profiling and automated decision-making technologies, allow for policing tactics and orchestrated initiatives to be aided by the precision and efficacy of artificial intelligence to organise and execute policing forecasts and procedures. Automated decision making in the area of policing can be further incorporated into strategic planning and prioritising either on a macro-level regarding operational intelligence or on a micro-level to make risk assessments in relation to individuals. Broadly speaking, there are two main avenues that automated predictive policing tools can take. One avenue is to make aticsystemic decisions relating to geolocations of crimes to draw links between places and events and predict where and when crimes are more likely to happen. The other, more contentious avenue, is using artificial intelligence to forecast potential perpetrators of crime and to predict who has a higher chance of being involved in future criminal activity. This type of automated profiling can draw on data such as gender, ethnicity and more, and it is this type of data analysis that understandably holds concern for EU data protection law. Whilst acknowledging the European fundamental rights *acquis* including the European Charter for Fundamental Rights and the European Convention on Human Rights,[3] [4] it is the General Data Protection Regulation which is the main regulatory armour that ought to be analysed when addressing such data privacy issues of data subjects *vis-a-vis* predictive policing profiling.[5] This article will evaluate whether the Regulation satisfies the objectives of data protection in the area of predictive policing profiling and give commentary as to its effect and potential regulatory mitigation strategies.

[1] Author is a Law and Technology LLM student currently studying at Utrecht University.

[2] Aleš Završnik, 'Criminal Justice, Artificial Intelligence Systems, and Human Rights' (2020) 20 ERA Forum 567 < https://doi.org/10.1007/s12027-020-00602-0> accessed 11 February 2022.

[3] Charter of Fundamental Rights of the European Union (2000).

[4] European Convention on Human Rights Act (1950).

[5] Regulation (EU) 2016/679 of the European Parliament (EP) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1. Introduction

As a result of globalised digitalisation and innovative artificial intelligence techniques, automated decision-making (ADM) has infiltrated almost every aspect of society, from assessing the creditworthiness of borrowers to the welfare allocation of citizens. ADM in the area of law enforcement activities and procedures has been generally welcomed by law enforcement actors in light of slicker internet crime techniques such as hacking and scamming, online terrorist propaganda and child abuse material dissemination. The influx of novel crime techniques has spurred the application of ADM particularly in the area of predictive policing.[6] However, when a decision is made by AI, it is harder to pinpoint where the accountability lies. In the US, the data mining company Palantir provided software to a New Orleans Police Department programme so they could survey all of the citizens in the community.[7] The software used a variety of data, including social media data, to predict the likelihood that individuals would commit acts of violence or become victims.[8] Palantir's prediction model was described to be 'as if New Orleans were contracting its own version of the NSA to conduct 24/7 surveillance of the lives of its people'.[9] Yet regardless of the pervasive existence of this artificial intelligence (AI) monitoring, it was reported that this type of surveillance went completely under the New Orleans community radar, with not even city council members knowing about it. This type of surveillance is not far off European shores, as it has been reported that in Germany, Palantir has contacts with police forces in various states such as Hesse and North Rhine-Westphalia for the sautilization of their software program Gotham. It is therefore imperative to regulate stringently and avoid the numerous implications ranging from consequent privacy infringements. If these technologies are not heavily monitored, so-called 'chilling effects' may occur, creating a deep mistrust of citizens towards law enforcement and governmental actors, resulting in the fragmentation of society as a whole. It is therefore necessary to dissect the General Data Protection Regulation (GDPR) in order to ensure that technologies such as profiling and automated decision making in the area of predictive policing are inherently protected under its regulatory framework.[10]

2. Predictive Policing and Personal Data Usage

The GDPR lays down rules for the protection of natural persons concerning the processing of their personal data. Personal Data under Articles 4(1) is defined as 'any information relating to an identified or identifiable natural person'.[11] From this reading, the definition of personal data has three constituent elements: (1) any information that (2) relates to (3) an identified or identifiable person. The Article 29 Working Party has

[6] Završnik (n 2).
[7] M. Smith, 'New Orleans alleged to have secretly used Palantir predictive policing' (*CSO*, 28 February 2018) <https://www.csoonline.com/article/3259445/new-orleans-alleged-to-have-secretly-used-palantir-predictive-policing.html> accessed 6 April 2022.
[8] ibid.
[9] ibid.
[10] GDPR (n 5).
[11] ibid art 4(1).

advised that each of these three elements should be interpreted expansively.[12] It thus suggests that *any information* can also include information that would be considered *private* for the purposes of the right to respect for private life. The CJEU stated in Nowak that the expression of *any information* is used to reflect the legislature's aim to 'assign a wide scope to that concept'.[13] Acknowledging this, a data subject can be 'identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[14] In the context of predictive policing profiling, personal data such as names, geographical and social data are all data elements that relate to an individual and that renders an individual as identifiable. Therefore, it would seem that any type of personal data used for purposes of predictive policing can be justified under the expansive criteria of Article 4. However, in order to process personal data of a data subject, or in this context a suspect, there must be a purpose in the form of a legal basis. Article 6 governs the legal basis for personal data. It is questionable under what criteria the processing of personal data in the context of predictive policing profiling could establish a legal basis. The GDPR allows Member States to enact limitations to specified provisions in certain contexts, notably when it is necessary to reconcile data protection rights and restrict the application of data protection principles to pursue specified purposes such as national security, defence, public security and law enforcement.[15] This is pertinent to the area of predictive policing and data usage as already it can be identified that the processing of personal data in this context is subject to a flexing of the rules laid out in Article 6 of the GDPR.

3. Profiling and Predictive Policing

Profiling under the GDPR is defined under Article 4(4) as:

> any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[16]

In the instance of predictive policing, the data subjects concerned would be those considered to be suspects in police investigations whose data is used to profile them as criminal offenders. As can be seen from the definition under Article 4 paragraph 4, profiling is an applicable concept that entails the automated processing of personal data for the purpose of evaluating personal aspects to aid decision making about a data subject.[17]

---

[12] Article 29 Working Party, 'Guidance from the European Data Protection Board' (*Data Protection Commission)* <https://www.dataprotection.ie/en/dpc-guidance/guidance-from-the-european-data-protection-board> accessed 11 February 2022.

[13] Case C-434/16 *Peter Nowak v Data Protection Commissioner* (2017), para 34.

[14] Smith (n 7).

[15] GDPR (supra n5) Article 23(a)-(d).

[16] ibid Article 4(4).

[17] ibid Article 22(4).

Under the GDPR, the concept of ADM overlaps with profiling as they both act on three types of data: data provided by the individual, data observed the process of making a decision by automated means without any human involvement and inferred data.[18] There is a clear interplay between ADM and profiling, so they can be viewed together when analysing the GDPR.

