Northern Ireland
Legal Quarterly
Summer Vol. 73 No. 2 (2022) 283–309
Article DOI: 10.53386/nilq.v73i2.959

Digital technology and privacy attitudes in times of COVID-19: formal legality versus legal reality in Ireland

Edoardo Celeste*
Dublin City University

Sorcha Montgomery
Dublin City University

Arthit Suriyawongkul
Trinity College Dublin
Correspondence email: edoardo.celeste@dcu.ie

ABSTRACT

The adoption of digital technologies to counteract the spread of COVID-19 has resulted in a major exposure of our rights to privacy and data protection. An empirical study conducted in Ireland by the Science Foundation Ireland-funded project PRIVATT demonstrates that privacy attitudes have shifted, resulting in a greater willingness to share personal data in order to combat the pandemic, while, at the same time, upholding a persistent mistrust in the public and private institutions overseeing this global health crisis. This article interprets these findings from a socio-legal perspective, arguing that people tend to overlook the inalienable nature of the essence of their rights to privacy and data protection, the compression of which is not admissible under EU law. Moreover, the widespread mistrust of public and private actors evidences a divergence between the formal legality of the technological solutions adopted and the legal reality that brings about the Irish public's perception of government measures as potentially infringing their fundamental rights. These considerations will prompt recommendations in pursuit of enhancing transparency, involvement in decision-making processes and data protection literacy amongst the population.

Keywords: COVID-19; digital technology; privacy and data protection; efficiency; essence of fundamental rights; formal legality; legal reality; transparency; fundamental rights literacy.

* This work was supported by Science Foundation Ireland through the Covid Rapid Response Programme grant number 20/COV/0229. The survey at the basis of this article was conducted by Dr Irina Tal, Dr Rob Brennan, Dr Malika Bendechache, Dr Ramona Trestian, Dr Guodong Xie, Dr Pintu Lohar, Dr Kristina Kapanova, Dr Evgeniia Jayasekera and Dr Edoardo Celeste. We would like to thank the editors of this special issue and the anonymous reviewers for their constructive comments and feedback on earlier versions of this article.

INTRODUCTION

The outbreak of the COVID-19 pandemic in 2020 has led the media to evoke the deadly 1918 influenza pandemic, which, spread by troops fighting in the First World War, killed 20 million people worldwide.[1] Black and white photos of people wearing masks have illustrated that many of the public health measures currently in place to fight the spread of coronavirus are not new.[2] Social distancing, travel restrictions, coughing and sneezing etiquettes had all already been put in place over a century ago.[3] However, among the main differences between the COVID-19 pandemic and the 1918 pandemic, one can certainly mention the widespread use of digital technology to limit the diffusion of the virus.

Indeed, in the COVID-19 pandemic, digital technology has played a crucial role. Pre-existing digital technology tools have been adapted to the fight against the virus. New digital solutions have been introduced to maximise the efficiency of containment measures imposed by state and health authorities. The coronavirus has been elevated to the ranks of the main public enemy, often leading to the decision to prioritise public health over our liberties. However, one cannot underestimate the risks that the misuse of digital technologies may have on our fundamental rights, particularly on the rights to privacy and data protection. Most of the digital technology tools introduced to limit contagions significantly interfere with our personal life, and often process sensitive personal data, increasing the risks associated with our 'digital selves'.

The project PRIVATT (Assessing Irish Attitudes to Privacy in Times of COVID), funded by Science Foundation Ireland, aimed to assess whether the introduction of digital technology tools to fight the pandemic in Ireland had also been accompanied by a change of attitude regarding privacy and data protection preferences. Our hypothesis was that, in general, the adoption of digital technology tools that might be more privacy intrusive and riskier from a data protection perspective is also accompanied by a major complacency within the population. A survey conducted on Irish residents showed that people had effectively changed their privacy attitudes in light of the current pandemic, becoming now more willing to share their data to counteract the spread of the virus, but that a significant portion did not trust the technological tools introduced by the Government, despite their formal legality.

---

1 Stephen Dowling, 'Coronavirus: what can we learn from the Spanish Flu?' (*BBC News* 3 March 2020).

2 Hannah Devlin, 'Four lessons the Spanish flu can teach us about coronavirus' *The Guardian* (London, 3 March 2020).

3 Nina Strochlic, 'How they flattened the curve during the 1918 Spanish flu' (*National Geographic* 27 March 2020).

This article does not include a detailed analysis of the hypotheses, methodology and full results of the survey conducted in the context of the PRIVATT project, which have been covered in other works in detail.[4] Instead, it aims to contextualise and critically assess the findings of the PRIVATT project from a socio-legal point of view. For this reason, following this introduction, in the second section we will start by providing an overview of the results of the survey. The third section will then illustrate the main privacy and data protection implications of the use of digital technology to counteract the spread of COVID-19, focusing on the risks associated to both public and private actors. In the fourth section, we will show that in some Asian countries, despite these threats, a duty of fully sacrificing privacy and data protection in favour of ensuring the most efficient use of the digital technology adopted to fight the virus has emerged during the pandemic. However, with reference to the recent case law of the Court of Justice of the European Union (CJEU), we will explain how such a rhetoric would not be acceptable in a European context, due to the inalienable nature of the essence of the rights to privacy and data protection. The fifth section will then examine the guidelines adopted in the EU in order to guarantee the introduction of fundamental rights-compliant digital solutions by member states for fighting the pandemic. We will explain that, despite this formal reassurance, a significant mistrust towards digital solutions for combating COVID-19 has been identified among Irish residents. From a socio-legal perspective, such a divergence between the formal legality of technological solutions adopted and the legal reality that brings about the Irish public's perception of government measures as potentially infringing their fundamental rights will be interpreted as evidence of a lack of transparency and involvement of the population in decision-making, as well as literacy related to the legal safeguards offered by fundamental rights in general, and in particular, by the rights to privacy and data protection. The final section will conclude with a series of recommendations for ensuring that digital solutions used to fight the virus are both legally compliant from a formal point of view but also, in view of maximising their efficiency, that they are accepted, understood and endorsed at a social level.

4 See Malika Bendechache et al, 'Public attitudes towards privacy in COVID-19 times in the Republic of Ireland: a pilot study' (2021) 0 Information Security Journal: A Global Perspective 1; Ramona Trestian et al, 'Privacy in a time of COVID-19: how concerned are you?' [2021] IEEE Security and Privacy 2.

COVID-19 AND THE SHIFT OF PRIVACY ATTITUDES IN IRELAND

The PRIVATT project conducted an online survey from 11 November 2020 to 12 January 2021.[5] Targeted at members of the general public over the age of 18 resident in Ireland, the main objective of the survey was to investigate and report on the attitudes to privacy of the residents of Ireland during COVID-19. The main research questions at the basis of the survey were:

i) What is the general attitude towards privacy in times of COVID-19?
ii) Has this attitude changed compared to normal circumstances with the desire to help control the spread of COVID-19?
iii) Do privacy concerns prevent Irish people from using digital technology tools (eg the Health Service Executive (HSE) COVID Tracker app) that may help to manage the crisis?
iv) Are people in Ireland concerned about the long-term effects of these technologies on their privacy beyond the current health crisis?

The questionnaire was therefore structured in three parts: demographics, privacy profiles and privacy attitudes during COVID-19. The first part collected demographic data, while the second part aimed to build a general privacy profile of the respondents and used the Privacy Segmentation Index methodology coined by Alan Westin that classifies individuals into three groups based on their privacy attitude.[6] The third part of the questionnaire aimed to capture the attitudes toward privacy in times of COVID-19. This included questions related to sharing personal data in the interest of saving lives, usage of the COVID tracker app, and possible factors influencing privacy attitudes.

