Antonella Zarra, Silvia Favalli,
Matilde Ceron

Algorithms and Prejudice? Covid-19, Contact Tracing and Digital Surveillance in the EU

1. *Introduction*

The Covid-19 pandemic has revamped the debate over algorithmic surveillance and its potentially detrimental effects on fundamental rights. Digital tools have been heavily employed to track and curb the curve of contagion as well as to monitor vaccination campaigns. While many governments have released artificial intelligence (AI)-enabled applications to complement manual contact tracing or enforce lockdown measures, a parallel exercise has been carried out by non-institutional actors, which have developed their own set of surveillance technologies supporting a smooth return to daily activities past the early phase of the emergency. After the most severe restrictions were lifted, digital tools remained a primary mitigation and tracing measure. In substance, the pandemic has served as a catalyst for a gargantuan proliferation of AI surveillance

1 We warmly thank the editor and two anonymous referees for their thoughtful comments and precious feedback on the manuscript. The contribution of Matilde Ceron and Silvia Favalli to this research was conducted under the research project 'RISID - Realizing the right to Social Inclusion for persons with Disabilities through new tools of smart communication and sharing knowledge: from international to local effectiveness', financed by Fondazione Cariplo http://risid2020.wordpress.com/. On the whole, this article is the product of joint reflection. However, sections 1 and 4 were written by Matilde Ceron, sub-sections 2, 2.1 and 3.3 were written by Antonella Zarra, and sub-sections 3, 3.1 and 3.2 were written by Silvia Favalli. Sub-sections 2.2 and 5 were written by Matilde Ceron, Antonella Zarra and Silvia Favalli together.

through massive data collection and tracking. If, on the one hand, the spread of these AI-powered tools has increased the public awareness towards the use of technology for surveillance and monitoring, on the other, such a pervasive presence into individuals' private sphere raises significant legal and ethical concerns that may extend well beyond the immediacy of pandemic management.

A central concern relates to whether and to what extent threats to public health may justify a State's – or a firm's – intrusion on individuals' rights. Most countries attempted to control the outbreak through draconian lockdowns combined with thorough testing and tracing strategies. After the implementation of drastic monitoring measures by China and South Korea at the beginning of the pandemic, EU Member States launched their own digital tracing initiatives. The European approach is widely benchmarked for higher attention to citizens' rights, not only in comparison to non-democratic regimes but also, for example, against the American uninhibited libertarian approach. For these reasons, the EU offers a salient case in the analysis of how safeguards may prove insufficient under the pressure of health and economic concerns.

Additionally, the relevance of digital pandemic surveillance is not limited to early waves and lockdowns. In late 2021, containment measures remain in place as Covid-19 continues to ravage. At the same time, the public debate has largely archived official contact tracing apps, which gained limited participation in most countries (Seto *et al.* 2021), to focus on vaccinations and Digital Certificates. Nevertheless, nearly two years after the Covid-19 crisis rose to the ranks of a global pandemic, digital surveillance remains a cornerstone of the mitigation of contagion. At the same time, the largely uncontested proliferation beyond official apps undermined the voluntary focus characteristic of the EU approach, as surveillance has at times become a requirement for accessing workplaces, universities or services. Implications of choices – and their distributive consequences – during the pandemic may also be long lasting as the boundaries of individual rights have been tested and contested by the health crisis. Under such premises, the impact of digital pandemic management on privacy, discrimination and inclusion is at the frontier of concerns over the ethics of AI.

The analysis considers the human rights implications of pandemic surveillance against well-established pre-existing challenges in relation

to the use of automated decision-making systems. In doing so, building on the literature on the ethics of AI, the analysis of the relevant EU legal framework and case studies of problematic pandemic digital surveillance tools, the article outlines the balance between public health and algorithmic injustice, defined here as the exacerbation of existing inequalities and socio-economic disadvantages endured by vulnerable groups through the use of algorithmic technology.[2] The assessment highlights the strengths and weaknesses of the EU legal framework in protecting human rights within the digital ecosystem. The analysis identifies possible problematic aspects of the wide variety of digital solutions introduced in the public and private sector including contact tracing and exposure notification applications, wearables and other devices to enforce social distancing, AI-based symptoms checking questionnaires and biometric solutions to access physical spaces (e.g. workplace, education). From such a perspective, the analysis provides empirical evidence through selected case studies of Covid-related apps and digital tools within the EU displaying shortcomings in the arenas of privacy violations, bias and/or discriminatory outcomes and limits to accessibility.

Findings put a dent in the comparative claim of limited ethical concerns within the European model, especially in the highly fragmented ecosystem which exceeds official apps. Such results are robust to the potential additional safeguards under the Proposal for an AI Regulation (hereinafter AI Act) (COM(2021) 206 final) tabled by the European Commission, whose multi-tier risk-based approach marks a step forward in identifying the inherent risks of algorithmic tools, but which in its current form risks delivering further legal uncertainty. In fact, without changes to the current draft of the proposal, in particular when it comes to the provisions on biometric identification systems, even in the protective

[2] The existing literature refers more generally to algorithmic discrimination or bias, namely the phenomenon of intended or unintended biases in software that lead to unfair outcomes for particular groups of individuals (see, for instance Barocas 2016; Hacker 2018; Xenidis and Senden 2020; Zuiderveen Borgesius 2020; Wachter *et al.* 2021). However, for the purpose of this analysis, we refer to algorithmic injustice, which in our view better addresses the multifaceted consequences of algorithmic surveillance during the pandemic, which are not only limited to discrimination but also to privacy and accessibility concerns.

ecosystem of the European legal framework, human rights may remain at the mercy of the proliferation of digital surveillance tools.

The work contributes to the extant literature on AI ethics and digital policy in the Covid-19 context with an assessment of how the pandemic offers a breeding ground for algorithmic injustices. In this respect, a particular concern emerges about the risks of fragmentation and privatization of tracing as local entities and companies have developed their own tracing systems without the transparency and scrutiny of official apps. Such complementary tools are already imposed on citizens when going to work, school or accessing services even in the absence of mandatory general use, and they may be the most problematic insofar they are harder to map, decodify and monitor by public authorities. The analysis hence not only sheds some light on the problems of algorithmic injustice in the pandemic within the EU borders, but also indicates how such an extreme case is a powerful cautionary tale of the challenges ahead as algorithms – whose boundaries of acceptance have been further expanded by the health emergency – take an increasingly pervasive space in our daily activities.

2. *The risks and ethics of digital surveillance in a pandemic*

The pandemic is *per se* an example of a phenomenon far from egalitarian in the impact of the health crisis and its mitigation on society. Covid-19 has exacerbated pre-existing unjust conditions, disproportionately affecting disadvantaged and vulnerable groups categories of individuals that were already suffering from economic and social disadvantages. The direct health and economic cost of the pandemic has indeed increased inequalities (Deaton 2021). Indirectly, inequalities extend to social control and repression by authorities, also by means of technology-led surveillance, which is more widespread in delicate times characterized by political tension, protests and health emergencies (European Parliament. Directorate General for External Policies of the Union, 2021).

In parallel, the health crisis has deeply accelerated the pre-existing trend of the datafication of society as AI-powered and biometric solutions became ubiquitous. Private and public actors have had access to a wider range of information, from live time location to sensitive health

data. In light of the augmentation of surveillance powers in the aftermath of the pandemic, it is worth assessing the role of technology in managing contagion and supporting mitigation measures. In placing the analysis within the existing literature of digital and AI ethics, the section considers (i) the use of digital technology in tackling the pandemic, (ii) comparative differences in the EU approach, (iii) features and risk across the taxonomy of pandemic surveillance and (iv) its ethics and distributive implications.