4. Automated Decision Making and Predictive Policing

Article 22 of the GDPR states,

> The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The guidelines of the Article 29 Data Protection Working Party state for data processing to significantly affect someone the effects of the processing must be that the decision has 'the potential to significantly affect the circumstances, behaviour or choices of the data subjects; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals'.[19] Without question, automated decisions in the context of predictive policing could affect the lives of data subjects, have a long-term impact on them and in the case of biased data sets, result in discrimination of individuals. That would mean predictive policing under Article 22(1) of the GDPR is prohibited. However, a lacuna exists the more that Article 22 is examined. Article 22(2) states that Article 22(1) shall not apply based on several exceptions. These exceptions include contract necessity, explicit consent of the data subject and special categories of data. Article 22(4) goes on to state that:

> Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

5. Exception under Article 9

Article 9(1) states that:

> The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data,
> biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

However, this prohibition shall not apply under exceptions listed in Article 9(2). Article 9(2)(a) states that one of the exceptions are if 'the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the

[18] Smith (n 7).
[19] Working Party (n 12).

prohibition referred to in paragraph 1 may not be lifted by the data subject'.[20] As data subjects (or victims of a police investigation) will most likely not provide their explicit consent to be profiled, Article 9(g) is the most appropriate to use in this case. Article 9(2)(g) further relates to necessary processing purposes for public interest reasons. It also details that processing should be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[21]

Applying the criteria under 9(g) is necessary, and step-by-step approach is helpful. In order to justify the processing of personal data revealing racial or ethnic origin etc., the criteria to satisfy are whether it is necessary for reasons of substantial public interest, if there is a legal basis under Member State law, if it respects the essence of the right to data protection and if there are suitable and specific measures in place to safeguard the fundamental rights, freedoms and interests of the data subject. If these criteria are fulfilled, then a data subject shall not have a right to not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affecting them.

6. Analysis of the Exception Criteria

In order to fully grasp the gravity of the aforementioned criteria, it is relevant to answer these questions in the context of predictive policing. Firstly, is predictive policing profiling necessary for reasons of substantial public interest? It can be argued that perhaps profiling in the context of predictive policing is necessary for crime prevention and for the protection of the general public against potential criminals. However, whether it respects the essence of the right to data protection, this type of profiling is arguably quite invasive, especially if there is no legal basis given on behalf of a suspect to use this data under Article 4(1). The criteria for establishing suitable and specific measures to safeguard the fundamental rights of the data subject is where predictive policing profiling is quite contentious. This is because the usage of data to profile in this context can label individuals as a criminal, which would inevitably affect their personal life in the case of employment, relationships, and general reputation. This could lead to an infringement on their private and family life, which is protected under Article 8 of the Charter for Fundamental Rights.[22] Notwithstanding the fact that falsely identifying an individual as a criminal could result in biased and discriminatory outcomes, reiterated by the report of the Civil Liberties Committee.[23]

In summary, there seems to be more disadvantages compared to advantages when justifying any sort of exception under Article 22 for the purposes of predictive policing. The European Digital Rights Group

[20] GDPR (n 5).
[21] ibid art 9(g).
[22] CFREU (n 3).
[23] Committee on Civil Liberties, Justice and Home Affairs, 'Draft Report on the Commission's 2021 Rule of Law Report' (2021/2180(INI) <https://www.europarl.europa.eu/doceo/document/LIBE-PR-704642_EN.pdf> accessed 11 February 2022.

criticises the dilution of the right not to be subjected to automated decisions in Article 22, stating, 'through profiling, highly sensitive details can be inferred or predicted from seemingly uninteresting data, leading to detailed and comprehensive profiles that may or may not be accurate or fair.'[24]

This dilution can be exhibited in the following breakdown of the articles as detailed in the earlier passages; Article 22(1) prohibits solely automated decision making but Article 22(2) gives exceptions to this prohibition. Article 22(4) states that's special categories of data cannot be permitted in this exception except in situations that comply with 9(2)(a) or 9(2)(g). Article 9(1) prohibits *inter alia* processing of personal data based on racial or ethnic origin but Article 9(2) permits exceptions to this prohibition. Article 9(2)(a) states that one of the exceptions is explicit consent (not applicable to predictive policing. Article 9(2)(g) further states one of the exceptions could be based on the necessity to substantiate public interest under Member State law which could indirectly be applied to predictive policing and the prevention of crime and leaving this exception up to each Member State for consideration. Therefore, a Member State can decide that a solely automated decision is permissible based on racial and ethnic origin, and it does not violate the GDPR if it is necessary for reasons of substantial public interest, based on Union or Member State law. The principles of being necessary and for public interest are two nuanced terms that provide Member States with substantial power in the realm of predictive police profiling.

7. Criticism

To elucidate this observation, in 2021 members of the European Parliament passed a resolution to endorse the report of the Civil Liberties Committee.[25] The report expresses opposition to the use of predictive policing tools which operate on artificial intelligence software that make predictions about the behaviour of individuals or groups 'on the basis of historical data and past behaviour, group membership, location, or any other such characteristics.'[26] This opposition is based on the fact that predictive policing tools cannot make reliable predictions about the behaviour of individuals.[27] Although this resolution is non-binding, the opinion of the European Parliament relatively reflects verbatim the previously addressed weaknesses of the GDPR which can inevitably spill over into real world scenarios of victims of unregulated data processing. It stands to reason that AI cannot predict with accuracy someone's propensity to commit a crime because 'data has both homogenous and heterogenous character'.[28] Similarly, where automated processing is permitted under the exceptions, the data controller must implement suitable measures to safeguard the data subject's rights and

[24] Privacy International, 'Data Is Power: Profiling and Automated Decision-Making in GDPR' (2017) https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr> accessed 22 April 2022.
[25] ibid, 21.
[26] ibid.
[27] ibid.
[28] ibid.

freedoms and legitimate interests, the right to obtain human intervention on the part of the controller, to express their point of view and to contest the decision.

8. Conclusion

Whilst Europe has been slow in its adoption of predictive policing technologies, there has already been backlash regarding its usage. An application of Pol-Intel in Denmark has faced recent scrutiny by yielding 'inaccurate and false results […] on the premise of historical data already skewed towards certain ethnic designations based on pre-existing discriminatory practice'.[29] This method used by law enforcement authorities in Denmark controversially determined that residential areas with more low-income non-Western Danes than Western Danes, were to be understood as ghettos. In other words, the socio-economic circumstances of the Black and Brown poor was to be made synonymous with their ethnic makeup and ultimately 'gave physical expression to what had remained an unspoken Danish reality of institutional racism'.[30] With the interplay between ADM and policing techniques gaining traction in Europe, it is important to ensure that they are regulated, and do not infringe the fundamental rights such as right to non-discrimination as demonstrated in Denmark. Demonstrably, the ostensible capability of these technologies to predict future criminal outcomes based on big data analytics can have an array of issues from discriminatory outcomes to a lack of data protections. The crux of the issue is that whilst these technologies can have a positive impact on law enforcement procedures, there is simply not sufficient regulation under the GDPR for the protection of data subjects to justify the activity. One software developer has been quoted saying, 'if I recognise patterns, I can look into the future, and when I can look into the future, I can shape the future'.[31] This can be read in both an optimistic or ominous tone, depending on how the future is perceived. With predictive policing ADM, yes, there could be more people surveilled and a higher level of police protection, but there in turn could also be severe discrimination and data rights infringements. Taking into account the previously outlined criteria for the GDPR to apply to ADM and predictive policing profiling, regulatory mitigation should remove the lacuna permitted by the dilution of Article 22 and account for the regulatory lacunas before predictive policing ironically becomes a lawless law enforcement tactic in Europe.

[29] N.T. 'NoTechFor: Forced Assimilation' (*No Tech For Tyrants,* July 2020) <https://notechfortyrants.org/2020/07/13/notechfor-forced-assimilation/> accessed 11th February 2022.
[30] ibid.
[31] Mareile Kaufmann, Simon Egbert, Matthias Leese, *'Predictive Policing and the Politics of Patterns'* (2019) The British Journal of Criminology 59 (3), 674–692.