An intermediate step in designing the national survey was represented by a pilot study conducted between 24 August 2020 and 15 September 2020 during which 258 participant responses were collected. The questionnaire used in the pilot study was refined on the basis of participant and stakeholder feedback, and the final survey conducted on a national level was closed in January 2021. It was circulated on mailing lists and on the websites of universities involved, social media, news articles, including the *Irish Times* and *Irish Tech News*,[7] and received 1011 responses.

---

5 See Trestian et al (n 4 above); Bendechache et al (n 4 above).

6 Ponnurangam Kumaraguru and Lorrie Faith Cranor, 'Privacy indexes: a survey of Westin's Studies' (Institute for Software Research International, School of Computer Science, Carnegie Mellon University 2005) CMU-ISRI-5-138.

7 See 'Personal privacy vs "we're all in this together": a survey in Covid-19 times' *Irish Times* (Dublin, 11 December 2020); 'Do you trust the Government with your data?' (*Irish Tech News* 2 December 2020).

Of all participants, 48.85 per cent were male and 48.95 per cent were female, 18 people preferred not to say and 4 people were non-binary. We provided four age groups, 18–24, 25–44, 45–64 and over 65 for participants to select. The largest age group was between 25–44 years old, accounting for 50.0 per cent of the total. Regarding the location of participants, 62.3 per cent of the participants came from County Dublin. Participants of the survey were generally well-educated, with 30.3 per cent of the respondents holding a master's degree and 22.2 per cent holding a bachelor's degree. The third largest educational group finished secondary school (16.8 per cent).

In the second part of the survey, participants were asked questions to determine their privacy attitudes based on the Privacy Segmentation Index developed by Westin and were classed accordingly as 'pro-privacy', 'ambivalent' or 'dismissive', to use a terminology which appears as less value judgement-laden.[8]

Pro-privacy persons are termed 'privacy fundamentalists' by Westin and 'are the most protective of their privacy. These consumers feel companies should not be able to acquire personal information for their organizational needs and think that individuals should be proactive in refusing to provide information'.[9] They are also described as supporting 'stronger laws to safeguard an individual's privacy'.[10] Ambivalent persons are termed 'pragmatists' by Westin and 'weigh the potential pros and cons of sharing information; evaluate the protections that are in place and their trust in the company or organization. After this, they decide whether it makes sense for them to share their personal information.'[11] Dismissive persons are termed 'unconcerned' by Westin and 'are the least protective of their privacy – they feel that the benefits they may receive from companies after providing information far outweigh the potential abuses of this information. Further, they do not favour expanded regulation to protect privacy.'[12]

The PRIVATT survey found that 54 per cent of the participants were privacy ambivalent, 17 per cent were privacy dismissive and 29 per cent were pro-privacy. Interestingly, a shift in attitude towards sharing data to combat COVID-19 was demonstrated by responses to the question: 'Would you agree to share your mobile data (data stored or related to your mobile device) with the government and relevant institutions to help defeat COVID-19?' – 61 per cent of respondents chose 'Strongly Agree' and 'Agree' and 47 per cent changed from the 'Disagree' given to questions referring to normal times to 'Neutral'

8 Kumaraguru and Cranor (n 6 above).
9 Ibid 15.
10 Ibid.
11 Ibid.
12 Ibid.

or 'Agree', demonstrating an increase in their willingness to share their data to fight COVID-19 compared to usual circumstances. The greatest change came from the privacy dismissive with a 57 per cent increase, while pro-privacy and ambivalent respondents demonstrated an increase of 46 per cent and 44 per cent respectively. In this article, we will contextualise this finding, arguing that, in the complex times we are living, where public health is threatened by a global pandemic, people often think that they are free to dispose of their rights to privacy and data protection in the pursuit of the public good. However, as we will explain, this argument is untenable in the EU, where the essence of these rights cannot be given up and solutions preserving these rights must always be sought.

We will combine this analysis with a second interesting finding deriving from the survey. Despite the general willingness to share data with the Government to help counteract the virus, a still significant percentage of respondents were concerned by potential misuse of their data by government agencies. Indeed only 12 per cent of the respondents answered that they were not concerned at all in relation to how their personal data would be used by the Government and relevant institutions in order to defeat COVID-19.[13] When asked about specific concerns, the top concerns were 'privacy issues' (582 respondents), 'lack of trust in the Government and the institutions managing the data' (483 respondents), 'security issues' (469 respondents), 'creating a dangerous precedent' (418 respondents), and 'other' (30 respondents). Moreover, when specifically asked about concerns in relation to use of the HSE COVID Tracker App, 28 per cent of respondents reported worries about the implications of using the app for their privacy and data protection; 30 per cent feared that the app could be used as a surveillance tool beyond its primary aim of fighting the spread of COVID-19; and 42 per cent of respondents who are using the HSE COVID Tracker App had concerns about what will happen to their data after they leave the app. These data reveal that people do not fully trust the formal legality of measures adopted by government agencies to counteract the spread of the virus while preserving their privacy. The legal reality indeed shows a different image: individuals who are willing to help fight the pandemic are still not persuaded that their government will not misuse their data.

13 Trestian et al (n 4 above).

DIGITAL TECHNOLOGY AND FUNDAMENTAL RIGHTS IMPLICATIONS

All digital technology instruments introduced to limit the circulation of COVID-19 have fundamental rights implications, in particular on the right to privacy and data protection. Firstly, they all rely on the processing of data related to identifiable individuals in order to achieve their purposes, from contact-tracing to quarantine enforcement.[14] Secondly, they process information related to aspects of our personal and family lives, such as our social interactions, movements and health status. In Europe, as we will explain in the next few sections, the adoption of these technologies is legitimate in so far as data protection principles are respected and the intrusion into our personal and family life is justified, necessary and proportionate to the purpose of solving a global health crisis. Around the world, however, the use of digital technology tools to limit the spread of COVID-19 has produced a series of violations of these fundamental rights. In this section, we will focus in particular on an examination of aspects relating to the rights to privacy and data protection as conceived by European case law, or, using the denomination commonly used in the United States (US), aspects related to data privacy. Without aspiring to provide an exhaustive investigation of the topic, the aim of this overview is to offer an introductory analysis of the fundamental rights implications derived from the use of digital technology tools during the pandemic. In the following section, we will explain how, in Europe, differently from countries in other regions, specific measures have been taken to prevent these risks. This analysis will be used in the final section to highlight the current discrepancy between formal legality of the use of digital tools in Ireland and the persistent fear of the general population that government and private companies may misuse these instruments.