2.1. The rise of pandemic surveillance: features and risks

The isolation of symptomatic individuals and the tracing of asymptomatic individuals have been two key aspects in strategies aimed at containing the spread of Covid-19. Contact tracing procedures follow two paths: manual contact tracing, based on interviews by health care personnel to reconstruct infection chains, and digital tracing, through apps installed on smartphones exploiting network effects (i.e. the more users adopt the technology, the better the monitoring). While manual contact tracing has shown several limitations in terms of costs and efficacy,[3] digital contact tracing promised to complement the recollection of contact chains, potentially reducing contagion with limited resources (Barrat *et al.* 2020; Cencetti *et al.* 2021). In light of this enhanced capillarity in tracking people's movements, these applications have been employed extensively by both institutional actors (such as health authorities and governments but also local entities), and private ones (like companies for their employees or universities for their students) throughout the pandemic. However, their effectiveness is strictly dependent on the rate of adoption of the app, unsatisfactory in most voluntary contexts (Seto *et al.* 2021). A sizable refusal of digital tracing not only hinders its efficacy, but also signals citizens' distrust of public authorities when their privacy is at stake (Privacy International 2020a). In France, according to a poll on the national application

[3] It is time-consuming, costly and not always effective in tracking down people exposed to the virus. For instance, in February 2021, a manhunt of a hundred passengers from a London-Rome flight was conducted after one passenger had tested positive and local health authorities struggled to locate the passengers from the flight list (Pistilli 2021).

StopCovid carried out by the observatory Data Publica, 67% of interviewed people believe to be badly informed about the end-use of their personal data, and 54% do not trust the use of their data by the State (Cazzola 2020). The implications are twofold, supporting the need of adequate safeguards and warning against de facto mandatory uses.

Against this background, technology choices in digital surveillance change radically the risk of harming individuals. In this respect, we must distinguish between apps embracing Bluetooth technologies, which exploit proximity data, and solutions adopting Global Positioning System (GPS), which use location data. With systems based on proximity, devices placed within a few meters exchange Bluetooth Low Energy (BLE) signals that create an encrypted, random and temporary key code. In the case of positivity to Covid-19, the infected subject can update his status on the app and provide his consent to share his key, so that his contacts will receive an exposure notification. Conversely, geo-tracking works in real time by collecting people's coordinates: applications capture location data through GPS, share them with a centralized server and track movements as they occur. The former system has been adopted by most EU countries, while the latter is active, among others, in China, Israel and South Korea. Furthermore, and particularly in the case of proximity-based automated decision-making (ADM) systems, there are applications that adopt centralized data collection systems and others operating in a decentralized manner. In a centralized setting, health authorities have access to the chain of contagions and can better track the evolution of the pandemic, whereas opting for a decentralized solution allows for anonymity and more effective safeguard of privacy.

A further element to be considered when assessing the level of intrusiveness of mobile apps is whether they are made mandatory or voluntary. Voluntary use is a precondition for compliance with the EU legal framework. Conversely, official governmental apps are compulsory in countries such as South Korea where it is required for people entering the country (Joo and Shin 2020), and Russia, where it is mandatory only for individuals who tested positive (Dellanna 2020). Other countries, such as China, required individuals to download the app in order to move across cities (Seto, Challa and Ware 2021). In other instances, mandatory apps, such as the one adopted by the Qatari government, were violated by hackers, exposing sensitive data of more than one million users. A further con-

cern emerges about the risks of fragmentation and privatization of tracing caused by several initiatives promoted by companies and other private organizations that have developed their own tracing systems without the transparency protocols provided by official apps.

In the realm of the classification of technological solutions, biometric identification systems – allowing for the recognition of faces, gaits, fingerprints, voice, DNA and other biometric signals – warrant particular attention. The pandemic fostered the mainstreaming of such technologies as well. Facial recognition systems have been employed in several cities to monitor the enforcement of social distancing and other restrictions. In Russia, the pandemic has accelerated the process of installation of a network of 100,000 facial recognition cameras used to monitor people in quarantine (BBC N*ews* 2020). The pervasive use of such a tool emerged also within the EU. In France surveillance cameras help monitor whether people are adhering to social distancing or wearing masks (Vincent 2020). In Poland, a biometrics app allows authorities to check whether people who tested positive to the virus stay under quarantine (Privacy International 2020b).

Biometric systems are alarming from a privacy perspective insofar they enable real-time and *ex post* location tracking without individuals' consent. According to civil rights associations, their use infringes several human rights enshrined in the Charter of Fundamental Rights of the EU (hereafter, EU Charter) (EDRI, 2021). In this respect, grassroot campaigns such as 'Reclaim Your Face' are raising awareness calling for a ban of all types of biometric identification. The privacy risks embedded in biometric identification systems vary according to the identified feature. In the case of facial recognition, the use of surveillance tools to track individuals' location may lead to the wrong identification of people if the algorithm is not well trained but also to the identification of persons that did not give any consent to figure in a database. Finally, privacy may be impacted also in the case of voice recognition, as well as in the case of DNA-based identification systems.

2.2. Ethical considerations in times of algorithmic surveillance

The overview of the use of technology to manage the pandemic results in the key message that a simple characterization of an EU approach to Covid-19 digital surveillance as a sharp break from problematic inva-

sions of individual rights in the rest of the world may be far too simplistic. While the regulatory framework illustrated in the section to follow provides extensive guarantees, the pandemic has tested such boundaries both in the arena of government initiatives and especially in the uncontrolled proliferation of private and local tools.

Against this backdrop, the limitation of certain rights in the context of a public health emergency cannot *per se* be classified as problematic. On a purely legal account exceptions are explicitly foreseen. Reasonable limitations on certain rights, such as freedom of movement, right to peaceful assembly, right to personal liberty and right to privacy, are allowed in international human rights law when they are necessary to protect public health, as in the case of the Covid-19 pandemic (Human Rights Committee 2020). To limit the risk of arbitrary actions taken by the State and to protect the rule of law, any restriction must be consistent with the principles of legality, necessity, proportionality and non-discrimination. Namely, they must be limited in duration, geographical coverage and material scope, and any measures taken, including eventual sanctions, must be proportional in nature. In this context, the development of algorithmic surveillance technologies in compliance with such human rights standards could strengthen the effectiveness of global efforts to address the health crisis, as it would increase users' trust and the ability of such tools to support public health (Christou *et al*. 2020).

However, legal compliance alone does not guarantee a shield against algorithmic injustice. The AI ethics literature in this respect has highlighted the lack of consideration for a societal perspective in the broader discussion on algorithmic regulation. More specifically, it has been argued that the current debate fails to capture broader societal harms of AI (e.g. Smuha 2021). From such a perspective, the mainstream focus on assessing and regulating AI from an individual or at most collective right perspective leads to the underestimation of risks, for example, concerning "democracy, equality or the rule of law" (*ibidem*, 9).

While the use of invasive digital tools may be justified during a health crisis, it is worth considering whether in a long-term scenario, the asymmetry of power resulting from a *de facto* surveillance of citizens by private entities (as opposed to the State) may cause societal harm. Moreover, although human rights' concerns and ethical considerations related to public authorities' digital surveillance tools have been timely addressed

(WHO 2020; Ranish *et al.* 2020), major issues arise from the uncontrolled proliferation of similar technologies in the unregulated private ecosystem. While in adopting such solutions, the State is guided by public interests' goals (with ethical values embedded in constitutions and international human rights treaties), private actors follow their own interests, thus potentially taking advantage of contingency solutions to the detriment of society overall and vulnerable groups in particular.

A further concern covers the distributive implications of digital surveillance. Alike the pandemic itself and mitigation measures more in general, the widespread use of technology to support crisis management may result in unduly higher burdens for vulnerable groups. A special category of injustices in this domain relates to algorithmic discrimination, a challenge well-established within the literature ahead of the pandemic (e.g. O'Neil 2016), as AI may be biased or harmful for women, minorities, people with disabilities, or reveal the sensitive information of belonging to such vulnerable groups, for example in relation to gender identity (Fosch-Villaronga *et al.* 2021). Similar reasoning, in broader terms apply to socio-economic status, as mandatory use of certain tools may exclude those who do not have the skills or resources to access certain apps or platforms. As such, among the ethical weak points of pandemic digital surveillance there may be the further exacerbation of pre-existing inequalities reflected in heterogeneous impact of mitigation strategies. For example, the under consideration of needs of vulnerable groups such as people with disabilities in policies to contain the outbreak is well-documented (e.g. Goggin and Ellis 2020) extending to the two sided relation between technology as both an asset and a liability for inclusion. Additionally, as fruition of public and private services became increasingly digital, accessibility shortcomings become even more problematic for the inclusion of people with disabilities.