A SCRATCH ON THE SOUL:

To What Extent is the Uncertainty of Applying Article 82(1) for the Assessment of Immaterial Damage Detrimental to the Ability of Data Subjects to Successfully Claim Immaterial Damages under the GDPR?

Kristijan Pejikj[1]
Rijk Rouppe van der Voort[2]
Imane Faïza Wijsman[3]

Abstract

Since its adoption, the General Data Protection Regulation (GDPR) has established itself as one of the main legislative acts of the European Union and a forefront of the so-called Brussels effect. However, despite its extensive reach, not every aspect of its provisions has been clear-cut. For example, claiming compensation for material damage has already been established in practice without much ambiguity, as to under which circumstances compensation can be claimed and how the amount to be awarded should be assessed. Conversely, claiming such compensation for immaterial damage has been surrounded with uncertainty. Article 82(1) GDPR provisions the right to compensation for data subjects who have suffered material or immaterial damage from a data controller who has infringed upon the GDPR. However, the concept of damage itself is not defined in the GDPR; only Recital 146 stipulates that its interpretation should be taken in light of CJEU case law. But this position of the GDPR is the cause for much uncertainty - how can there be reliance on case law when such case law is - at present - almost non-existent? This paper examines whether this uncertainty is detrimental to the ability of data subjects to successfully claim immaterial damages under the GDPR.

[1] Kristijan Pejikj is an LL.M. candidate in Law and Technology in Europe at Utrecht University. He already holds an LL.M. in Commercial Law from the University of Ss Cyril and Methodius, Skopje, and has passed the bar exam in North Macedonia. His current focus is on the detrimental effect of exploitative nudging algorithms used by Big Tech companies on consumers.
[2] Rijk Rouppe van der Voort is an LL.M. candidate in Law and Technology in Europe at Utrecht University. He holds an LL.B. in Dutch Law with a Minor in Law, Innovation and Technology from Utrecht University. His latest interest is the legality of the use of consent pop-ups in light of the GDPR.
[3] Imane Faïza Wijsman is an LL.M. candidate in Law and Technology in Europe at Utrecht University. She also holds an LL.B. in Dutch Law with a Minor in International Relations and Human Rights Law and an LL.M. in International and European Union Law from the Erasmus University Rotterdam. She focuses on the effect of and protection against cyber-attacks on the public services of states in the European Union.

1. Introduction

Imagine a hacker phished bank credentials from an individual due to insufficient safety measures of the bank. In its capacity as a data controller, the bank is required to implement adequate security measures to protect its customers (i.e., the data subjects). Under Article 82(1) of the General Data Protection Regulation (GDPR),[4] data subjects have the right to claim compensation for both material and immaterial damage they have suffered because of a GDPR infringement by the data controller or processor. If the individual actually suffered a monetary loss due to the phishing attack, they would have no issue claiming their loss, provided that the loss is clear, identifiable, and attributable.[5] This demonstrates that the rules for claiming material damages have already been well established in European legal systems; therefore, claiming such damages under the GDPR has not been contested much.[6]

Conversely, the legal framework for immaterial damages under the GDPR remains rather divisive - the absence of a thoroughly defined regime for claiming immaterial damages leads to an uncertain and unclear application of the concept. Does the potential fear of ever using a bank again, resulting from this uncertainty, also grant individuals the right to claim immaterial damages?

This ambiguity leads to discrepancies between different EU Member States' approaches in the application of Article 82(1) for awarding immaterial damage claims vis-à-vis the GDPR. Therefore, this paper attempts to answer whether the uncertainty in the application of Article 82(1) GDPR by Member States' national courts, and the uncertainty in interpreting the concept of damage is detrimental to the ability of data subjects to successfully claim immaterial damages under the GDPR. Regarding its scope, this paper will limit itself in two aspects, using a legal doctrinal and evaluative approach.

The first chapter will compare the relevant case law in the Netherlands and Germany to examine what is the prevalent national interpretation of the concept of immaterial damage. The second chapter will illuminate three relevant pending preliminary questions referred to the Court of Justice of the European Union (CJEU) by the courts in Austria, Bulgaria, and Germany, regarding the interpretation of the concept of immaterial damage. Lastly, the third chapter will provide a succinct overview of the previously discussed matter, as well as the relevance of the immediacy to resolve the discrepancies in the interpretation of the concept of immaterial damage, and the ability of data subjects to seek compensation for their immaterial loss.

[4] Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
[5] David Flint, 'Does non-material damage under GDPR need to be material or is that immaterial?' [2021] 43/1 BULA 159.
[6] Aleid Wolfsen, 'Privacyblog Aleid Wolfsen: Smartengeld', Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, 22 February 2021) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/privacyblog-aleid-wolfsen-smartengeld> accessed 6 February 2022.

2. Immaterial Damages at the National Level

This chapter will focus on the pertinent case law of the Netherlands and Germany regarding immaterial damages claims, and identify the discrepancies in the approach between these Member States.[7] Beforehand, it is necessary to briefly discuss the interpretation of the concept of damage under the GDPR.

2.1. What is damage?

Article 82(1) GDPR provides the right to compensation for data subjects that have suffered material or immaterial damage. However, the concept of damage is outlined in Recital 146, paragraphs 3 and 4. Pursuant to these paragraphs, the concept of damage must be interpreted 'broadly in the light of the case law of the CJEU in a manner which fully reflects the objectives of the GDPR, without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law'. This shows that the GDPR does not provide an explicit definition for damage, and further relies on CJEU case law as its sole source of interpretation.

The following two paragraphs discuss whether reliance on Article 82(1) read in conjunction with Recital 146 is sufficient to provide adequate and proportionate protection of data subjects for claiming immaterial damages on a national basis.

2.2. The Netherlands - Possibility for a precedent?

Over the course of the last three years, there have been multiple decisions of Dutch courts awarding compensation when immaterial damage occurred. Most prevalent has been the examination of the concept of immaterial damage under the GDPR by a series of four cases at the Highest Administrative Court.[8] All appeals concerned a claim for immaterial damages due to an alleged GDPR infringement (ECLI:NL:RVS:2020:898 concerned the unlawful sharing of a medical record by a psychiatric clinic, ECLI:NL:RVS:2020:899 concerned the only partial fulfillment of a freedom of information request by a municipality, ECLI:NL:RVS:2020:900 and ECLI:NL:RVS:2020:901 concerned the loss of control over personal data due to processing by a municipality).[9] Therefore, the Highest Administrative Court joined the cases and adopted identical reasoning that could be used as a potential precedent,[10] starting with applying the *Manfredi* rule.[11] It stated that as there is an absence of clear EU rules on awarding compensation for immaterial damage, national legislation can be relied upon, notwithstanding that EU law principles of effectiveness and

[7] These two Member States were chosen due to the authors of this paper's proximity and knowledge of Dutch and German language and law as well as the prevailing number of court cases regarding the subject of this paper.
[8] ABRvS 1 April 2020, ECLI:NL:RVS:2020:898; ABRvS 1 April 2020, ECLI:NL:RVS:2020:899; ABRvS 1 April 2020, ECLI:NL:RVS:2020:900; ABRvS 1 April 2020, ECLI:NL:RVS:2020:901.
[9] ibid.
[10] see Rb. Rotterdam 12 July 2021, ECLI:NL:RBROT:2021:6822, para 3.2.
[11] Joined Cases C-295/04 to C-298/04 *Vincenzo Manfredi and Others v Lloyd Adriatico Assicurazioni SpA and Others* [2006] ECR I-6619.