State actors: mass surveillance and mission creep risks

The most concerning scenario is offered by states where government authorities are carrying out a systematic monitoring of location, travel history and contacts between natural persons, using the fight against COVID-19 to justify the implementation of mass surveillance measures. An apparent example is provided by the indiscriminate use by the Chinese Government of the data collected by the Health Code

14 For a comprehensive overview of digital technology instruments used to fight COVID-19, see Trestian and others (n 4 above).

apps.[15] However, some have also observed that measures implemented to halt COVID-19 also emerge as 'extensions of already ongoing moves by democratic states to engage in domestic surveillance'.[16] This appears to be the case in Israel where the Government has employed legal mechanisms intended for counterterrorism purposes in order to use its security services to harness and utilise location and contact data for contact-tracing and to serve isolation orders.[17] In any case, as stated by the European Data Protection Board (EDPB), the use of digital technologies adopted to limit the spread of the virus for mass surveillance purposes represents a 'grave intrusion into people's privacy' and illustrates the risk of mission creep of the use of technology in combating the pandemic.[18]

Indeed, as Eck and Hatz argued, one may fear that 'governments will not be willing to abandon the new surveillance opportunities these apps offer and that personal data will be collected indefinitely and used for unanticipated ends'.[19] These concerns are not unfounded in circumstances where, presently, the Government of the United Kingdom (UK) 'plans to retain the data it collects for up to 20 years and denies individuals an absolute right to have their data deleted upon request',[20] and where such instances have existed in the past, such as surveillance measures implemented in the US in the wake of 9/11 that remain in place today.

Moreover, this mission creep is a grave concern as millions of citizens worldwide entrust their personal data to authorities for the protection of their health and the health of those around them via commonly used digital technology tools such as smartphones. Although many are presently optional, fears remain of the possibility

15 See Fan Liang, 'Covid-19 and Health Code: how digital platforms tackle the pandemic in China' (2020) 6 Social Media and Society 1; Helen Davidson, 'China's coronavirus Health Code apps raise concerns over privacy' *The Guardian* (London, 1 April 2020); Paul Mozur, Raymond Zhong and Aaron Krolik, 'In coronavirus fight, China gives citizens a color code, with red flags' *New York Times* (1 March 2020).

16 Kristine Eck and Sophia Hatz, 'State surveillance and the Covid-19 crisis' (2020) 19 Journal of Human Rights 603, 606.

17 Amir Cahane, 'Counterterrorism measures to counter epidemics: Covid-19 contact tracing in Israel' (*Blog Droit Européen* 18 July 2020); Rachel Noah, 'Using counterterrorism for fighting the pandemic: Israel during the days of Covid-19' (University of Oxford Faculty of Law, 19 June 2020); Dan Williams, 'Israel to halt sweeping Covid-19 cellphone surveillance next month' (*Reuters* 17 December 2020).

18 European Data Protection Board, 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak' (EDPB 21 April 2020).

19 Eck and Hatz (n 16 above) 607.

20 Ibid.

of COVID-19 tracking technologies becoming mandatory in the future through the introduction of their use being 'necessary to access workspaces', or being used as 'a condition of lifting restrictions', as is already occurring in India.[21] This kind of argument has indeed recently become apparent even in the EU, where passenger locator forms currently require travellers to declare their recent cross-country movements as well as prospected national whereabouts,[22] and some member states are requiring a COVID vaccination certificate to access workplaces or perform leisure activities.[23] The European Commission, citing the ePrivacy Directive, emphasises the requirement for necessity, appropriateness and proportionality in the use of these apps that have 'a high degree of intrusiveness', thus recommending that they remain voluntary.[24] This extends both to governments and providers of third-party services, so that 'choosing not to use the app may not adversely affect access to third parties' services, such as shopping malls, public transportation, or workplaces'.[25]

Private companies: function creep and lack of transparency

Similar concerns of a potential function creep of digital solutions developed to limit the spread of the virus have arisen in relation to the involvement of commercial actors. Reuse of data collected by private apps for commercial purposes, such as targeted advertising, often represents a breach of the data minimisation, retention and purpose limitation principles. Companies must collect only data which are necessary to the purposes of the processing, and they must not retain them if they are no longer necessary to those ends. Moreover, companies must not illegally exploit data originally collected for a significantly different purpose.

This apprehension is not groundless considering data controversies that have occurred in the past. For example, Alipay and Wechat have contractually secured the right to keep data collected in China after the

21 Rob Kitchin, 'Civil liberties *or* public health, or civil liberties *and* public health? Using surveillance technologies to tackle the spread of Covid-19' (2020) 24 Space and Polity 362.

22 See eg the European Digital Passenger Locator Form (dPLF); Government of Ireland, COVID-19 Passenger Locator Form.

23 See eg European Commission, EU Digital COVID Certificate; Government of Ireland, Department of the Taoiseach, 'Public health measures in place right now'.

24 European Commission, 'Guidance on apps supporting the fight against Covid 19 pandemic in relation to data protection' (2020/C124 I/01).

25 Klaudia Klonowska and Pieter Bindt, 'The Covid-19 pandemic: two waves of technological responses in the European Union' (Hague Centre for Strategic Studies April 2020).

pandemic.[26] The International Digital Accountability Council found that many apps 'request permissions that have the potential to be invasive if misused' and could 'allow apps to access other shared files on the device that could be used to infer personal information about the user, such as location, through calendar invites, or image metadata'.[27] Many contact-tracing applications, including Ireland's, have employed the Exposure Notification System developed jointly by Apple and Google. Despite their 'public-spirited' presentation, it remains that Apple and Google are private companies whose primary objective is to make profit and share it among their stakeholders. Bradford et al have drawn attention to the system's 'reserved functionality for additional unspecified associated metadata that might be collected later'.[28] It has also been noted that these apps do not operate in isolation on user's devices, and, as stated by Kitchin, 'by opening up location data, either via GPS or Bluetooth, a device is being made trackable by a range of adtech embedded in other apps, enrolling it into the ecosystem of location-based data brokers'.[29]

A further area of concern is the lack of transparency with regards to apps and other technologies developed by private companies to limit the spread of COVID-19. This is particularly true in the EU where full compliance with data protection law requires that data controllers disclose in an intelligible and accessible way the purpose and means of the data processing and that users have the option to exercise their rights, preferably through the app itself.[30] Transparency can ensure not only legal and fundamental rights compliance, but also increase trust in the population. An example of this being successful is Google's COVID-19 Community Mobility Report, which includes aggregated telecom data used by authorities in Ireland for mobility monitoring. This type of data is legally compliant through the use of anonymisation techniques, which allow location data to be processed in an aggregated form to prevent potential re-identification. Through Google's sharing of this aggregated location data with the public, it has been noted to potentially increase trust in the population by proving that private companies are really processing anonymised data and are not misusing personal information for hidden commercial purposes.[31]

26 Laura Bradford, Mateo Aboy and Kathleen Liddell, 'Covid-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes' (2020) 7 Journal of Law and the Biosciences lsaa034.

27 International Digital Accountability Council, 'Privacy in the Age of Covid: An IDAC Investigation of Covid Apps' (5 June 2020)

28 Bradford et al (n 26 above) 5.

29 Kitchin (n 21 above) 369.

30 See Emanuele Ventrella, 'Privacy in emergency circumstances: data protection and the Covid-19 pandemic' (2020) 21 ERA Forum 379.

31 Klonowska and Bindt (n 25 above).

Common risks: anonymisation and data breaches

Common to settings involving both public and private actors are the risks related to the collection of significant amounts of data, such as data breaches. Some measures have been implemented in the development of digital technologies to allow for a greater protection of personal data, such as the use of Bluetooth proximity tracing over GPS location tracking, the use of a decentralised approach over storing data on a centralised server, and processes of anonymisation or pseudonymisation. However, these approaches also appear to be flawed.