3. D*igital surveillance tools in the relevant* EU *legal framework*

The uncontrolled spreading of surveillance technologies has aggravated structural concerns which well-precede the health crisis, in relation to privacy and data protection, accessibility, equality and non-discrimination, with major risks for vulnerable groups at risk of social exclusion

(Sekalala *et al*. 2020; McGregor 2020). Digital technologies and apps have not only been using by public authorities to track the contagion curve, but also by private entities to avoid gatherings and regulate access to every day services. In this context, digital surveillance conditioned access to services and venues poses a high risk of exclusion for the population which may not have access to a smartphone or to a specific operating system. In this vein, such tools may be at the same time a powerful instrument for protecting public health and a dangerous source of discrimination and social exclusion.

Against this background, the EU legal framework provides an advanced protection to the fundamental rights of EU citizens, where data protection, equality and accessibility are well-established principles in the legal order. Nonetheless, the Union is now struggling to stay at pace with the new challenges posed by technological innovations, such as automatic decision-making systems also used in digital surveillance technologies.

3.1. Setting the scene of the EU relevant legal standards

First of all, the numerous digital surveillance and contact tracing tools developed in the wake of the pandemic must confront the comprehensive EU legislative framework on data privacy rights. More precisely, relevant provisions for digital surveillance tools can be inferred from the General Data Protection Regulation (hereafter GDPR, Regulation (EC) 2016/679) and the ePrivacy Directive (Directive 2002/58/EC). These address respectively personal data (Articles 6 and 9 GDPR), location data processed in an electronic communications network or by an electronic communication service (Articles 6 and 9 ePrivacy Directive) and data stored in and accessed from user's terminal equipment (Article 5 ePrivacy Directive) (Della Morte 2020a e 2020b; van Kolfschooten and de Ruijter 2020).

According to Article 5 GDPR, the processing of personal data must comply with the principles of lawfulness, fairness, and transparency, purpose limitation, data minimization, accuracy and keeping data up to date, storage limitation, integrity and confidentiality. More precisely, a distinction must be made whether the data involved in the processing of the digital surveillance tools belong to special categories, such as health data, or not (Bradford *et al*. 2020; Rugani 2020). Article 6 GDPR allows the

processing of data not included in special categories when this is necessary for the performance of a task in the public interest (Article 6(1)(e) GDPR). Article 9 permits the processing of health data (e.g., to monitor the health status of an infected individual) or biometric data (i.e. facial recognition) when required for reasons of public interest in the area of public health (Article 9(2)(i) GDPR), or for health care purposes (Article 9(2)(h) GDPR), or when necessary for scientific research purposes or statistical purposes (Article 9(2)(j) GDPR). Seemingly, the processing of data might also be based on explicit consent (Articles 6(1)(a) and 9(2)(a) GDPR). Nonetheless, the mere voluntariness of the contact tracing applications does not imply that there is valid consent, which depends on stricter requirements, *i.e.* this must be freely given, specific, informed and under an unambiguous indication of wishes (EDPB, 2020b).

The ePrivacy Directive, concerning the processing of personal data and the protection of privacy in the electronic communications sector, is relevant whereas contact tracing applications involve the storage or access to information stored in terminal equipment, in particular location data (Ventrella 2020). According to Articles 6 and 9, location data can only be transmitted to authorities or other third parties if they have been anonymized by the provider or, for data indicating the geographic position of the terminal equipment of a user, which is not traffic data, with the prior consent of the users. In addition, Article 5 imposes confidentiality of the communications collected directly from the terminal equipment. It allows access to the information stored only whether the user has given consent, or this access is strictly necessary for the information society service explicitly requested by the user. Re-use of location data collected for modelling purposes by the service provider can be further processed only with the additional consent of the user or based on legislative measures, a necessary and proportionate measure in a democratic society.

Another major issue refers to the accessibility of digital surveillance tools for users belonging to vulnerable groups at risk of social exclusion, such as persons with disabilities or older people. The 2006 United Nations Convention on the Rights of Persons with Disabilities (hereinafter, CRPD) lays down an international obligation to design accessible websites and to provide public information in accessible and usable online formats (Seaztu 2017; Charitakis 2018; Lawson 2018), also affirming its importance as a tool for participation and social inclusion (CRPD Com-

mittee 2014). As CRPD forms an integral part of the EU legal order (after the ratification of the CRPD by the EU in 2010: Waddington 2009; Ferri and Broderick 2020), the EU has recently developed several legal and policy initiatives addressing web accessibility (Waddington 2019).

Most notably, the Web Accessibility Directive (Directive 2016/2102/EU) establishes mandatory accessibility requirements for websites and mobile applications of public sector bodies, including contact tracing tools developed by public authorities. It also includes reference to the European standard EN 301 549 V2.1.2 (2018-08) (eHealth Network 2020), which has been recently amended in August 2021 by Decision (EU) 2021/1339. The latter, which has been developed by the three European Standardization Organizations (CEN, CENELEC and ETSI), is a merely voluntary standard so that it does not contain legally binding obligations. Nonetheless, it clarifies the functional accessibility requirements applicable to ICT products and services. In addition, this standard is in line with the most recent Web Content Accessibility Guidelines (WCAG 2.1.), developed by the World Wide Web Consortium (W3C),[4] which are internationally accepted as the primary standard by which accessibility should be measured.

Correspondingly, the European Accessibility Act (or EAA, Directive 2019/882/EU) regulates the accessibility requirements of key products and services in the internal market, such as, *inter alia*, mobile applications. This Directive establishes the legal basis for an obligation to comply with accessibility standard for contact tracing tools developed by private entities. However, it allows three years for its enforcement into the national laws of the Member States, meaning that the laws, regulations and administrative provisions necessary to comply with the Directive shall be adopted and published by the EU Member States by 28 June 2022 (Broderick 2019).

Finally, algorithmic surveillance systems are challenging the existing EU anti-discrimination legal framework. Equality and non-discrimination are basic fundamental values underpinning the EU legal order (Article 2 TEU) and permeate the entire legal framework. They are recognized as general principles of EU law (Tridimas 2006) and mentioned in vari-

[4] The World Wide Web Consortium (W3C) is an international consortium where member organizations, full-time staff, and the public work in tandem to pursue the accessibility of the Internet (https://www.w3.org/Consortium/).

ous provisions of the EU Treaties and the EU Charter, but also inspire a set of antidiscrimination directives, adopted after the adoption of the Amsterdam Treaty in 1999.[5]

Nonetheless, contact tracing systems are posing new and enhanced risks of inequalities and social exclusion. Also in this arena, issues relating to digital inclusions and the digital divide well precede the pandemic. From such a perspective, extensive effort has been devoted at the EU level in the context of the Digital Agenda for Europe to universal broadband access, whose success has even led to the claim of having bridged the digital divide (European Commission 2021). Nevertheless, broadband coverage and other barriers linked to socioeconomic background remain highly relevant. The acceleration of digitalization and online access to fundamental services including eHealth, education and teleworking has paralleled lockdowns and the pandemic containment effort. As digital technologies became a fundamental tool for inclusions in times of social distance, they are at the same time the culprit of an increasing digital divide especially among vulnerable groups (Shah *et al*. 2020; Campos-Castillo and Anthony 2021; Giansanti and Veltro 2021; Lai and Widmar 2021). ADM systems, as those used in contact tracing tools, are producing new forms of (algorithmic) discrimination (Hacker 2018; Xenidis and Senden 2020; Zuiderveen Borgesius 2020; Wachter *et al*. 2021). Not only algorithmic profiling reproduces and amplifies intersectional forms of discrimination, but also contributes to creating new patterns of discrimination (Xenidis 2020).

3.2. The European approach to contact tracing and digital surveillance

In such a context, the massive use of algorithmic surveillance to combat the spread of Covid-19 raised major concerns among the EU institutions, which at the very beginning of the pandemic offered a guidance to Member

[5] These are Directive 2000/43/EC, Directive 2000/78/EC, Directive 2006/54/EC and Directive 2004/113/EC). A Directive Proposal offering more symmetric protection is also pending since 2008 (Proposal for a Council Directive on implementing the principle of equal treatment between persons irrespective of religion or belief, disability, age or sexual orientation COM/2008/0426 final).