equivalence are respected. Subsequently, the Court applied the *Ombudsman/Staelen* case, following that immaterial damage, for which compensation is sought, must be actual and certain.[12]

The Highest Administrative Court continued by stating that national civil law is important in claiming compensation and therefore cited recent jurisprudence from the Dutch Supreme Court.[13] Even when no mental harm can be presupposed by the court or proven by the claimant, immaterial damages can be successfully claimed, provided that the nature and gravity of the violated norm and the consequences thereof, bring about impairment for the claimant, which shall be reviewed in regard of the concept of immaterial damages under Dutch civil law. The claimant must then provide concrete information supporting their claim. The claimant is exempt from this only when the violated norm has consequences so severe that an impairment can be presumed. However, as the Highest Administrative Court stated, a violation of a fundamental right is not enough to presume an impairment.[14]

Notably, in the cases that have allowed a claim for immaterial damages, the Dutch courts tended to award a monetary amount that could be deemed insignificant by the claimants. For example, in the first of four cases at the Highest Administrative Court, where a medical record was unlawfully shared by a psychiatric clinic, the Court, after having weighed the nature, duration and gravity of the impairment, awarded the claimants €500.[15]

2.3. Germany - Threshold frailty?

German case law has also shown a strict approach for awarding claims for immaterial damages - the actual damage threshold should be very high. In the first German decision regarding immaterial damages adopted by the District Court of Diez, the Court held that a violation of the GDPR alone does not directly grant a claim for compensation. Although a serious violation of human rights is no longer necessary, compensation for pain and suffering is still not to be granted for a minor offence or inconvenience; rather, there must be a noticeable and substantial disadvantage regarding an objectively comprehensible impairment of a personality-related matter.[16] Therefore, considering the facts of the case, the specific violation was insufficient to be awarded compensation. The reasoning of the District Court in this decision is roughly the general inclination that other German courts have followed;[17] a mere infringement is not justifiable to claim damages.[18]

---

[12] Case C-337/15 P *European Ombudsman v Staelen* (CFI, 4 April 2017) para 9.
[13] HR 15 March 2019, ECLI:NL:HR:2019:376.
[14] ABRvS 1 April 2020, ECLI:NL:RVS:2020:898, paras 27-29 and 32.
[15] ibid, para 36; other examples concern a data leak where €500 was awarded (Rb. Noord-Nederland 12 January 2021, ECLI:NL:RBNNE:2021:106) and unlawful processing where €250 was awarded (Rb. Overijssel 31 May 2021, ECLI:NL:RBOVE:2021:2264).
[16] Amtsgericht Diez [AG] [Local C] Nov 07 2018 8C 130/18 paras 10-11.
[17] Amtsgericht Bochum [AG] [Local Court] Mar 11 2019 65C 485/18; Landgericht Hamburg [LG] [Regional Court] Nov 04 2020 324S 9/19; Amtsgericht Frankfurt/Main [AG] [Local Court] Jul 10 2020 385C 155/19.
[18] Henrik Hansen,' Germany: new case-law on immaterial damages for GDPR infringements' (*Hogan Lovells*, 26 October 2020). <https://www.engage.hoganlovells.com/knowledgeservices/news/germany-new-case-law-on-immaterial-damages-for-gdpr-infringements> accessed 6 February 2022.

Despite this stringent GDPR interpretation, further (though limited) case law has shown a tendency to award such claims when the infringement concerns the data subjects' rights provisioned in Articles 15-22 GDPR. The Düsseldorf Labour Court awarded compensation of €5.000 where the infringing company responded to a data subject's access request partially inadequately and only after five months. The Labour Court concluded that a data subject may suffer immaterial damage if they are deprived of their right to data access pursuant to Article 15(1) GDPR. More importantly, the Court related the infringement with a fundamental rights violation: Article 8(2) Charter of Fundamental Rights of the EU,[19] which expressly guarantees the right to information. For awarding such a high amount, the Labour Court held that courts may also be guided by Article 83(2) GDPR, so that the criteria for assessment may include, *inter alia*, the nature, gravity, duration of the breach, degree of fault and measures taken to mitigate the damage suffered by data subjects. [20]

The reasoning in these decisions demonstrates the viewpoint of the German courts - there is a difference between a mere GDPR infringement and an actual violation of data subjects' rights. The German Federal Court of Justice is yet to issue a ruling on Article 82(1); therefore, the German approach regarding the concept of damage must currently rely on its national rules.

Conversely, in its most recent judgement,[21] the District Court of Munich I awarded €2.500 for immaterial damage suffered as a result of unauthorised third-party access to the subject's personal data. Moreover, the District Court found that the company at fault is obliged to compensate the plaintiff for all material future damage resulting from the data breach. With its decision, the Court interpreted Article 82 GDPR in a much broader scope, far beyond the previous reasoning of the German courts. There was no proof that the data subject's stolen personal data was actually used for fraudulent purposes, but the District Court found that it could *potentially* be used, thus ruling in favour of the plaintiff. As the Court applied a seemingly low threshold for its reasoning, this decision has the potential to open up the market for mass actions under the GDPR.[22] While this might be beneficial for ensuring full GDPR compliance by companies, such reasoning could potentially lead to an overflow of frivolous lawsuits.

2.4. Conjecture

The discrepancy in the position that Dutch and German courts have towards awarding compensation for immaterial damage seems to be stemming exactly from the lack of conceptual clarity. The current state of the

[19] Charter of Fundamental Rights of the European Union [2012] C 326/02.
[20] Arbeitsgericht Düsseldorf [ArbG] [Labour Court] Mar 05 2020 9 Ca 6557/18 para 75, 106 and 113.
[21] Landgericht München I [LG I] [Regional Court Munich I] Dec 9 2021 31 O 16606/20.
[22] Katrin Weixlgartner, Henrik Hanßen, 'German Court grants non-material GDPR damages following data breach' (*Hogan Lovells*, 1 February 2022) <www.engage.hoganlovells.com/knowledgeservices/viewContent.action?key=Ec8teaJ9VaqDTghmyr3KEsxgHJMKLFEppVpbbVX%2B3OXcP3PYxlq7sZUjdbSm5FIetvAtgf1eVU8%3D&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQ0qFfoEM4UR4%3D&emailtofriendview=true&freeviewlink=true> accessed 5 February 2022.

GDPR provides no uniform understanding of the concept of damage nor a threshold for Member States' national courts to rely upon. Reliance on the current paucity of relevant EU case law seemingly cannot provide suitable protection of data subjects for suffered immaterial damage. This, and the subsequent inadequacy of its reliability will be discussed in the next section.