The use of Bluetooth proximity technology over GPS location tracking is seen to be more privacy-preserving since it only ascertains whether two devices enter in contact rather than constantly tracking their location. However, this is not a perfect solution. Location may still be tracked by authorities by introducing Bluetooth receivers in open settings, such as squares, roads and other public spaces.[32] The use of decentralised over centralised servers, although more in line with the data minimisation principle, does not reduce the risk of identification of individuals.[33] The possibility of re-identification through technological means and simple human inference also remains with the use of pseudonymous, and sometimes anonymous, data.[34] Indeed, as asserted by Kitchin, 'it is well established in the big data literature that unless the data are fully de-identified it is possible to reverse engineer anonymisation strategies by combing and combining datasets'.[35]

SACRIFICING PRIVACY IN FAVOUR OF PUBLIC HEALTH: COMPARATIVE PERSPECTIVES

Asian countries and the 'war' against the pandemic

In many Asian countries, maximisation of efficiency and effectiveness of public health containment strategies is often cited as one of the aims of the digital solutions used against COVID-19. Consequently, debates on privacy versus public health are often framed as requiring the sacrifice of one for the other.

---

32 Hyunghoon Cho, Daphne Ippolito and Yun William Yu, 'Contact tracing mobile apps for Covid-19: privacy considerations and related trade-offs' (2020) Cryptography and Security.

33 Stephanie Rossello and Pierre Dewitte, 'Anonymization by decentralization? The case of Covid-19 contact tracing apps' (*European Law Blog* 25 May 2020).

34 See Bradford (n 26 above).

35 Kitchin (n 21 above) 369.

South Korea's Health Minister Park Neung-hoo described Seoul as a 'COVID-19 war zone': posters with a red germ that looked like a bomb ready to be exploded could be seen on the streets of the South Korean capital city.[36] China's President Xi Jinping vowed to wage a 'people's war'.[37] War metaphors, as we see in the use of expressions such as 'war against pandemic', 'battle plan', 'enemy', 'frontline',[38] and even 'war against stupidity',[39] spread also beyond Asian countries[40] and demonstrate how the discussions on the need to combat COVID-19 were framed, encouraging the public to bring out the big 'artillery' and do 'whatever it takes, fast' or die.[41]

The privileging of the efficiency of public health strategies over privacy led to the favouring of particular technological designs, categories of operational actors and law enforcement regimes to the detriment of fundamental rights, particularly the rights to privacy and data protection. In this section, we analyse three concrete examples of this approach, namely the adoption of centralised approaches in contact tracing, the use of pre-existing commercial apps and the declaration of the state of emergency in order to compel the use of apps.

The debate surrounding contact-tracing apps has primarily focused on centralised versus decentralised systems. Storing data related to people's close contacts, or even location, in a centralised database presents greater risks from a data protection perspective since it increases the chances of security risks, such as data breaches, or potential misuse by the relevant authorities.[42] However, in some countries, centralised approaches remained the preferred option because of the clear efficiency gains. Indeed, privacy and data protection considerations aside, the efficiency of centralised systems is clear. In decentralised systems, health authorities cannot identify users of the apps and instead rely on each individual to act responsibly and report any notification they receive. Individuals may decline or

36 Anthony Kuhn, 'South Korea's Health Minister describes Seoul as a "Covid-19 war zone"' (*NPR* 7 December 2020).

37 Yew Lun Tian, 'In "people's war" on coronavirus, Chinese propaganda faces pushback' (*Reuters* 13 March 2020).

38 Yasmeen Serhan, 'The case against waging "war" on the coronavirus' (*The Atlantic* 31 March 2020).

39 Molly Gamble, '"I'm fighting a war against Covid-19 and a war against stupidity," says CMO of Houston hospital' (*Becker's Hospital Review* 1 August 2020).

40 See eg Lisa McCormick, 'Marking time in lockdown: heroization and ritualization in the UK during the coronavirus pandemic' (2020) 8 American Journal of Cultural Sociology 324.

41 Rosamond Hutt, '"Act fast and do whatever it takes" to fight the Covid-19 crisis, say leading economists' (*World Economic Forum* 23 March 2020).

42 See Yann Sweeney, 'Tracking the debate on Covid-19 surveillance tools' (2020) 2 Nature Machine Intelligence 301; Joseph Duball, 'Centralized vs decentralized: EU's contact tracing privacy conundrum' (*iapp* 28 April 2020).

refuse to voluntarily report themselves to the relevant authorities, thus undermining the whole contact-tracing system. Owing to this reason, developers, such as those of MorChana, a leading contact-tracing app in Thailand and operated by the Digital Government Development Agency, opted for a centralised approach.[43] In their report on COVID-19 and the Right to Privacy in South Korea, authors from the Korean Progressive Network JINBONET and the Institution for Digital Rights said that 'considering the nature of public health authorities, it is highly likely that they focus on the efficiency and medical necessity of enforcement, while they might relatively neglect deliberation on other basic rights including the right to informational self-determination'.[44] From a study by DigitalReach, contact-tracing apps in Southeast Asian states tend to choose centralised approaches over decentralised ones in order to maximise the efficiency of these solutions, even if the option is manifestly 'more vulnerable to being misused, exploited or exposed to a data breach'.[45]

Another strategy used in Asian countries to maximise the efficiency of public health solutions was to allow the simultaneous use of commercial contact-tracing apps, some of which pre-existing and reconverted for COVID purposes. While the Singaporean Government acted swiftly and released the first contact-tracing app deployed to a large public, other governments in Asia were quite slow in contrast.[46] Civil society and private sector initiatives therefore tried to fill this gap, introducing new purpose-built apps. In some cases, existing commercial apps were repurposed for use with COVID-19 response activities, such as SydeKick (tracking individuals) and QueQ (queue management systems for restaurants and hospitals).[47] This phenomenon had both

43 *Blognone,* ทีมงานแอพหมอชนะแจง ไม่ใช้ Apple/Google API เพราะอยากได้พิกัด GPS, เก็บข้อมูลบนเซิร์ฟเวอร์ตลอดเวลา' (translation from Thai: 'MorChana team said it rejects Apple/Google API because they want GPS location and want the data to always be kept on the server') (*Blognone* 21 January 2021).

44 Byoung-il Oh, Yeokyung Chang and SeonHwa Jeong, 'Covid-19 and the right to privacy: an analysis of South Korean experiences' (*JINBONET* 4 December 2020)

45 Digital Reach, 'Digital contact tracing in Southeast Asia: the Summary Report Submitted to ASEAN Intergovernmental Commission on Human Rights (AICHR)' (*Digital Reach* 27 November 2020).

46 However, it is not that other governments came completely unprepared. Taiwan and Hong Kong, for example, relied on their experience with SARS and existing infrastructure for that. Temperature scans were actually a normal practice in Hong Kong airport long before Covid-19, and face masks can be considered a common clothing item on the streets of Taipei. Taiwan also implemented early-stage containment policy, so the in-country contact tracing was probably less necessary at the outset of the pandemic.