States to develop official contact tracing apps respecting the fundamental rights of EU citizens. In April 2020, the European Commission issued a common Union toolbox (Commission Recommendation (EU) 2020/518) and a Guidance on contact tracing apps concerning data protection (Commission Communication 2020/C 124 I/01). These documents recommend the exclusive use of voluntary apps, namely apps downloaded, installed and used on a voluntary basis by individuals and with opt-out options available. This position has been confirmed by the eHealth Network (eHealth Network 2020) and by the EDPB, which recalls that the general principles of effectiveness, necessity, and proportionality must be taken into account for any measure involving the processing of personal data (EDPB, 2020a). More precisely, contact tracing applications must respect the proportionality of the measure in terms of duration and scope, limited data retention, data minimization, data deletion, purpose limitation and genuine anonymization of data (Ponce 2020). In the same vein, national authorities, or entities carrying out a task in the public interest in the field of health, are required to act as data controllers to ensure the principle of accountability. Accordingly, Data Protection Authorities must be consulted in the context of the development of the applications.

Moreover, the EU Toolbox also addresses the importance of ensuring the compliance of contact tracing tools with accessibility standards. This document lists the relevant parameters to enable a coordinated development and use of officially recognized contact tracing applications, with the purpose to develop a common EU approach to support the gradual lifting of confinement measures (eHealth Network 2020). In this line, the digital accessibility of the contact tracing applications is referred to as a means to reach inclusiveness from both a human rights and an effectiveness perspective.

However, to date, there is a substantial difference among public and private digital surveillance tools in the EU legal order. The fragmented context of Covid-related surveillance tools far exceeds official contact tracing apps. Firstly, beyond national apps, several other initiatives have been launched for specific purposes. In some instances, local proliferation parallels a decentralized health system in which regions often develop their own initiatives. In this context, these multiple tools while remaining in the public domain do not necessarily attract the same attention, scrutiny and accountability processes of national contact-trac-

ing apps regarding data protection. Moreover, only contact tracing applications of public sector bodies must comply with accessibility standards. Namely, the content of public surveillance apps should meet the accessibility requirements set out in the transposition legislation of the Web Accessibility Directive. On the contrary, the same accessibility duty is not directly applicable for private tracing tools, as the implementation period of the European Accessibility Act has not yet expired.

Concomitantly, other relevant issues, such as the extensive use of biometric identification systems, including recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioral signals, has not been addressed by the European Commission and still remain without response in the EU legal and policy framework. Nonetheless, these technologies challenging the data privacy rights of EU citizens, as they enable real-time and ex post location tracking without individuals' consent. The European Data Protection Board, the European Data Protection Supervisor (EDPB 2021) and the European Parliament (EPRS 2021) called for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces.

3.3. A way forward with the new European Commission Proposal for an AI Regulation?

As illustrated above, the existing EU legal framework tackles some of the risks posed by the unrestrained use of automated decision-making systems in the pandemic context and beyond. In this respect, the EU has always adopted a paternalistic approach, opting for command-and-control regulation vis-à-vis more lenient attitudes. In doing so, the EU aims to become the leader in establishing a clear legal environment based on the protection of fundamental rights, a rationale that lies behind the recent proposal for an AI Act.

Beyond and preceding the ongoing legislative process for an AI Act, paralleled by the 2020 White Paper on AI (European Commission 2020), a strategy for Artificial Intelligence was already presented in 2018 (European Commission 2018). The plan highlighted the need for an EU framework capable of fostering technological benefits while ensuring compliance with the Union's values, including the protection of citizens from emerging ethical and legal challenges. The approach meant to balance the objective of

competitively leading in AI with leaving no one behind, thus balancing the need for safe products while protecting individuals' rights.

The AI Act was put forward in April 2021 by the European Commission and it aims to be the first horizontal and binding legal instrument harmonizing the European approach to the development and use of AI. In light of the heterogeneous nature of AI applications, in approaching the regulation of AI, a multi-tiered risk-based approach was adopted: under such framework, AI systems are classified into different categories of risk, from those posing an unacceptable risk (which are prohibited under EU law) to high-risks systems (allowed but subject to specific requirements) and minimal-risk systems (subject to transparency obligations). The adoption of a risk management system had been encouraged by a plethora of institutions, from the OECD to the IEEE, and governments (e.g. US, Canada and Singapore). The rationale of such an intervention stems from proportionality considerations, that is only harmful AI applications should be regulated, as well as from the need to avoid a one-size-fits-all measure.

The Commission opted for a prescriptive rather than procedural guidance, prohibiting in Article 5 AI systems that bring about unacceptable risks, namely those a) deploying subliminal techniques and/or b) exploiting vulnerabilities of a specific group of people due to age or disability to distort behaviour or cause physical or psychological harm, and c) classifying the trustworthiness of people based on social behaviour or personality characteristics leading to discriminatory treatment. The same article prohibits the deployment of real-time biometric identification in public spaces for law enforcement - with three exceptions, i.e. in case of missing children, prevention of terrorism, and detection, identification and localization of a suspect.

In the same vein, the AI Act refers to high-risk systems as those implying health or safety risks or adverse impacts on fundamental rights in certain areas. Applications such as remote biometric systems (e.g. public security cameras) figure in this category, regardless of whether they work in real-time or use previously collected images or video. High-risk applications belong to the following areas: i) biometric identification and categorization of natural persons; ii) management and operation of critical infrastructure; iii) education and vocational training; iv) employment, workers management and access to self-employment; v) access to and enjoyment of essential private services and public services and benefits;

vi) law enforcement; vii) migration, asylum and border control management; viii) administration of justice. These systems are permitted but are subject to certain essential requirements. For instance, providers of AI must carry out a conformity assessment and design a risk management system, ensuring high-quality of datasets and accuracy of their model.

Although in theory this holistic approach to the regulation of algorithms could usher in an ecosystem of accountability and transparency, some aspects of the proposal leave ample room for improvement, especially with respect to those AI systems that raise the most concern, namely biometric identification systems. More specifically, the proposal bans only some of their uses by law enforcement in real-time and in publicly accessible spaces. This automatically exempts remote biometric recognition, which is widely used, for instance, to identify ex-post people participating to protests (EDPB 2021). Another shortcoming of the proposal is the exclusion of "live" online biometric identification, as online spaces fall outside the scope of the proposed regulation (Veale and Zuiderven Borgesius 2021). Furthermore, in the Covid-19 context, biometric identification systems used for contact tracing ought to be considered as high-risk. However, as pointed out in the preamble of the act, under exceptional reasons of public security or protection of health, a conformity assessment could be avoided. Hence, tools used in extraordinary events such as the pandemic could be expected to be exempted from such obligations, resulting in potential infringements of the high-quality standards required under Title III of the proposal. At the same time biometric systems used for categorization purposes would be classified as low-risk systems, thus only subject to transparency obligations.

Finally, several commentators have emphasized that such a distinction between biometric identification systems as high-risk and biometric categorization systems as low-risk is flawed, because many of the current categorization systems posing high-risks of discrimination would be exempted from stricter requirements (Malgieri and Ienca 2021). In sum, despite the ambition of setting a new gold standard for regulating algorithmic surveillance, AI Act in its current form addressed only partially the inherent risks of invasive technologies such as face recognition and other biometric systems, which have been adopted extensively during the pandemic. The legal ambiguities of some of the definitions included in the proposal, together with the limited ban on certain practices that are widely recognized as harmful for vulnerable groups, hamper the ef-

fectiveness of the scope of the provision. To overcome these limitations, the political actors involved in the next stages of the policy process would need to strengthen the proposed safeguards extending the requirements to the remaining biometric systems that are currently outside the scope of the provision or only subject to information requirements.