3. Immaterial Damages at the Supranational Level

The lack of clarity and legal certainty regarding the application of the legal basis for claiming immaterial damages in national cases correlates to the lack of CJEU case law. However, its scarcity is understandable; the GDPR came into effect only four years ago. Therefore, this creates a paradoxical issue - can there be reliance on Article 82(1) read in conjunction with Recital 146 when CJEU case law is yet to be developed? This paragraph will discuss this issue by reflecting on three pending national cases, from Austria, Bulgaria, and Germany, where preliminary questions were referred to the CJEU, all concerning incurred immaterial damage.[23]

3.1. Austria - No harm suffered

The preliminary questions, in this case, concerned whether the GDPR infringement allows compensation to data subjects based on Article 82, even when no harm was suffered. Furthermore, the Austrian Supreme Court asked whether EU law requirements are necessary in addition to the principles of effectiveness and equivalence. Lastly, the preliminary reference aimed to clarify whether Article 82 can be interpreted to require that data subjects' damage must exceed the harm caused by the infringement for the national court to be able to award immaterial damages, and whether this interpretation is in accordance with EU law.[24] These questions signify the need for clarity on whether immaterial damages can be compensated in the absence of suffered harm, yet where considerable harm has been caused by the infringement.

3.2. Bulgaria - Fears, worries, and anxiety

In its preliminary reference, the Bulgarian Supreme Administrative Court directly challenges the concept of damage as to what the limits are to its application.[25] Are incurred fears, worries, and anxiety compensable in situations where misuse of data has not yet been established, but a risk of possible future misuse exists? The peculiarity of this question could possibly establish a precedent in further court deliberations on the scope of immaterial damages, specifically damage suffered in the absence of data abuse.

[23] Sebastião Barros Vale, 'Upcoming Data Protection Rulings in the EU: An Overview of CJEU Pending Cases' (*FPF,* 15 September 2021)
<https://fpf.org/blog/upcoming-data-protection-rulings-in-the-eu-an-overview-of-cjeu-pending-cases/> accessed 6 February 2022.
[24] Case C-300/21 Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 12 May 2021 – UI v Österreichische Post AG.
[25] Case C-340/21 Request for a preliminary ruling from the Varhoven administrativen sad (Bulgaria) lodged on 2 June 2021 — VB v Natsionalna agentsia za prihodite.

3.3. Germany - Long awaited answer or a bigger problem?

The CJEU ruling regarding the preliminary reference submitted by the German Federal Labour Court could be exactly what data subjects have been waiting for. The case concerned a €20.000 claim for, *inter alia*, immaterial damage resulting from the unlawful processing of health data.[26] If awarded, it would possibly be the largest compensation awarded for a case concerning incurred immaterial damage pursuant to Article 82(1). The CJEU is posed with the question of not only the status of the preventive character of the GDPR - whether it is general or specific - but also to what extent the incurred damage is taken into account when assessing immaterial damages. Further, the CJEU has to determine to what extent the data controller can be held liable when assessing the compensation of immaterial damage.

The CJEU's answer will certainly provide data subjects much-needed assurance regarding the liability of their data controllers, and simultaneously provide data controllers guidance as to their role and degree of fault in claims for immaterial damages. However, there is a possibility for the decision, if plaintiff-inclined, to be a gateway for an influx of GDPR-related claims from plaintiffs with financial motives. This could become a dangerously close approach towards frivolous litigation; therefore, it is of utmost importance for the CJEU to establish a well-reasoned, high threshold for assessing immaterial damage compensation claims.

3.4. A solution in sight?

The relevance of answering these pending questions is perhaps self-evident; CJEU guidance is much-needed when dealing with compensating immaterial damage under the GDPR. The proper application of Article 82(1) cannot be adequately maintained when there is a lack of EU case law that must be relied upon. It is however optimistic that the number of preliminary questions concerning immaterial damages claims under the GDPR is increasing. The benefit from the CJEU's decisions in the above-mentioned cases is three-fold: first, the Court will move closer towards establishing a comprehensive framework regarding compensation claims for immaterial damages under the GDPR; second, data controllers will have a clearer picture as to how to ensure their full compliance with the GDPR; last, and most important for the topic of this paper, the rulings will decrease data subjects' uncertainty when assessing whether they can claim immaterial damages under the GDPR. Therefore, the CJEU's ruling on these questions is much welcomed, as it might provide necessary clarity for the resolution of these uncertainties.

[26] Bundesarbeitsgericht [BAG] [Federal Labour Court] Aug 26 2021 8 AZR 253/20 (A).

4. Conclusion

This paper discussed how the continuous lack of legal certainty regarding the application of Article 82(1) GDPR and the interpretation of the concept of damage is detrimental to the ability of data subjects to successfully claim immaterial damages. Indeed, this lack of certainty is also harmful to the purpose and objective of the GDPR. The Dutch and German case law illustrated that currently, there exists a discrepancy in the Member States' application of the concept of immaterial damage and the GDPR's framework. Contrarily, reliance on CJEU case law is inadequate, because of its current scarcity. The CJEU's answers to the discussed pending questions should rectify this and provide legal certainty for data subjects.

These issues must be closely monitored to establish the legal framework according to the CJEU. Its immediate establishment is necessary for the adequate and proportionate implementation of the GDPR and to resolve the current issues. Recently, the chairman of the Dutch Data Protection Authority stated that 'immaterial damages should be the rule rather than the exception';[27] a scratch on the soul should also be compensable. However, this paper posits that such a threshold for claiming immaterial damages is too low, as that would give full reign to frivolous litigation. Awarding compensation for actual and certain damage constitutes truly adequate and proportionate protection for data subjects' rights. Moreover, this seems to fully reflect the objectives of the GDPR.

[27] Wolfsen (n 6).

The European Union's Right to Erasure - Influencing the Global Data Landscape?

Rosalie Vuillemot[1]

Abstract

The European Union's stance on data protection, specifically on the so-called 'right to be forgotten' notably encompassed in the Court of Justice of the European Union's case-law, is likely to have an impact on domestic courts all around the world, as recent cases in India show. The debates that such jurisprudence has created in the doctrine represent the difficulties of such a subject and the contradictions of European law and foreign national laws that this article aims to underline.

[1] Holder of a master's degree in European law from the University of Strasbourg, Rosalie possesses a great interest in this field and has pursued several related professional eendeavours. During an internship in the legal department of *Mykolas Romeris University* in Vilnius, she was assigned to work on EU data protection law, and it is here from where this article was inspired. She also completed an internship at the European Court of Human Rights where she covered and wrote articles on plenary sessions of the European Parliament. She has just completed an internship with a member of the French Parliament and is now in Vienna, starting a new internship at the *European Law Institute*.

1. Introduction

The purpose of this research paper is to determine whether the case-law of the Court of Justice of the European Union on the right to erasure is logical, whether it has been, and whether it should be extended to other legal orders. Disputes relating to the right to erasure can be noted to arise all around the world. By taking the example of legal order that is geographically and culturally opposed to ours, the 2021 Indian cases *Jorawar Singh Mundy v. Union of India*, *Subhranshu Rout v. State of Odisha*, and *Karthick Theodre v. Registrar General* extensively examined the 'right to be forgotten'.[2] [3] The increasing number of Indian cases on the matter originates from a judgement of the Karnataka High Court in 2017, which concerned a request for a name removal of an order copy and of search engines, including Google and Yahoo.[4] The Court acceded to the first demand of the plaintiff by particularly retaining that 'This [was] in line with the trend in western countries of the "right to be forgotten" in sensitive cases involving women in general and highly sensitive cases'.[5] By quoting 'the trend in western countries of the "right to be forgotten"', the Indian Court referred particularly to the recent development of the right to erasure in European Union law.[6]

2. The European creation of a 'right to be forgotten'

In Europe, the origin of the right to be forgotten is likely to be found in the French doctrinal reflection on a *'droit à l'oubli'* (or right to oblivion) that concerns the oblivion and the rehabilitation of formerly convicted individuals.[7] Several associations have been calling for enhanced protection of the sentenced individual's rights, particularly in the media, and have demanded the creation of a proper '*droit à l'oubli* in French law'.[8] In a decision of 2010, the French Superior Audiovisual Council (CSA), even called for 'other precautions to be taken by publishers and producers of the program, in order to preserve the possibilities of reintegration of sentenced persons and improve their security as well as that of their family'.[9]

The right to erasure or the 'right to be forgotten' doctrine broadens the legal thought because this right aims to not only protect the sentenced individuals' integrity but everyone's personal data and image on

[2] Jorawar Singh Mundy v. Union of India [2021], High Court of Delhi, W.P.(C) 3918/2021 and CM APPL.11767/2021; Subhranshu Rout v. State of Odisha, [2020], Orissa High Court, 4592 OF 2020; Karthick Theodre v. Registrar General, [2021], Madras High Court, W.P.(MD) 12015 of 2021.