47 Norton Rose Fulbright, 'Contact tracing apps in Thailand' (Norton Rose Fulbright 11 May 2020); Jotham Lim, 'Queuing app that acts as social distancing tool' (*The Edge Markets* 20 May 2020).

positive and negative effects. On the one hand, these apps were widely used by the population, thus increasing the spread of contact-tracing solutions. On the other hand, however, many of these apps often did not offer sufficient safeguards for the rights to privacy and data protection. Thailand, for example, saw many COVID-19 apps popping up quickly during the first wave of the virus in March 2020; this effectively helped the work of contact-tracing officers, while at the same time often failing to provide a privacy policy.[48]

One final example of the maximisation of the efficiency of public health solutions and a corresponding compression of fundamental rights in Asian states is the declaration of the state of emergency used to compel the use of contact-tracing apps among populations. Many states across the world declared a state of emergency, which, in most cases, granted governments the power to adopt executive decisions in a quicker and more efficient way in order to respond to the rapidly changing situation.[49] In some Asian countries, these new powers were also used to mandate the population to use contact-tracing apps. In Thailand, for example, the Government used the power granted by the Emergency Decree on Public Administration in the State of Emergency, BE 2548 (2005) to force people in five 'red zone' provinces to install contact-tracing apps.[50] As we have seen, this solution was expressly rejected in Europe as it would have deprived individuals of their ability to fully enjoy their rights to privacy and data protection, including being free to dispose of these rights, and would have allowed government authorities to monitor movements and social interactions of the entire population, with the potential risk of mission creep. Moreover, the state of emergency declared in some Asian countries did not only restrict the population's rights to privacy and data protection, but also had a domino effect on other constitutional guarantees and fundamental freedoms, such as the balance of powers and due process

48 SydeKick, PedKeeper and MorChana apps on Android provide no information on privacy as of 20 April 2020: Location tracking / Contact tracing technology comparisons (COVID-19).

49 See, for example, Suzanne Lynch, 'Trump declares national emergency over coronavirus' *Irish Times* (Dublin, 13 March 2020); Benoit Van Overstraeten and Christian Lowe, 'France declares public health state of emergency over Covid-19' (*Reuters* 14 October 2020); Department of the Prime Minister and Cabinet of New Zealand, 'State of National Emergency and national transition period for Covid-19' (31 July 2020); Rebecca Ratcliffe, 'Malaysia declares Covid state of emergency amid political turmoil' *The Guardian* (London, 12 January 2021); Belén Carreño, 'Spain announces new state of emergency as Covid infections soar' (*Reuters* 25 October 2020); 'Coronavirus: Japan declares nationwide state of emergency' (*BBC News* 16 April 2020).

50 'Position-tracking app required in 5 provinces' *Bangkok Post* (8 January 2021).

51 Joseph Sipalan, Rozanna Latiff and Nick Macfie, 'Explainer: why a state of emergency raises concerns in Malaysia' (*Reuters* 12 January 2021).

rights. Indeed, in some Asian countries, the state of emergency made the regular checks and balances of government powers, such as administrative review, merely an option, and this also had the effect of suspending the right to appeal.[51]

Inalienable nature of privacy and data protection in Europe

Arguments of sacrificing privacy and data protection in favour of preventing the spread of disease have gained momentum across the globe. Even within Europe, one may have a similar impression by reading the words that the Data Protection Commissioner of the Council of Europe and Chair of the Convention 108 stated at the beginning of the COVID-19 pandemic:

> data protection can in no manner be an obstacle to saving lives, and that the applicable principles will always allow for a balancing of the interests at stake.[52]

However, while balancing the right to privacy and data protection against other rights and competing interests is definitively possible, it is important to stress that in the European context a specific limit to this compression exists. Arguments of a substantial derogation of privacy and data protection in order to prevent and slow the spread of COVID-19 are unworkable in Europe owing to the inalienable nature of fundamental rights in EU law. The Charter of Fundamental Rights of the European Union safeguards the rights to privacy (article 7) and data protection (article 8), including the requirement in article 52(1) to 'respect the essence' of all fundamental rights. This last provision is particularly important because, as stated by Lenaerts, it 'defines a sphere of liberty that must always remain free from interference'.[53] This norm is interpreted as that rights protected by the Charter contain a core that cannot be compromised, no matter the strength of the competing interest. Accordingly, although privacy and data protection rights may be relaxed to allow for a greater balancing against other interests, such as the efficiency of measures seeking to reduce the extent of a global pandemic, a compression of the core principles of the rights to privacy and data protection is not possible in the EU. This is an important point to stress, and which probably people should be made more aware of, as we will argue in the next sections. Our perception is indeed, as the PRIVATT survey may empirically demonstrate for Ireland, that individuals, notwithstanding their privacy attitude, can be persuaded that they have the power to dispose of their fundamental

52 Alessandra Pierucci and Jean Phillippe Walter, 'Joint statement on the right to data protection in the context of the Covid-19 pandemic' (Council of Europe, 30 March 2020).

53 Koen Lenaerts, 'Limits on limitations: the essence of fundamental rights in the EU' (2019) 20 German Law Journal 779, 781.

rights to privacy and data protection freely in order to satisfy apparently more important values, such as public health. Conversely, the knowledge of the inalienable nature of their core privacy rights could foster a critical attitude among the general population vis-à-vis digital technology instruments that can potentially be unnecessarily restrictive of fundamental rights. Moreover, an increased awareness of the duty of state authorities to preserve privacy and data protection rights in any circumstance, even in the presence of other important interests to satisfy, could ultimately enhance people's trust in the measures adopted by governmental actors.

The development of the concept of 'essence' of fundamental rights under article 52(1) was first interpreted in a CJEU case that, coincidentally, involved the rights to privacy and data protection and was initiated in Ireland: *Digital Rights Ireland*.[54] On that occasion, the extensive retention of data imposed by the Data Retention Directive was not seen as affecting the essence of the rights to privacy and data protection.[55] Yet, the Directive was eventually invalidated because it represented 'a particularly serious interference with those rights', which was not proportionate to the objectives of investigating, detecting and prosecuting serious crime.[56] While this was the first development of the notion in EU law, the idea of the 'essence' of fundamental rights is present in the constitutional case law of many EU member states and in international human rights treaties, which Brkan notes share the 'purpose' of preventing 'the holder of the fundamental right to be stripped of the inalienable core of her fundamental right'.[57]

The 'essence' of fundamental rights was further developed in *Schrems I*, in which the CJEU stated that US legislation allowing national security authorities to access EU data on a generalised basis compromises the essence of article 7 of the EU Charter of Fundamental Rights enshrining the right to respect for private life. Ojanen posits that the judgment in *Schrems I* represents a concrete judicial implementation of article 52(1) of the Charter by pragmatically explaining that fundamental rights present an inviolable core that

54 *Digital Rights Ireland* [2014] ECJ Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paras 39–40.

55 Ibid.

56 Ibid para 39. See Edoardo Celeste, 'The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios' (2019) 15 European Constitutional Law Review 134.

57 Maja Brkan, 'The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning' (2019) 20 German Law Journal 864, 866; see also Jerome J Shestack, 'The philosophic foundations of human rights' (1998) 20 Human Rights Quarterly 201.

cannot be compressed in any circumstance.[58] *Schrems I* determines that fundamental rights under the Charter are not just 'principles that may be balanced and weighed against other competing principles', but are also 'capable of generating rules that should be applied in an either/or manner'.[59] Therefore, they can prevail against other interests, 'no matter how weighty or pressing the legitimate aims of any restriction are, or any other legal arguments made'.[60] Likened to the inner core of an onion by Brkan, the 'essence' is considered as representing

> the untouchable core or inner circle of a fundamental right that cannot be diminished, restricted or interfered with. An interference with the essence of a fundamental right makes the right lose its value for society and, consequently, for the right holders.[61]

Accordingly, while measures can be implemented to reduce and prevent the spread of COVID-19 through the use of digital technology, the core of the fundamental rights to privacy and data protection cannot be given up, as doing so would interfere with the 'essence' of fundamental rights in the EU.