4. P*andemic digital surveillance in practice: a survey of problematic tools within the* EU

The current and prospective legal framework with the AI Act Proposal has already pinpointed theoretical strength and weaknesses in the context of the pandemic. As illustrated, beyond the realm of official contact tracing apps, substantial gaps have been outlined, at times especially in the private domain as in the case of accessibility. Against such backdrop, the multiplication of a variety of tools directly addressing the mitigation of contagion or indirectly supporting mitigation measures provides for a variety of cases potentially infringing specific individual or collective right, as well as posing general societal challenges, for instance to equality. The question addressed within this survey, in evidencing the argument of non-negligible algorithmic injustices at the hand of pandemic surveillance in the EU, is whether challenges to privacy, accessibility, non-discrimination and inclusion emerge in practice. Short of untenable comprehensive mapping of unofficial Covid-19 related apps and digital tools – many of which may not be publicly disclosed – this section provides problematic examples refuting the claim of the EU as a safe haven from invasive pandemic surveillance even in the absence of coordinated government mass surveillance.

The analysis avoids overtly technical assessment of compliance with standards. Rather it focuses on (i) instances in which the implied anonymity is blatantly violated by the choice of technology or the app or service request for access to identifying information, (ii) likewise evident problems in accessibility and/or reported issues from interest groups of people with disability and (iii) technology type (e.g. facial recognition), restriction to specific ecosystems (e.g. iOS) or preferential access through apps inherently problematic for digital inclusion and discrimination. In doing so it shows how the risk for algorithmic injustice may loom quite at the surface of the European fragmented and largely unregulated ocean of pandemic digital tools.

4.1. Privacy

Two levels of concern emerge in the realm of privacy. On one side, we highlight instances in which tools violate in practice the presumption of anonymity or employ technology outside of the EU approach (e.g. location data). On the other, we indicate use-cases which are not fully voluntary (e.g. conditioning access to workplaces or education) hence inherently not complying with freely given consent. A final concern emerges in the duplication of tracing efforts in the private and public subnational domains, which do not fall under the extensive transparency, accountability and scrutiny devoted to the official ones at the country level. Examples abound on all accounts.

WhatsApp bots and services linked to users' phone numbers include the Croatian Andrija digital assistant[6], a discontinued AI powered health self-assessment tool developed by the private sector and deployed by the government. Another discontinued public tool[7] in Estonia likewise implies anonymity of the online self-assessment questionnaire while it records the IP address of the users. A German private app – Coronika - Your Corona Diary[8] – goes as far as importing contacts and saving locations readily shareable with public health authorities, hence implying a far more invasive tracing and potential for exposing sensitive information of third parties. Finally, in Spain the private comprehensive Mediktor[9] app, which includes a Covid symptom self-assessment, asks for access to the user location albeit implying anonymity and expands beyond the symptoms and risk factors questions to include previous disease and vaccination status. Additionally, problematic technologies include the extensive use of biometric data, which in the context of facial recognition in physical spaces implies consent-free real tracking of citizens exact location. Arguably the most controversial instance in the EU landscape pertains to a government initiative in Poland, Kwarantanna domowa,[10]

[6] Andrija digital assistant (https://andrija.ai/).

[7] Koroonaviirustest (https://mhealth-hub.org/coronatest).

[8] Coronika (https://www.coronika.app/).

[9] Mediktor (https://www.mediktor.com/en).

[10] Privacy International. Poland: App helps police monitor home quarantine (https://privacyinternational.org/examples/3473/poland-app-helps-police-monitor-home-quarantine).

a mandatory app requiring people under quarantine to respond with a selfie within 20 minutes of an unscheduled notification, using both facial recognition and location data. Other examples in the public domain include the use of facial recognition enabled CCTV in France to monitor masking compliance,[11] controversial and claimed to be illegal by privacy interest groups.[12] Along the same line, biometric enforcement of quarantines through drone has been blocked by the judiciary in France,[13] which was, however, successfully deployed in Greece.[14] Moreover, biometric infringements on privacy are not contained to physical spaces. An example is the use of facial recognition for monitoring remote educational and work activities. Notably, technology-driven monitoring of employees and data-driven management allows firms to maintain and strengthen their control over workers both in a work-from-home setting and on-site. Workers who kept their in-person occupations were required to install softwares or applications proving their Covid-free health status, but also to wear biometric devices such as ultrasonic bracelets beeping in case of a virus catching proximity between blue-collars (Aloisi and De Stefano 2021). Concomitantly, universities and other education institutions adopted AI-enabled tools to monitor students during exams from home, collecting tons of personal information.[15] In Italy, a university deployment of digital proctoring software for virtual exams was recently fined

---

[11] Mathieu Pollet, "France to use CCTV to monitor mask-wearing on public transport", E*uractive*, 16 March 2021 (https://www.euractiv.com/section/data-protection/news/france-to-use-cctv-to-monitor-mask-wearing-on-public-transport/).

[12] 'Le Sénat doit s'opposer à la reconnaissance faciale des masques", L*a Quadrature du Net*, 15 March 2021 (https://www.laquadrature.net/2021/03/15/le-senat-doit-sopposer-a-la-reconnaissance-faciale-des-masques/; https://www.laquadrature.net/2021/03/15/le-senat-doit- sopposer-a-la-reconnaissance-faciale-des-masques).

[13] La Quadrature du Net, "France: First victory against police drones", EDRI, 27 May 2020 (https://edri.org/our-work/france-first-victory-against-police-drones/).

[14] Homo Digitalis, "Covid-Tech: Covid-19 opens the way for the use of police drones in Greece", EDRI, 24 June 2020 (https://edri.org/our-work/covid-tech-covid-19-opens-the-way-for-the-use-of-police- drones-in-greece/).

[15] "Universities are using surveillance software to spy on students", W*ired* UK, 15 October 2020 (https://www.wired.co.uk/article/university-covid-learning-student-monitoring (accessed: 2 October 2021)).

by the DPA in relation to tools which have been widespread in assisting online monitoring across numerous institutions.[16] The tools were needed to help professors supervise written tests and are used by many other campuses. In the judgement it is stressed that such systems must not be unduly invasive and involve monitoring of the student in excess of actual needs.[17] The decision points out that the university failed to properly inform students not mentioning the photograph taken by the system at the beginning of the test nor the retention periods for personal data, which was being transferred to the United States. In other words, according to the DPA, the consent provided by the student at the beginning of the exam was not a sufficient condition processing biometric data.

Moving onto the fragmentation and duplication of public and private tracing services and eHealth apps, examples proliferate across several Member States. In Austria, the city of Vienna deployed its own symptom homecare app[18]. In Belgium, private services for triage, home-monitoring and access to testing abound, including the Moveup.care[19], Bingli[20] and the Andaman7[21] app. In France public hospitals in Paris[22] and Marseille[23] have developed apps to track patients and individuals at risk of exposure. In Italy several regional authorities have

---

[16] "Maxi multa di 200mila euro alla Bocconi per gli esami con il 'riconoscimento facciale'", *MilanoToday*, 28 September 2021 (https://www.milanotoday.it/attualita/multa-bocconi-esami-privacy.html).

[17] Garante Privacy, *Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano - 16 settembre* 2021 [9703988] (https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9703988 (accessed: 2 October 2021)).

[18] Homecare app (https://futurezone.at/apps/coronavirus-stadt-wien-ueberwacht-heimquarantaene-per-app/400780490).

[19] Moveup.care (https://futurezone.at/apps/coronavirus-stadt-wien-ueberwacht-heimquarantaene-per-app/400780490).

[20] Bingli (https://chat.mybingli.com/#/covid).

[21] Adaman7 (https://www.andaman7.com/en/covid-19).

[22] Covidom (https://www.aphp.fr/actualite/application-covidom-mise-disposition-gratuitement-pour-lensemble-des-medecins-et-les).

[23] Covid ap HM (http://fr.ap-hm.fr/actu/covid-aphm-l-intelligence-numerique-au-service-des-patients-covid-19-de-l-aphm).

deployed their own app to track travelers, such as the Sicilia Si Cura[24] app, or self-assessment questionnaires such as the Cerca Covid[25] app in Lombardy or the HCasa app of the Puglia region, which extends into a fully-fledged telemedicine tool.[26] In some countries, such as in Italy, local initiatives have already received warnings from privacy oversight authorities for violation of the current regulatory framework.[27]

Some of the previous examples of apps mandating registration of travellers already land in the realm of non-voluntary tools. In this arena two use-case, which carry important implications beyond the domain of consent and privacy, emerge: universities and workplaces policing of access to physical spaces. Universities, which at times publicly disclose their digital mitigation procedures, evidence potential abuses in both domains through invasive tracing tools forced onto students and employees. They may involve a combination of digital contact tracing and self-assessment questionnaires required for in-person activities. University College of Cork in Ireland employs the UCC Covid Tracker and Day Pass App[28] for students and staff. Similarly, the IE University in Spain has developed the Covid-19 Tracer app[29] imposing daily completion of a health questionnaire, which the health protocol available online[30] indicates a prerequisite for the "Health Passport" greenlighting access to campus.