[3] WMP (MD) 9466 of 2021 ; Kamala Naganand and Ronak v. Chhabria, 'The Right to be Forgotten: Arising disputes in India', <https://s3.amazonaws.com/documents.lexology.com/8e1797e8-9972-4677-81e2-f864462633b4.pdf?AWSAccessKeyId=AKIAVYILUYJ754JTDY6T&Expires=1639823627&Signature=HlMhAYUHjb3vXxnPamoAE4gxurw%3D> in Lexology 2021 accessed 12 February 2022.

[4] Sri Vasunathan v. Registrar General [2017], Karnataka High Court, Writ petition 62038 of 2016.

[5] ibid §5.

[6] ibid.

[7] This right would supposedly stem from French Criminal law's the right to erasure of the criminal record with the passage of time (Article R70-1 Criminal Procedural Code), the right to rehabilitation (Article 133-13 of the Criminal Code), the right to protection of one's image and dignity (Article 17 of the International Covenant on Civil and Political Rights, Article 2 of the French Declaration, Article 2 of the Declaration of Human and Civil Rights, Article 226-1 of the Criminal Code).

[8] Association for communication on prisons and incarceration in Europe, 'Le droit à l'oubli', in 2011, <http://prison.eu.org/IMG/pdf/droit_a_l_oubli.pdf> accessed 9 February 2022.

[9] CSA, Decision **'**Émission Faites entrer l'accusé : intervention auprès de France 2**'**, Plenary Assembly, 7 January 2010.

the internet and globally, in the media. The right to erasure derives from the desire to balance the asymmetrical relationships between tech giants and data subjects, allowing the latter to withdraw their consent to the use of their personal data.[10]

This 'right to be forgotten' notably relates to the right to privacy contained in Article 7 of the Charter of Fundamental Rights of the European Union and Article 8 of the European Convention on Human Rights (ECHR). Interestingly, the Charter of Fundamental Rights provides for the right to the protection of personal data, which is another basis for the right to erasure, whereas the ECHR does not provide for such a right. However, the right to protection of personal data can uncontestably be found in the European Court of Human Rights jurisprudence.[11]

The Directive 95/46/EC[12] is the first legally binding instrument dealing with data protection in the European Union. Without quoting once the 'right to be forgotten' some important features of what would become this right are touched upon in this directive. Indeed, the right of access to one's own data (Article 12) and the data subject's right to object (Article 14) represent the premises of the right to be forgotten.
With the rise of European citizens' concern for the protection of their data,[13] the former European Commissioner Viviane Reding announced in 2012 the creation of the General Data Protection Regulation (GDPR). The GDPR would include the right to be forgotten, which she introduced as follows:

> Another important way to give people control over their data: the right to be forgotten. I want to explicitly clarify that people shall have the right – and not only the 'possibility' – to withdraw their consent to the processing of the personal data they have given out themselves.[14]

The former Vice-President of the European Commission justified the need for such a right, particularly by the pressing issue of protecting teenagers from content they would put online and could not delete afterward.[15]

---

[10] J. Ausloos, '*The Right to Erasure in EU Data Protection Law: From Individual Rights to Effective Protection*' in Oxford University Press, 2020.

[11] ECtHR, *Klass c. Allemagne*, no. 5029/71, 6 September 1978; ECtHR, *Malone c. Royaume-Uni*, no. 8691/79, 2 August 1984.

[12] Council Directive (EC) 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] *OJ L 281.*

[13] "81% of German citizens [were] worried they are no more in control of their personal data" in 2012. See V. Reding Vice-President of the European Commission, EU Justice Commissioner 'The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age Innovation Conference Digital'< https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_26>, in2012, accessed 9 January 2022.

[14] ibid.

[15] J. Rosen, 'Response – the right to be forgotten' in Standford law review, Volume 64 [February 2012], accessed 18 December 2021.

Thus, the 'right to be forgotten' was introduced in the GDPR in Article 17, which stipulates the following:

> 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
> (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
> (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing.[16]

Article 19 GDPR also provides for a notification obligation regarding rectification or erasure of personal data or restriction of processing.[17] There is reason to question the interpretation and the effectiveness of this right in the jurisprudence of the Court of Justice of the European Union (CJEU), as it exists several contradictions in the Court's judgements.

3. The CJEU's praetorian construction of the right to erasure: the *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos* case

Before the entry into force of the GDPR, the Court of Justice of the European Union issued an important judgement that will impact and push forward the creation of a right to erasure. The Google and Spain case examines the question of a possible obligation for internet operators to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person.[18]

Google notably argued that the principle of proportionality put the responsibility on the publishers of the website because they are the ones who make the information public.

The CJEU recalled the importance of data subjects' fundamental rights, that the processing of personal data is susceptible to endanger, particularly the right for private life and the right to protection of personal data contained in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and the specific obligations contains in Articles 6, 7, 12, 14, 28 of Directive 95/46. The controllers must respect the safeguards enacted in Article 6 of the Directive 95/46, which base the processing of data on fairness, proportionality and consent of the data subject.[19] They should also respect Article 7, which balances the

[16] Regulation (EU) 2016/679 of the Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016], and repealing Council Directive (EC) 95/46 (General Data Protection Regulation), Article 17.

[17] Ibid, art 19.

[18] *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD)*, CJEU C-131/12, [13 May 2014].

[19] ibid § 72.

opposing rights and interests of, on one side, the controllers, the third parties or parties to whom the data are disclosed, and, on the other side, the data subjects.[20]

The Court stated that requests by data subjects under Articles 12(b) and 14 of the Directive must be examined by the controller, with a possibility for the data subject, where the control does not accede to their demands, to bring the matter before the supervisory or the judicial authority.[21] Such authority may order the search engine's operator to remove web pages published by third parties and containing information about a person from the list of search results.[22] A data subject's request for removal can't be granted in cases where the search result(s) 'appear to be inadequate, irrelevant or no longer relevant or excessive in the light of the time that had elapsed'.[23]

The individual can request that the information no longer be made available to the general public and the supervisory authority. However, that would not be the case if it appeared that the interference with their fundamental rights is justified by the preponderant interest of the general public in having access to the information in question. One reason that may lead to this conclusion is the role played by the data subject in public life

Even though the Court never uses this express term in its ruling, academics read the 2014 judgement as providing the 'right to be forgotten' and marks the first step to frame this right under EU law.[24] The main outcome of this judgement is that internet search engines must consider requests from data subjects to delete links from a search of their name which led to free websites.