To conclude this comparative section, it is important to stress that the geographical factor plays a significant role: the concepts of privacy, data protection and consequently the derived notion of the 'essence' of these rights do not receive a univocal definition worldwide, especially in terms of their balancing with other fundamental rights. Therefore, the finding of the PRIVATT survey that highlighted an increased willingness of the Irish population to compress their privacy rights, or to be less privacy-concerned, has to be read within the specific context of Europe and its fundamental rights tradition, as established by decades of case law of the CJEU and the European Court of Human Rights. It is interesting to observe that the starting point of this shift is not a situation where these specific rights are usually considered as subordinate to other interests, but contrariwise a context where their primary relevance has now been consolidated from a legal perspective. This point is particularly telling because it exposes a more significant divergence between the legal dimension and societal perception, an element which the next section will further analyse with reference to a detected mistrust of the Irish population towards the digital technology solutions adopted to counteract the spread of COVID-19.

---

58 Tuomas Ojanen, 'Making the essence of fundamental rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter: ECJ 6 October 2015, Case C-362/14, Maximillian Schrems v Data Protection Commissioner' (2016) 12 European Constitutional Law Review 318.

59 Ibid 322.

60 Ibid.

61 Maja Brkan, 'The concept of essence of fundamental rights in the EU legal order: peeling the onion to its core' (2018) 14 European Constitutional Law Review 332, 333.

FORMAL LEGALITY VERSUS LEGAL REALITY

Fundamental rights-compliant solutions in the EU

Absent the possibility of sacrificing the core principles of the right to data protection and privacy on the altar of public health, EU authorities and member states began working together to provide guidelines on how to introduce fundamental rights-compliant digital solutions in the EU. During the first wave of the pandemic, in March 2020, one can lament a certain delay in providing a coordinated and adequate response at EU level. Amid internal trepidation, national governments acted as solo actors in search of the right contact-tracing app, hastily organising calls for tenders and heavily relying on private companies and spontaneously emerging scientific consortia. Only on 8 April 2020 did the EU Commission announce the imminent creation of a common toolbox on the use of digital technology to combat the spread of COVID-19, stressing that a lack of coordination in the deployment of similar apps could also significantly impact the functioning of the single market.[62] On 15 April 2020, the eHealth Network adopted a first series of recommendations to design contact-tracing apps in the EU, followed soon after by detailed guidelines from both the European Commission and EDPB.[63]

Reading these different documents together, the response of the EU to fears of incumbent mass surveillance and potential mission creep in Europe is clear. Firstly, these documents recall that the General Data Protection Regulation (GDPR) and the ePrivacy Directive prohibit the bulk collection, access and storage of health data and location data in any circumstance, even in the context of a global pandemic, since this would violate the essence of the fundamental rights to privacy and data protection.[64] What contact-tracing apps in the EU can do therefore is limit their processing to 'proximity data', namely information about the likelihood of virus transmission based on the epidemiological distance and duration of contact between two individuals. Simultaneous processing of other kinds of data is discouraged in order to comply with the principle of data minimisation.[65]

---

62 European Commission, 'Commission Recommendation of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the Covid-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data' C(2020) 2296 final.

63 eHealth Network, 'Mobile applications to support contact tracing in the EU's fight against Covid-19: Common EU Toolbox for Member States' (2020); European Commission (n 24 above); EDPB (n 18 above).

64 See *Digital Rights Ireland* (n 54 above); see also Celeste (n 56 above).

65 EDPB (n 18 above).

Proximity-tracking apps rely on a radio technology such as Bluetooth to estimate the distance between two devices using signal strength, assuming a device is a representation of the existence of a user. In the context of COVID-19 tracking, the app developer can decide that, if two users are in a sufficient proximity for a sufficient period of time, the apps in both devices exchange identifiers. Each app logs an encounter of the other's identifier, which can be later used for contact tracing and notification. The identifier is not necessarily personally identifiable to an actual person, it can only be an identifier of a device. The identifier can also change over time. These implementation details can be different among proximity-tracking apps: for example, Apple and Google's Exposure Notifications change the identifier every 10–20 minutes.[66] The users' locations are not necessary, as the application need only know if the users are sufficiently close together to create a risk of infection. However, some proximity-tracking apps may collect location data as well.[67] Location data can be collected from the sensors present in the device itself (like GPS and WiFi) and from the 'check-in' feature.

While, in general, the design of the proximity-tracking functionality among apps are similar, the mechanisms for keeping logs of contacts and notifying users about infection risk can differ significantly.[68] Some apps rely on central authorities that have privileged access to information about users' devices. With the real contact information provided during the app registration, the central authority can contact people who are at risk through channels outside of the app. Some apps, instead, do not ask for real contact information, and instead are only able to send the notification to the device and ask the user to contact the authority. This last solution was the one embraced by the EU Commission guidance: data about close contacts should not be automatically shared with health authorities, but should be up to the individual user to decide whether to do so. Furthermore, a warning received by the app should not lead to an automatic decision aiming to restrict the fundamental rights of the users in order to avoid the risks of a blind form of automated decision-making, in line with article 22 GDPR. Digital contact-tracing apps can complement, but should not

66 Google, 'Exposure notifications: using technology to help public health authorities fight Covid-19'.

67 Kif Leswing, 'Utah has rejected the Apple-Google approach to tracing coronavirus, and is using an app made by a social media start-up instead' (*CNBC* 13 May 2020); Andrew Clarance, 'Aarogya Setu: why India's Covid-19 contact tracing app is controversial' (*BBC News* 15 May 2020).

68 Andrew Crocker, Kurt Opsahl and Bennett Cyphers, 'The challenge of proximity apps for Covid-19 contact tracing' (*Electronic Frontier Foundation* 10 April 2020).

replace, traditional contact tracing in a way that they automatically log every contact during the day.[69] This complements human less-than-perfect memory and may make it easier for health practitioners to work. However, an app treats all 'contacts' between two people the same. Spending the same amount of time in the same proximity with a grocery clerk in a shop who is protected by adequate equipment and with your partner in a private room carry, of course, different risks of transmission. False positives may also arise for two people who are in separate rooms, with thin walls, next to each other.[70]

EU guidance on the topic also made clear that national health authorities should play a primary role, possibly as data controllers, thus depriving private companies of the power to define the purpose and means of data processing.[71] The use of apps should remain voluntary, in order to avoid potential discrimination in public spaces and in the work place, and consent should not be asked for a 'bundle of different functionalities'.[72] The EDPB, however, recommends that consent should not be used as the legal basis for data processing, but rather the 'public interest' should be relied on.[73] This would be justified by the asymmetry between data controllers, which are often health authorities, and single individuals, who could feel the pressure to provide their consent vis-à-vis state authorities. Apps should be dismantled as soon as the health emergency is over in order to prevent the risk of mission creep after the end of the pandemic.[74] Collected data should not be reused for other purposes, especially other commercial or law enforcement purposes, unless provided for by law for scientific objectives.[75] Apps should reflect both the latest public health guidance and should rely on the most modern technologies in terms of privacy compliance, cybersecurity and accessibility.[76] The apps' source code should be made public and available for review.[77] Users' data should be processed for specific purposes, possibly defined by law, should be at least pseudonymised, stored securely and automatically deleted after a period of time proportionate to the incubation period.[78] A data protection impact assessment (DPIA) following article 35 GDPR is

69 EDPB (n 18 above).
70 '"App thought I'd catch Covid through neighbour's floor"' (*BBC News* 5 October 2020).
71 European Commission (n 24 above).
72 Ibid.
73 EDPB (n 18 above).
74 eHealth Network (n 63 above).
75 European Commission (n 24 above).
76 eHealth Network (n 63 above).
77 European Commission (n 24 above).
78 Ibid; eHealth Network (n 63 above); EDPB (n 18 above).