---

[24] Sicilia Si Cura https://www.ansa.it/sicilia/notizie/sanita_sicilia/2020/03/28/coronavirus-sicilia-si-cura-app-monitorare-asintomatici_e109bae4-424c-4a10-9a8a-f96897b8dd5a.html

[25] Cerca Covid (https://www.openinnovation.regione.lombardia.it/b/572/regioneaicittadiniunapppermonitorareladiffusionedelcovid).

[26] Hcasa (https://www.openinnovation.regione.lombardia.it/b/572/regioneaicittadiniunapppermonitorareladiffusionedelcovid).

[27] Garante della privacy (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9590434).

[28] UCC Covid Tracker and Day Pass App (https://www.ucc.ie/en/emt/covid19/ucc-covid-app/).

[29] Covid-19 Tracer (https://it.ie.edu/news/detail/COVID-19-Tracer).

[30] IE university. Health Protocol for Accessing IE University. (https://docs.ie.edu/weareready/07-Health-Protocol.pdf).

4.2. Accessibility, inclusion and discrimination

As apps multiply, potentially even precluding in-person access to education services and workplaces, concerns expand over the risk of exclusion. Any service requiring an app or other digital tool to obtain access is especially problematic as the older demographic may overwhelmingly not own smartphones (Gasser *et al*. 2020). The same applies to economic barriers affecting the digital divide (e.g. smartphone or broadband ownership). Beyond tout-court exclusion, cumbersome and slower alternatives may imply delays in accessing certain services, as crucial as vaccination enrolment discriminating against users unable to book electronically quickly saturated slots, for example, becoming available online at midnight. Additionally, discrimination may occur as a result of inherently problematic technologies, such as facial recognition which the previous section evidenced used by several public and private surveillance tools.

A further and especially delicate arena is that of accessibility. Fragmentation returns as a particularly problematic aspect. Firstly, the proliferation of private applications excludes the legal obligation for accessibility which so far only applies to public services. Such a voluntary feature, generally well-advertised by apps as an element of pride, is overwhelmingly not mentioned by many of the apps surveyed here. Additionally, even in the public arena, scrutiny is relevant also for the domain of accessibility. While the spotlight of interest groups monitors official apps, such screening becomes less feasible when facing the plethora of public digital tools multiplying across specialized policy domains and the regional and local level. Nevertheless, even as only a single usability study has been carried out for official digital contact tracing tools within the EU (Bente *et al*., 2021), even some of such apps have attracted accessibility complaints. In Italy the institute for assistive technology INVAT has identified several concerns for the Immuni app (INVAT 2020). Likewise, the Spanish app RadarCOVID has been deemed unfit for the needs of the blind community (E*uronews* 2020). The emerging picture is hence far from unproblematic from an accessibility standpoint, as even the benchmark official app initiatives at time failed to reach the mandated standard.

5. *Conclusions*

The pandemic has exponentially accelerated digitalisation and the mainstreaming of AI based tools, in a context of higher acceptability of compression of individual rights justified by crisis management under a public health emergency. The analysis of the constraints imposed by the relevant EU legal framework highlights its advanced protection in comparison to less consumer-centric regulatory environments. At the same time, the findings show far from minor gaps allowing for numerous and highly problematic use-cases to proliferate. Moreover, the theoretical and empirical assessment indicates how the sole focus on privacy fails to capture the complex and diverse risks of algorithmic injustices operating in the context of pandemic digital surveillance. Conversely, under the umbrella of a broader human-rights-oriented-approach, the analysis signalled the implications of shortcomings in the legal framework in relation to non-discrimination and inclusion. Against this framework, findings support the core argument that while the EU may comparatively represent a best practice, existing protections against algorithmic injustices are insufficient faced with the high tide of the explosion of algorithmic injustices, especially in an emergency context such as the pandemic. Additionally, the evaluation of the current proposal for an AI Act by the European Commission shows that the adoption of a risk-based approach could indeed tackle some of the challenges posed by AI applications for concerning use case (e.g. systems used to manipulate vulnerable people). However, as it stands, the proposal fails to adequately regulate biometric identification systems, which have been heavily employed in the pandemic context.

Conversely, we show that pandemic digital surveillance aggravated pre-existing inequalities. The datafication of society, which relies on the ubiquitous collection of personal information, coupled with the augmentation of surveillance powers by public authorities and private organizations, have led to a massive use of AI-enabled tools to track the evolution of contagion and monitor the enforcement of restrictive measures. Although digital contact tracing may be a powerful tool for the protection of public health thanks to its cost-effectiveness and capillarity, it may as well entail risks in terms of privacy, accessibility and discrimination, thus resulting in further social exclusion. In particular, biometric identification systems and mobile applications used at the

local level and by private entities have opaque features that do not always ensure the protection of fundamental rights. In such a context, voluntary and highly scrutinised official contact tracing apps differ in light of the extensive protection and proportional and minimised intrusion into user lives and rights. While imperfect, as evidenced, for example, by shortcomings in the Italian and Spanish app in term of accessibility, such pandemic digital management tools may arguably be well-justified against the challenge of protecting public health in an emergency. Conversely, blatant violations of voluntary use and privacy friendly technologies such as the Polish quarantine app can hardly fall within the same category. Similarly, we showed empirically a broad array of problematic use-cases in the biometric realm, encompassing tools such as CCTV and likewise *de facto* mandatory submission to digital surveillance for accessing universities and workplaces.

Against this backdrop, the EU comparatively devotes a high priority within its regulatory framework to the protection of citizens from infringements of their right to privacy, equality and accessibility. Nonetheless, owing to the uncontrolled proliferation of such pervasive technologies, which often rely on ADM systems, it may struggle to keep the pace and may lag behind in protecting individuals from subtle abuses. Results hence support the urgent need of further regulating against algorithmic injustices, as purported by the AI Act proposal, following a human (rights) centred and risk-based approach. Therefore, it is of the utmost importance that the new regulatory regime, which already employs a tailored risk-based approach, does not underestimate the extent of the problems of fragmentation, proliferation and augmentation of contact tracing solutions and other tools for digital surveillance. The proposed Regulation takes positive steps in such direction, for example, in recommending in Recital 81 voluntary additional requirements, such as accessibility and the participation of stakeholders, in the design and development of AI systems which may foster a human rights-oriented approach to artificial intelligence. At the same time, the ambition of the AI Act proposal may prove insufficient if adequate safeguards on a reckless use of biometric identification and categorization systems used by private actors are not adopted.

In concluding, our analysis evidences how the commitment to privacy through use of proximity-based apps rather than location-based ones, the

recourse to decentralized architecture and voluntary use of official digital contact tracing apps do not alone guarantee against problematic tools emerging in the fissured ecosystem and hence algorithmic injustices. The theoretical and empirical assessment of the case of pandemic digital surveillance against the EU legal framework contributes to the literature on AI ethics, EU digital policies, and their implication for human rights. Specifically, the analysis constitutes a warning against dismissing concerns over ethical and human rights challenge on the basis of the false reassurance of a comparatively advanced and protective legal framework. Conversely, we also show how proposed solutions such as the AI Act may prove insufficient against the gaps and shortcomings evidenced by the case of pandemic surveillance, of high relevance and timeliness for the unfolding policy debate over the future regulation of artificial intelligence in the EU.

References

Aloisi A., De Stefano V. (2021), "Essential Jobs, Remote Work and Digital Surveillance: Addressing the Covid-19 Pandemic Panopticon", *International Labour Review*, p. ilr.12219. doi:10.1111/ilr.12219.