4. The obligation to balance fundamental rights holds on private actors: the *GC et al v. CNIL* case

The Court of Justice rendered two landmark judgments in 2019 interpreting the GDPR and the 'right to be forgotten'. The first case concerned a decision of the French data protection authority (CNIL) in which it ordered Google to globally remove search result listings to pages containing false information about a person. The following year, Google introduced a geo-blocking feature that prevents European users from being able to see delisted links. However, Google did not censor search results for people in other parts of the world, and thus the CNIL imposed a €100 000 fine on Google.

[20] ibid § 76.
[21] ibid § 77.
[22] ibid § 82.
[23] ibid § 92.
[24] See, e.g. E. Pirkova and E. Massé, 'EU Court decides on two major 'right to be forgotten' cases: there are no winners here'<https://www.accessnow.org/eu-court-decides-on-two-major-right-to-be-forgotten-cases-there-are-no-winners-here>/in Accessnow, 23 October 2019, accessed 9 January 2022.

In a 2019 judgement,[25] the CJEU stated that if Article 17(1) provides the right to erasure, Article 17(3) provides grounds for exceptions to such a right, among which is the exercise of the right to freedom of expression and information.

This right is not absolute but has to be read in combination with other fundamental rights, according to the principle of proportionality. Article 17 GDPR balances the rights to privacy and protection of personal data, on the one hand, and the right of freedom of information and expression as contained in Article 11 of the Charter of Fundamental Rights, on the other. For data to enter the scope of the exceptions provided in Article 17 (3) GDPR, the data subjects have to give their 'explicit' and 'specific' consent to the operators, and the asking for delisting assumes that the data subject withdraws their consent.

A data user's request for delisting signifies the withdrawal of consent, which is a ground in Article 17(1)(b) GDPR justifying the right to erasure. Nevertheless, Article 17(3) GDPR provides for exceptions, among which is the exercise of the right of freedom of expression and information[26]. The right to erasure is therefore not an absolute right. On the contrary, it must be read and interpreted in relation to its function in society, and be balanced with other fundamental rights, according to the principle of proportionality.[27] Article 17 is interpreted as asking for a balance between the rights to privacy and protection of personal data and the right of freedom of information under Article 11 of the Charter.[28]

The Court underlined the importance of a 'specific consent' given by the data subjects to the operators, and the request for de-referencing assumes that the data subject withdraws their consent[29]. When the operator of a search engine receives a request for de-referencing, he must ascertain, 'having regard to the reasons of substantial public interest', and considering the seriousness of the interference with the data user's rights, 'whether the inclusion of the link to the web page in question in the list displayed following a search on the basis of the data subject's name is necessary for exercising the right of freedom of information of internet users'.[30] The Court mainly followed the opinion of Advocate General Szpunar in considering such balancing.[31] In conclusion, an operator can then refuse a request for de-referencing after having made this assessment and not found a too severe interference with the data user's rights.

[25] *GC e.a. v. Commission nationale de l'informatique et des libertés*, CJEU C-136/17, [24 September 2019].
[26] ibid § 56.
[27] ibid § 57.
[28] ibid § 59.
[29] ibid § 61 – 62.
[30] ibid § 66.
[31] See Opinion of Advocate General Szpunar in the case GC and Others v. CNIL, 10 January 2019, and particularly §92.

The Court of Justice had balanced these different fundamental rights on several occasions within the data protection field.[32] What is new is that, here, the Court puts the responsibility of balancing individuals' fundamental rights on private actors - the operators. Google ultimately decides what information and data entry in the scope of public interest and can refuse the dereferencing for such reasons. Google, and other tech giants, therefore become the adjudicator of fundamental rights in the online space.[33]

However, there might be a justified basis for the Court's reasoning: tech giants are mainly based abroad, specifically in the United States, and by stating that this obligation binds them, the CJEU recognises the exportation of its norms to foreign actors.

5. The territorial scope of the right to erasure: *CNIL v. Google* case

The second case also concerned a CNIL decision that ordered Google to remove the links from all versions of its search engine worldwide. Google refused to comply and continued to limit its de-referencing to search results conducted in the versions of its search engines with domain extensions within the EU and the European Free Trade Association. CNIL imposed a € 100,000 fine on Google for noncompliance. Google then appealed to the French Highest Administrative Court, the *Conseil d'Etat*, which referred questions to the Court of Justice for a preliminary ruling concerning the scope of application of Arts 12(b) and 14(a) of Directive 95/46.[34]

The measures taken by Google, de-listing links from all EU and EFTA extensions and de-listing links from all searches conducted in the French territory, were considered insufficient by CNIL to ensure the effectiveness of the 'right to erasure'. The CNIL also argued that internet users located in France are still able to access the other versions outside the EU and removing links about an individual residing in France only from the French version is not enough to protect data users, thus violating the Directive 95/46.[35] On the contrary, Google stated that the right to erasure 'does not necessarily require that the links are to be removed without geographical limitation from all its search engine's domain names'.[36] Google considered that CNIL misinterpreted the directive and, by doing so, it amounted to a violation of public international law's principles of 'courtesy and non-interference', and the disproportionate infringement of the freedoms of expression, information, communication, and the press.

[32] Such as the conservation of data concerning localization in the case CJEU Quadrature du Net et autres, C-511/18, C-512/18 and C-520/18, 6 October 2020.
[33] E. Pirkova and E. Massé, **'**EU Court decides on two major 'right to be forgotten' cases: there are no winners here'<https://www.accessnow.org/eu-court-decides-on-two-major-right-to-be-forgotten-cases-there-are-no-winners-here>/in Accessnow, 23 October 2019, accessed 9 January 2022.
[34] Council Directive (EC) 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] *OJ L 281*.
[35] *Google v. Commission nationale de l'informatique et des libertés* (CNIL*),* [24 September 2019], CJEU C-507/17, § 38.
[36] ibid.

In the judgment *Google v. CNIL*, the Court had to interpret the territoriality of the right to erasure, namely, whether de-referencing meant that a search engine operator is required to remove links worldwide, within the EU, or only at the national level. [37]

According to the Court, in a globalised world, internet users' access, including outside the Union, is likely to have 'immediate and substantial' effects on a person located in the Union, which is enough to justify the competence of an EU legislation to ask for de-referencing worldwide.[38]

Nevertheless, numerous third States do not recognise the right to de-referencing.[39] Moreover, the right to the protection of personal data is not an absolute right but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.[40] The dispositions in the Directive and the GDPR regarding the 'right to be forgotten' do not specify that they would apply beyond the Member States, and they did not intend to oblige search engine operators a de-referencing obligation to include non-EU national versions of their search engines either.[41] The Court concluded that the right to erasure must be understood as EU-based. Search engine operators are required to remove all the links on all the versions in the EU.[42] In deference to national authorities and DPAs, the Court acknowledged their competence to balance the rights to privacy and data protection against the freedom of information in light of national standards of protection of fundamental rights.[43] Without specifically mentioning the geo-blocking technique, the Court considered that search engine operators are required to supplement the de-referencing through measures that would prevent or seriously discourage an internet user located in the EU to gain access to delisted links when using a search engine version outside the EU.[44]

The Court also held that the balancing of interests can be different among the Member States, with the GDPR permitting necessary exemptions and derogations at the Member State level with regards to processing for journalistic purposes and artistic or literary expression. Therefore, even though the Court ruled that EU law did not require search engine operators to automatically de-list links globally, the judgment explicitly permits national courts and DPAs to order, when appropriate, a de-referencing at a global level.[45]

---

[37] ibid.
[38] ibid § 57 – 58.
[39] ibid § 59.
[40] ibid § 60.
[41] ibid § 61 – 62.
[42] ibid § 66.
[43] ibid § 69.
[44] Google v. Commission nationale de l'informatique et des libertés (CNIL*),* 24 September 2019, C-507/17, § 70.
[45] M. Samonte, '*Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law*', in *European Papers,* Vol. 4, [2020], pp. 839-851, accessed 9 January 2022.