recommended given the processing of special categories of data on a large scale.[79] Furthermore, the EDPB recommends the publication of the DPIA in order to enhance the level of transparency of decision-making among the general population as well as public scrutiny.[80]

Last, but certainly not least, from an EU perspective, contact-tracing apps should be interoperable, and thus able to work properly in a context where cross-border movements are resumed. Given the improving situation and wider distribution of vaccines, when more people begin travelling from one country to another, the interoperability of these apps is getting more attention. The EU Commission is keeping track of the app interoperability: out of 27 member states, 21 have an app with only 11 being interoperable with others.[81] The situation in Ireland as regards contact tracing is particularly complicated by the presence of two jurisdictions, the Republic of Ireland and Northern Ireland, on the same island. Ireland is not part of the Schengen area, but is instead part of a Common Travel Area with the UK. More specifically, on the island of Ireland, at the moment, there is no physical border between the Republic and Northern Ireland. The UK did, however, leave the European Union in January 2020, and, owing to the Northern Ireland Protocol, Northern Ireland *de facto* remains part of the European internal market.[82] The conundrum that the introduction of contact-tracing apps has therefore created on the island of Ireland relates to the interoperability of multiple contact-tracing apps, respectively developed in an EU and a non-EU country. To make the situation even more complex, Northern Ireland has developed its own app, announcing its interoperability with both the Irish and British (including the apps of Scotland, Jersey and the NHS app used in England and Wales).[83] In a context where the Brexit negotiations reopened the question of the Irish border, with a pandemic which conversely knows no frontiers, the choice by individuals of which contact-tracing app to download becomes an issue of political allegiance, and the use by health authorities of data collected by those apps may trigger the complexities of a cross-border data transfer to a third country. An all-Ireland approach seems to be more than ever needed.[84] Only in this way can digital technology

79 EDPB (n 18 above).

80 Ibid.

81 European Commission, 'Mobile contact tracing apps in EU member states'.

82 Protocol on Ireland/Northern Ireland to the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community [2019] OJ C 384 I/92.

83 NI Direct Government Services, 'Coronavirus (Covid-19): StopCovid NI proximity app'; 'Ireland achieves world first in contact tracing app interoperability – Minister Donnelly' (*Gov.ie* 4 August 2020).

84 See further the articles by Mary Dobbs and Katharina Ó Cathaoir and Christie MacColl, in this issue.

simultaneously be at the service of public health, facilitate freedom of movement and be respectful for the rights to privacy and data protection.[85]

Lastly, the European Commission launched the EU Digital COVID Certificate (DCC) on 1 July 2021.[86] The data contained on the DCC includes the holder's name, date of birth, date of issuance, and information about type of vaccine, COVID-19 test or date of recovery from the virus, as well as a personal identifier, with this data being stored on the certificate without being retained by the app when checked by a third party.[87] The measure has received criticism owing to difficulties in its implementation and its impact on fundamental rights, beyond the rights to privacy and data protection. In particular, it was noted that a data protection impact assessment was not conducted due to the 'urgency' of the situation, thus potentially intensifying the risks of an already problematic system processing sensitive data related to the health of individuals.[88] Moreover, concerns over discrimination were strengthened in Ireland as the DCC could be used to access indoor hospitality in Ireland.[89] Implementation difficulties were indeed faced in Ireland as delays in implementing the system were criticised as denying those eligible their freedom of movement and right to travel.[90]

Lack of trust in Ireland: the importance of transparency and data protection literacy

Despite a series of criticalities related to the way the EU and the single member states are deploying digital technology to fight against the virus, it is possible to highlight that the attention to and respect of fundamental rights was a key character of the European approach. Yet, the results of the PRIVATT survey found that the Irish population perceives digital technology solutions employed to control the spread of COVID-19 as potentially infringing their fundamental rights, despite these solutions formally respecting the specific EU guidance and

85 See further the article by Maria Grazia Porcedda in this issue.

86 Regulation (EU) 2021/953 of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable Covid-19 vaccination, test and recovery certificates (EU Digital Covid Certificate) to facilitate free movement during the Covid-19 pandemic 15.6.2021 OJ L211/1; European Commission (n 23 above).

87 Ibid.

88 See Oskar Josef Gstrein, 'The EU Digital COVID Certificate: a preliminary data protection impact assessment' (2021) 12 European Journal of Risk Regulation 370.

89 Department of Health and Department of An Taoiseach, 'EU Digital Covid Certificate' (*Gov.ie* 11 August 2021).

90 Barry O'Halloran, 'Delay over EU digital passes will deny travel rights to 1.5m Irish people – Ryanair' *Irish Times* (Dublin 1 July 2021).

national law. We argue that this data, from a socio-legal perspective, exposes a discrepancy between the formal legality and legal reality of the digital solutions adopted by the Government. In other words, we note that there is an apparent inconsistency between what is formally legal and what is perceived as fully safeguarding fundamental rights by Irish residents.

Firstly, from a socio-legal perspective, this observation exposes a potential lack of transparency and involvement of the general population in the decision-making processes that have coordinated the response to the virus. The necessity to resort to specialists, such as epidemiologists and virologists, has unavoidably positioned the political debates about the measures to implement in order to defeat the virus far from the general population. Also, the tight timeframe that governments and health authorities had in order to introduce restrictions to counteract the rapid spread of the virus did not favour a high level of inclusion in decision-making processes. This lack of involvement – combined with contradictory claims by experts and politicians and a general absence of transparency both at national and international level – was one of the factors that contributed to a general mistrust towards the actions of the Government in Ireland, in particular in relation to the deployment of digital technology solutions.

Secondly, this observation more generally begs two intertwined questions related to the level of awareness of legal safeguards offered by fundamental rights, and in particular in relation to the right to data protection, among the general population. One can indeed dispute to what extent the existence of concrete data protection guarantees, which aim to protect citizens against potential misuse of their data, is known by the general public. Privacy concerns related to the potential misuse of mobile apps introduced to fight COVID-19 are certainly not unfounded. As we have seen, in some countries, contact-tracing apps process location data and have been used by governments for purposes that went well beyond the mere fight against the virus. However, the response to this concern at EU level, albeit slow, was net and clear. The EU Commission, the e-Health Network and the EDPB issued detailed guidance on the use of digital technology in order to fight COVID-19 while at the same time safeguarding EU fundamental rights. And, beyond that, this bold approach was adopted thanks to the solid legal framework that has emerged over the past few decades in the case law of the CJEU, which has repeatedly affirmed that the essence of the right to data protection and privacy cannot be compressed to the benefit of other important interests, such as national security or public health. If, despite this commitment by EU institutions to make sure that technology employed to fight the pandemic respects the essence of fundamental rights, Irish residents still perceive a certain level of risk associated with

the technology solutions adopted, one could question to what extent EU legal guarantees are really understood by the general population.

The discrepancy between digital strategies which are formally compliant with EU data protection rules and people perceiving the risk of potential infringement of their fundamental rights might expose an issue in terms of knowledge of EU legal safeguards, in particular in relation to data protection law. Indeed, in some sectors, there was a widespread belief that data protection only emerged with the entry into force of the GDPR in 2018. While this is not the case, European data protection law is still a relatively recent body of law, emerging in the 1970s in response to technological developments surfacing in Europe.[91] Moreover, EU data protection and privacy norms are not codified in a single piece of legislation, but are stratified in different EU and national constitutional texts, EU regulations, directives and national statutes, as well as EU and national judicial decisions. We therefore hypothesise that Irish residents – although this observation can likely be extended to the entire EU population – may still have to familiarise themselves with the legal safeguards that this fragmented body of norms offers them.