Barocas S., Selbst A.D. (2016), "Big Data's Disparate Impact", *California Law Review*, vol. 104, p. 671.

Barrat A., Cattuto C., Kivelä M., Lehmann S., Saramäki J. (2020) "Effect of Manual and Digital Contact Tracing on Covid-19 Outbreaks: A Study on Empirical Contact Data", *medRxiv*, p. 2020.07.24.20159947, doi: 10.1101/2020.07.24.20159947.

BBC News (2020), "Russia Uses Facial Recognition to Tackle Virus", 4 April. https://www.bbc.com/news/av/world-europe-52157131 (accessed: 30 June 2021).

Bente B.E., Van 't Klooster J., Schreijer M.A., Berkemeier L., van Gend J.E., Slijkhuis P.J.H., Kelders S.M.,van Gemert-Pijnen L. (2021), "The Dutch Covid-19 Contact Tracing App (the CoronaMelder): Usability Study", JMIR *Formative Research*, vol. 5, n. 3, p. e27882, doi: 10.2196/27882.

Bradford L., Aboy M., Liddell K. (2020), "Covid-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes", *Journal of Law and the Biosciences*, vol. 7, n. 1, pp. 1-21.

Broderick A. (2019), "The European Accessibility Act: A Paradigm of Inclusive Digital Equality for Persons with Disabilities?", in C. Ricci (ed.), *Building an Inclusive Digital Society for Persons with Disabilities New Challenges and Future Potentials*, Pavia, Pavia University Press, 2019, pp. 19-38.

Campos-Castillo C., Anthony D. (2021), "Racial and Ethnic Differences in Self-reported Telehealth Use During the Covid-19 Pandemic: A Secondary Analysis of a US Survey of Internet Users from Late March", *Journal of the American Medical Informatics Association*, vol. 28, n. 1, pp. 119-125, doi: 10.1093/jamia/ocaa221.

Cazzola F. (2020), "StopCovid: une majorité de Français inquiets de l'utilisation de leurs données par l'application", *France Bleu*, https://www.francebleu.fr/infos/politique/sondage-stop-covid-une-majorite-de-francais-inquiets-de-l-utilisation-de-leurs-donnees-par-l-1589445489 (accessed: 19 June 2020).

Cencetti G., SantinG., Longa A., Pigani E., Barrat A., Cattuto C., Lehmann S., Salathé M., Lepri B. (2021), "Digital Proximity Tracing on Empirical Contact Networks for Pandemic Control", *Nature Communications*, vol. 12, n. 1, p. 1655, doi: 10.1038/s41467-021-21809-w.

Charitakis S. (2018), *Access Denied: The Role of the European Union in Ensuring Accessibility under the United Nations Convention on the Rights of Persons with Disabilities*, Maastricht, Intersentia.

Christou T.A., Sacco M.P., Bana A. (2020), *Digital Contact Tracing for the Covid-19 Epidemic*: A *Business and Human Rights Perspective*, International Bar Association's Report, June 2020.

Commission Implementing Decision (EU) 2018/2048 *of* 20 *December* 2018 *on the Harmonised Standard for Websites and Mobile Applications in Support of Directive* (EU) 2016/2102 *of the European Parliament and of the Council*, 2018, OJ L 327, p. 84-86, https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32018D2048

Commission Recommendation (EU) 2020/518 *of* 8 *April* 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* (2020), C/2020/3300, OJ L 114, 14.4.2020

Communication from the Commission Guidance on Apps Supporting the Fight Against Covid-19 Pandemic in Relation to Data Protection (2020), C 124 I/01, C/2020/2523, OJ C 124I, 17 April 2020.

Convention of the Rights of Persons with Disabilities,2006, opened for signature 13 December 2006, 2515 UNTS 3 (entered into force 3 May 2008)

CRPD Committee (2014), *General comment No. 2, Article 9: accessibility*, CRPD/C/GC/5.

Deaton, A. (2021), *Covid-19 and Global Income Inequality*, Working Paper 28392. National Bureau of Economic Research, doi:10.3386/w28392.

Della Morte G. (2020a), "La tempesta perfetta. Covid-19, deroghe alla protezione dei dati personali ed esigenze sorveglianza di massa", SIDI*blog*, 30 March [accessed 29 June 2021], http://www.sidiblog.org/2020/03/30/la-tempesta-perfetta-covid-19-deroghe-alla-protezione-dei-dati-personali-ed-esigenze-di-sorveglianza-di-massa/.

– (2020b), "Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano", *Diritti umani e diritto internazionale*, vol. 14, n. 2, pp. 303-335.

Dellanna, A. (2020), "Russia's Tracking App Sparks Fury After Mistakenly Fining Users", *Euronews*, https://www.euronews.com/2020/06/02/coronavirus-russia-s-tracking-app-sparks-fury-after-mistakenly-fining-users (accessed: 30 June 2021).

Directive (EU) 2016/2102 *of the European Parliament and of the Council of* 26 *October* 2016 *on the accessibility of the websites and mobile applications of public sector bodies* (*Text with* EEA *relevance*), 2016, OJ L 327, 2.12.2016, pp. 1-15, https://eur-lex.europa.eu/eli/dir/2016/2102/oj.

Directive (EU) 2019/882 *of the European Parliament and of the Council of* 17 *April* 2019 *on the accessibility requirements for products and services* (*European Accessibility Act*), 2019, OJ L 151, p. 70-115, https://eur-lex.europa.eu/eli/dir/2019/882/oj.

Directive 2002/58/EC *of the European Parliament and of the Council of* 12 *July* 2002 *concerning the processing of personal data and the protection of privacy in the electronic communications sector* (*Directive on privacy and electronic communications*), 2002, OJ L 201, 31.07.2002.

EDPB (2020a) *Guidelines* 04/2020 *on the Use of Location Data and Contact Tracing Tools in the Context of the Covid-19 Outbreak*, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

– (2020b), *Guidelines* 05/2020 *on Consent Under Regulation* 2016/679, *Version* 1.1, 4 May, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (accessed: 29 June 2021).

– (2021), EDPB & EDPS *Call for Ban on Use of* AI *for Automated Recognition of Human Features in Publicly Accessible Spaces, and Some Other Uses of* AI *That Can Lead to Unfair Discrimination*, 21 June, https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-humanfeatures- publicly-accessible_en (accessed: 22 September 2021).

EDRI (2021), "Ban Biometric Mass Surveillance!", *European Digital Rights* (EDRI), https://edri.org/our-work/blog-ban-biometric-mass-surveillance/ (accessed: 30 June 2021).

eHealth Network (2020), *Mobile Applications to Support Contact Tracing in the EU's Fight Against Covid-19 Common* EU *Toolbox for Member States*, *Version* 1.0, 15 April, https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-19_apps_en.pdf [accessed: 29 June 2021].

EPRS (2021), *Regulating Facial Recognition in the* EU, PE 698.021-September.

Euronews (2020), *Flaws in Spain's Covid-tracking App 'Are Exposing Blind People to Virus'*, https://www.euronews.com/2020/09/08/flaws-in-spain-s-covid-tracking-app-are-exposing-blind-people-to-virus- (accessed: 30 June 2021).

European Commission (2018) *Communication Artificial Intelligence for Europe*, https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe (accessed: 2 June 2020).

– (2020), *White Paper on Artificial Intelligence: a European Approach to Excellence and Trust*, https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en (accessed: 13 March 2020).

– (2021a), *Europe Closes the Digital Divide*, https://digital-strategy.ec.europa.eu/en/news/europe-closes-digital-divide (accessed: 30 June 2021).

– (2021b), *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*).

European Parliament. Directorate General for External Policies of the Union (2021), *Digital Technologies as a Means of Repression and Social Control*, https://data.europa.eu/doi/10.2861/953192 (accessed: 30 June 2021).

Ferri D., Broderick A. (2020, eds), *Research Handbook on* EU *Disability Law*, Cheltenham, Edward Elgar.

Fosch-Villaronga E., Poulsen A., Søraa R.A., Custers B.H.M. (2021), "A Little Bird Told Me Your Gender: Gender Inferences in Social Media", *Information Processing & Management*, vol. 58, n. 3, p. 102541, doi:10.1016/j.ipm.2021.102541.