The judgment can be read as restricting the territory effect of the de-referencing obligation for internet operators to the E.U. This can be criticised as it decreases the effectiveness of the right to be forgotten and the possibility for individuals to control their personal data. This limits the impact of an effective right to be forgotten because it will be restricted to searches performed within the European Union, and that 'this might obviously be frustrating for people who will see that people from outside Europe will still be able to find the delisted search results when performing the same search on Google in New York, Shanghai, or any other place in the world'.[46]

Nevertheless, the CJEU has likely limited this territorial effect because data protection is radically different in Europe compared to other continents, especially in the United States. The differences between the two legal frameworks emerge firstly in the Constitutions: whereas the right to privacy and the right to free speech both appear in European Constitutions, there is no mention of the right to privacy in the US Constitution. The US Data Protection Law tends to strongly make the freedom of the press prevail, in line with the constancy of liberalism of the US legal culture and contrary to the European approach.[47] Notably because of these constitutional differences, there is no legal recognition of a 'right to be forgotten' in US law. The apparition of a right to be forgotten in Europe has been the subject of numerous critics in the US.[48] The CJEU 2014 judgment has particularly been criticised, especially because it considered that EU Data protection law would apply to an American operator that would be forced to take into consideration a request for de-referencing. The Court is likely to have wanted to take a step back from this line of jurisprudence and limit the exterritorial effect of EU data protection law and the de-referencing obligation of operators with its 2019 judgment.

Moreover, the Court expressly added an exception for national judges and authorities to allow de-referencing at the global level. Accordingly, in a press release just after the CJEU judgment, the CNIL expressly declared that it had 'authority to force a search engine operator to delist results on all the versions of the search engine if it is justified in some cases to guarantee the rights of the individuals concerned'.[49]
Furthermore, the *Glawischnig-Piesczek v. Facebook* decision, delivered just a week later than the *CNIL v. Google* judgment, slightly counterbalances the previous judgments. In the case, an Austrian politician had obtained a Court order to remove defamatory comments on Facebook, but the latter only removed links in Austria, and the politician sued the company before the CJEU. The Court ruled that EU law 'does not preclude those injunction measures from producing effects worldwide'.[50] On one hand, the CJEU cautioned that considering

---

[46] P. Van Eecke, 'Right to be forgotten', but only in Europe?', in DLA Piper 2019, https://blogs.dlapiper.com/privacymatters/right-to-be-forgotten-but-only-in-europe/ accessed 23 December 2021.

[47] F. Werro, '*The right to be forgotten: a comparative study of the emergent right's evolution and application in Europe, the Americas, and Asia*', [2020] 3-6.

[48] J. Rosen, '*Response – the right to be forgotten'* in Standford law review, Volume 64, [February 2012].

[49] Commission nationale de l'informatique et des libertés, 'Right to Be Forgotten": The CJEU Ruled on the Issue' 2019, <https://www.cnil.fr/en/right-be-forgotten-cjeu-ruled-issue>.

[50] *Eva Glawischnig-Piesczek v. Facebook Ireland Limited*, [4 June 2019], CJEU C-18/18.

the global aspects of electronic commerce, the EU legal framework has to be consistent with international rules and therefore the Member States must ensure the measures they take and have effects worldwide 'take due account of those rules'.[51] On the other hand, the Court enables national courts, and in this case, Austrian courts, to impose obligations on Facebook 'to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law'.[52]

Data subjects in Europe are now given a choice to request the de-referencing of their personal data, even with the limits of the 2019 judgments. In 2020, Google received over 850,000 requests to de-list over 3.3 million URLs across all Member States since the *Google Spain* decision,[53] among which 190 000 dereferencing requests from French citizens, who requested the delisting of more than 670 000 URLs. They were successful in removing 49.4 percent of requested URLs.[54]

6. Conclusion: The empowerment of data subjects in Europe

Data subjects in the European Union are being empowered by the CJEU case-law. By leaving the door to extraterritorial de-referencing open, the CJEU is likely to transform the global data privacy landscape.[55] Indeed, the CJEU's stance on the 'right to be forgotten' has already impacted foreign contentious, as the recent case-law of Indian courts shows.[56] Nevertheless, the CJEU is the most advanced in the defense of a right to be forgotten, and more generally in the protection of individuals' data, and most other legal systems have not yet adopted any regulation in this area. Moreover, the propagation of this right as contained in the case-law of the Court also means that the contradictions criticized by part of the doctrine as to the interpretation that the Court makes of this right, and which relates in particular to the fact that the obligation to strike a balance between fundamental rights is up to private actors, will also tend to be duplicated in other legal systems.

---

[51] ibid § 52.
[52] ibid § 53.
[53] *Requests to Delist Content Under European Privacy Law*, Google Transparency Rep., *at* < https://transparencyreport.google.com/eu-privacy/overview >showing all countries' requests to delist).
[54] *Requests to Delist Content Under European Privacy Law*, Google Transparency Rep., *at* < Kamala Naganand and Ronak v. Chhabria, 'The Right to be Forgotten: Arising disputes in India', <https://s3.amazonaws.com/documents.lexology.com/8e1797e8-9972-4677-81e2-f864462633b4.pdf?AWSAccessKeyId=AKIAVYILUYJ754JTDY6T&Expires=1639823627&Signature=HlMhAYUHjb3vXxnPamoAE4gxurw%3D> in Lexology 2021 accessed 12 February 2022> (showing all requests to delist from France).
[55] M. Samonte, 'Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law', <https://www.europeanpapers.eu/en/europeanforum/google-v-cnil-territorial-scope-of-right-to-be-forgotten-under-eu-law#_ftn32> in *European Papers*, Vol. 4,2020, pp. 839-851, accessed 9 January 2022.
[56] Kamala Naganand and Ronak v. Chhabria, 'The Right to be Forgotten: Arising disputes in India', <https://s3.amazonaws.com/documents.lexology.com/8e1797e8-9972-4677-81e2-f864462633b4.pdf?AWSAccessKeyId=AKIAVYILUYJ754JTDY6T&Expires=1639823627&Signature=HlMhAYUHjb3vXxnPamoAE4gxurw%3D> in Lexology 2021 accessed 12 February 2022.

The ELSA the Netherlands Law Review is a student-run, peer-reviewed journal of legal scholarship. The Review aims to serve as an academic forum that enables both students and legal professionals to analyse and discuss contemporary legal issues. While contributions are welcome from all members of the legal community, the Review, in particular, aims to provide law students and young lawyers with the opportunity to have their voices heard.

The European Law Students' Association

THE NETHERLANDS