Secondly, this point raises the interrelated question of to what extent the EU data protection and privacy framework is accessible to the general population. We already mentioned the issue of stratification of legal provisions related to privacy and data protection. An issue that is further exacerbated at national level given the 'unenumerated nature' of the right to privacy within the Irish Constitution.[92] In Ireland, indeed, the Constitution does not explicitly enshrine those rights, which have been progressively inferred from the text of the Constitution by Irish courts.[93] The GDPR, from this perspective, represents a turning point in EU data protection law because it introduces a uniform set of rules across Europe and stresses the importance of using clear and intelligible language.[94] However, further work is still probably required in order to achieve an adequate level of literacy among the general population in the field of data protection and privacy. We suggest that the current pandemic, among the many lessons that it offers us, will not only be an opportunity for state authorities and private companies to enhance their level of compliance with EU and national law and good practices in the field of data protection and privacy, but will also help the general

91 Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right* of the EU (Springer 2014).

92 Eoin Carolan and Ailbhe O'Neill, *Privacy and the Irish Constitution* 2nd edn (Bloomsbury Professional 2019)

93 *Ryan v Attorney General* [1965] IR 294; *McGee v Attorney General* [1974] IR 284; *Norris v Attorney General* [1984] IR 36.

94 See article 12 GDPR.

population to familiarise themselves with those norms and understand the safeguards that they may offer. An enhanced knowledge of the legal protection offered by EU and national law in terms of privacy and data protection rights may ultimately lead to two positive effects. On the one hand, it could strengthen the critical attitude of the general population vis-à-vis technology solutions adopted by state authorities. This might be particularly useful if the Government were to implement effective participatory practices to allow the population to express their views on key measures potentially restricting the exercise of their freedoms. In this way, indeed, a population which is more aware of its legal entitlements could more easily contribute to decision-making processes by advancing critical comments and propose innovative ways to promote fundamental rights-compliant solutions. On the other hand, increasing the general population's knowledge of privacy and data protection guarantees will also help consolidate people's trust in innovative digital technology solutions proposed by state actors after accurate and transparent fundamental rights impact assessments. A virtuous-circle effect would emerge from this process: an enhanced commitment by state authorities to guarantee fundamental rights combined with an increased level of transparency would produce even better results if achieved in conjunction with a higher level of awareness among the general population of their legal entitlements, as well as an active involvement in decision-making processes. The dichotomy between states seen as absolute regulators and distrustful passive citizens would be overtaken by the prospect of a society where mutual trust between state and individuals is built on transparency and inclusion in decision-making processes, commitment to fundamental rights and a critical attitude from both sides towards new policies involving the adoption of digital technology tools.

CONCLUSION

In times of public emergencies, assessing people's potential perception of novel policy measures is quintessential to ensuring an elevated level of norm compliance and the ultimate success of a regulatory strategy. The ongoing COVID-19 pandemic has projected state actors and individuals into a state of uncertainty. Policymakers had to test different regulatory strategies in order to limit the spread of the virus. For many citizens this was the first global public emergency of their life. This feeling of uncertainty, which was shared across all societal actors, was at times combined with the fear of potential function creep of the instruments introduced by public authorities to counteract the diffusion of the disease, with particular apprehension about digital technology tools.

Indeed, in contrast to previous health emergencies, the current crisis is a technological one. Digital technology solutions are significantly contributing to help limit the spread of the virus. Their role is, however, Janus-faced. In this article, we have analysed the risks associated with the use of digital technology in the fight against the pandemic, highlighting in particular their potential compression of privacy and data protection rights as well as the broader danger of degeneration of these tools into mechanisms of state control. In several states across the world, the adoption of a war rhetoric has paved the way for a consolidation of government surveillance through digital technology solutions and, at first sight, an indefinite suspension of constitutional guarantees. A mistrust in the technological measures adopted by the Government to fight the pandemic as well as privacy and data protection concerns also characterised Irish residents' perception of the policy strategies adopted in the Republic, as highlighted by the results of the PRIVATT project. This article has proposed a socio-legal interpretation of these findings, highlighting a potential link between Irish privacy attitudes during the pandemic and a lack of legal literacy and an insufficient level of transparency and participation in decision-making.

The survey conducted in the context of the PRIVATT project has indeed revealed a shift in the propensity of Irish residents to consent to the use of their personal data to fight the spread of COVID-19. If at first sight this trend might be interpreted as evidence of trust in the Government's strategy to counteract the virus, the survey simultaneously shows that a still significant portion of the population has concerns related to potential privacy and data protection infringements through the use of digital technology tools introduced to fight the pandemic. This data exposes a discrepancy between the formal legality of the technological solutions adopted in Ireland and the legal reality where individuals perceive these solutions as potentially infringing their fundamental rights. In this paper, we have explained that, in the EU, the core principles of the rights to privacy and data protection cannot be relinquished in favour of public health, as their essence should remain preserved. This has led a multiplicity of EU actors to adopt detailed guidelines on how to unlock the potential of digital technology in the fight against the pandemic while preserving the essence of the fundamental rights to privacy and data protection. The fact that the measures adopted in Ireland explicitly follow these guidelines, but at the same time Irish residents still manifest privacy concerns, is argued to also expose a broader set of issues related to legal literacy of the population and transparency of decision-making practices. We posit that EU data protection law as well as Irish privacy law are not easily accessible to the general population due

to their relative novelty, complexity and stratification. Increasing the level of privacy rights literacy among the population may trigger a virtuous circle, enabling critical feedback from citizens as well as more participative decision-making processes. This result, combined with an enhanced level of transparency by the Government, may lead to a major awareness of the need to restrict fundamental freedoms, increase trust in the policy measures and, ultimately, ensure a higher level of compliance.

In light of our analysis, we conclude with a series of recommendations in relation to the adoption of digital technology tools to combat the spread of a pandemic. We encourage their use as general guidelines for enabling the measures necessary in emergency situations to become more trustworthy to people. From our analysis we understand that enhancing transparency and data protection literacy is of utmost importance. Adequate information should be provided to data subjects, even if legal bases other than consent for data processing are available. This information should be offered using clear and intelligible language in order to help improve the population's understanding of the norms and methods implemented by digital responses to COVID-19. This should be ensured with regards to the methods used and actors involved in digital responses to the COVID-19 crisis. Policymakers should be upfront about the challenges posed by the lack of knowledge and experience of events like the current pandemic. Indeed, while governments and policymakers may be doing their best with the information available to make responsible choices for the entire population, sometimes responses might fail despite these good intentions.

Moreover, in order to increase levels of trust of the general population in digital technology tools introduced to counteract a pandemic, more transparency and participation should be sought during decision-making processes. Involvement with and communication to the wider population in early phases of decision-making processes related to the employment of digital technology solutions to fight COVID-19 is crucial to enhance the level of legitimacy of the adopted solutions and as a trigger for greater transparency of the decision-making processes. To this end, a greater involvement of and reliance on public actors is recommended. The involvement of private actors just for the sake of efficiency should be avoided, and, in circumstances where they are used, how and why public and private actors are cooperating should be fully explained to minimise the discrepancy between formal legality of the measures adopted and a legal reality witnessing a general mistrust from the population.