Gasser U. *et al.* (2020), "Digital Tools Against Covid-19: Taxonomy, Ethical Challenges, and Navigation Aid", *The Lancet Digital Health*, vol. 2, n. 8, pp. e425–e434, doi: 10.1016/S2589-7500(20)30137-0.

Giansanti D., Veltro G. (2021), 'The Digital Divide in the Era of Covid-19: An Investigation into an Important Obstacle to the Access to the mHealth by the Citizen", *Healthcare*, vol. 9, n. 4, p. 371, doi: 10.3390/healthcare9040371.

Goggin G., Ellis K. (2020), "Disability, Communication, and Life Itself in the Covid-19 Pandemic", *Health Sociology Review*, vol. 29, n. 2, p. 168.

Hacker P. (2018), "Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law", *Common Market Law Review*, vol. 55, n. 4, pp. 1143.-1186.

Human Rights Committee (2020), *Statement on Derogations from the Covenant in Connection With the Covid-19 Pandemic*, 30 April 2020, CCPR/C/128/2.

INVAT (2020), https://www.invat.info/news/16/ICT-news-0620#art2 (accessed: 30 June 2021).

Joo J., Shin M.M. (2020), "Resolving the Tension Between Full Utilization of Contact-tracing App Services and User Stress as an Effort to Control the Covid-19 Pandemic", *Service Business*, vol. 14, n. 4, pp. 461-478, doi: 10.1007/s11628-020-00424-7.

Lai J. and Widmar N.O. (2021), "Revisiting the Digital Divide in the Covid-19 Era", *Applied Economic Perspectives and Policy*, vol. 43, n. 1, pp. 458-464.

Lawson A.M. (2018), "Article 9: Accessibility", in I. Bantekas, M.A. Stein, D. Anastasiou (eds), *The Convention on the Rights of Persons with Disabilities*: A *Commentary*, Oxford, Oxford University Press, 2018, pp. 258-286.

Malgieri, G., Ienca, M. (2021) 'The EU Regulates AI But Forgets to Protect Our Mind', E*uropean Law Blog*, 7 July, https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/ (accessed: 26 November 2021).

McGregor L. (2020), "Contact-tracing Apps and Human Rights", EJIL:*Talk*!, 30 April, https://www.ejiltalk.org (accessed: 29 November 2021).

O'Neil C. (2016), W*eapons of Math Destruction*: H*ow Big Data Increases Inequality and Threatens Democracy*, Crown.

Pistilli C. (2021), C*ovid, caccia a cento passeggeri di un aereo*: *da Londra a Roma con un positivo a bordo*, 16 February, https://roma.repubblica.it/cronaca/2021/02/16/news/covid_aereo_da_londra_a_roma_con_un_positivo_a_bordo_caccia_a_cento_passeggeri-287817944/.

Ponce A. (2020), "Covid-19 Contact-tracing Apps: How to Prevent Privacy from Becoming the Next vVictim", ETUI *Research Paper-Policy Brief*, n. 5.

Privacy International (2020a), "Covid Contact-tracing Apps Are a Complicated Mess: What You Need to Know", P*rivacy International*, http://privacyinternational.org/long-read/3792/covid-contact-tracing-apps-are-complicated-mess-what-you-need-know (accessed: 19 June 2020).

– (2020b), "Poland: App Helps Police Monitor Home Quarantine", P*rivacy International*, http://privacyinternational.org/examples/3473/poland-app-helps-police-monitor-home-quarantine (accessed: 28 November 2021).

Ranisch R., Nijsingh N., Ballantyne A., van Bergen A., Buyx A., Friedrich O., Hendl T., Marckmann G., Munthe C., Wild V. (2020), "Digital Contact-tracing and Exposure Notification: Ethical Guidance for Trustworthy Pandemic Management", E*thics and Information Technology*, vol. 23, pp. 285-294.

R*egulation* (EU) 2016/679 *of the European Parliament and of the Council of* 27 A*pril* 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*), OJ L 119, 4.5.2016.

Rugani G. (2020), "Le condizioni ricavabili dal Regolamento generale sulla protezione dei dati per le applicazioni nazionali di tracciamento dei contatti: alcune considerazioni", E*uropean Papers*, vol. 5, n. 1, pp. 633-644.

Seaztu F. (2017), "Article 9", in V. Della Fina, R. Cera, G. Palmisano (eds), T*he United Nations Convention on the Rights of Persons with Disabilities*: A *Commentary*, Cham, Springer, pp. 225-242.

Sekalala S., Dagron S., Forman L., Meier B.M. (2020) "Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance During the Covid-19 Crisis", H*ealth and Human Rights*, vol. 22, n. 2, pp. 7-20;

Smuha N.A. (2021), "Beyond the Individual: Governing AI's Societal Harm", *Internet Policy Review*, vol. 10, n. 3, https://policyreview.info/articles/analysis/beyond-individual-governing-ais-societal-harm.

Seto E., Challa P., Ware P. (2021), "Adoption of Covid-19 Contact-tracing Apps: A Balance Between Privacy and Effectiveness", *Journal of Medical Internet Research*, vol. 23, n. 3, p. e25726, doi: 10.2196/25726.

Shah S.G.S., Nogueras D., van Woerden H.C., Kiparoglou V. (2020) "The Covid-19 Pandemic: A Pandemic of Lockdown Loneliness and the Role of Digital Technology", *Journal of Medical Internet Research*, vol. 22, n. 11, p. e22287, doi: 10.2196/22287.

Tridimas T. (2006), *General Principles of* EU *Law*, Oxford, Oxford University Press, 2006.

Van Kolfschooten H., De Ruijter A. (2020), "Covid-19 and Privacy in the European Union: A Legal Perspective on Contact-tracing", *Contemporary Security Policy*, vol. 41, n. 3, pp. 478-491.

Veale M., Zuiderveen Borgesius F. (2021), *Demystifying the Draft* EU *Artificial Intelligence Act*, preprint, SocArXiv, doi:10.31235/osf.io/38p5f.

Ventrella E. (2020), "Privacy in Emergency Circumstances: Data Protection and the Cpvid-19 Pandemic", ERA *Forum*, vol. 21, n. 3, pp. 379-393.

Vincent J. (2020), "France is Using AI to Check Whether People Are Wearing Masks on Public Transport", *The Verge*, https://www.theverge.com/2020/5/7/21250357/france-masks-public-transport-mandatory-ai-surveillance-camera-software (accessed: 28 November 2021).

Wachter S., Mittelstadt B., Russell C. (2020), "Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-discrimination Law and AI", *Computer Law & Security Review*, vol. 41, pp. 1-31.

Waddington L. (2009), "Breaking New Ground: The Implications of Ratification of the UN Convention on the Rights of Persons with Disabilities for the European Community", in O.M. Arnardottir, G. Quinn (eds), *The* UN *Convention on the Rights of Persons with Disabilities*: *European and Scandinavian Perspectives*, Leiden-Boston, Brill, pp. 111-140.

– (2019), "Regulating e-Accessibility and Digital Equality in Europe from a Multilevel Perspective", in C. Ricci (ed.), *Building an Inclusive Digital Society for Persons with Disabilities New Challenges and Future Potentials*, Pavia, Pavia University Press, 2019, pp. 3-18.

WHO 2020, *Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies For Covid-19 Contact-tracing*, Interim guidance, 28 May.

Xenidis R. (2020), "Tuning EU Equality Law to Algorithmic Discrimination: Three Pathways to Resilience", *Maastricht Journal of European and Comparative Law*, vol. 27, n. 6, pp. 736-758.

Xenidis R., Senden L. (2020), "EU Non-discrimination Law in the Era of Artificial Intelligence: Mapping the Challenges of Algorithmic Discrimination", in U. Bernitz, X. Groussot, J. Paju, S.A. De Vries (eds), *General Principles of* EU *law and the* EU *Digital Order*, Kluwer Law International, pp. 151-182.

Zuiderveen Borgesius F.J. (2020), "Strengthening Legal Protection Against Discrimination by Algorithms and Artificial Intelligence", *The International Journal of Human Rights*, vol. 24, n. 10, pp. 1572-1593.