Keele Law Review, Volume 3 (2021), 1-19
ISSN 2732-5679

The Curious Case of the Failure of the Contact Tracing Apps: In Search of a Balance Between the Right to Health and the Protection of Fundamental Rights During the Covid-19 Crisis

*Daniela Messina**

Abstract

The extraordinary speed with which the Covid-19 virus has been spreading throughout the world, penetrating the fabric of distant countries and traditions, revolutionising their daily habits and gestures, has pushed governments to find far-reaching emergency solutions. These interventions have inevitably impacted the sphere of recognised and guaranteed rights that represent the 'beating heart' of democratic constitutional systems. In a landscape characterised by continuous digital evolution, the search for remedies has invariably concentrated also on technology tools, such as remote working platforms, body temperature scanners, food and grocery delivery apps, whose peculiar characteristics have immediately become great allies against the spread of the virus. In the wake of the first experiments carried out in China and South Korea, the possibility of adopting contact tracing tools to support the diagnostic activities to reconstruct the chain of infection has strongly emerged. However, the results obtained have been somewhat disappointing so far. In a pandemic scenario where the potentialities of technological tools could be a fundamental weapon in fighting the virus, the various experiences of digital contact tracing have highlighted the need for an extensive analysis of the relationship between individual rights and technologies. The paper aims to highlight two crucial lessons that can be learnt from this first phase of digital implementation in a time of crisis, and their impacts on the future evolution of technology in democratic societies.

I. The Outbreak of Covid-19 and New Technologies

It has been a year since the outbreak of Covid-19, a virus which spread throughout the world, penetrating the fabric of distant countries and traditions, revolutionising their daily habits and gestures.[1] Within this serve health crisis scenario, working and recreative activities, as well as interpersonal relationships,

* Daniela Messina, Adjunct Professor in Information and Communication Law, Università degli Studi di Napoli "Parthenope", Italy.

[1] The World Health Organization has officially declared a pandemic outbreak Covid- 19 on March 11, 2020, following the international intensification of cases outside of China's borders, where, as is known, there was the first documented outbreak of epidemic at the end of 2019 and the beginning of 2020.

have been forced to a sudden and sharp shutdown in order to limit transmissions, vital to preserve the health of individuals and the community.

The need to limit this unknown enemy as quickly as possible, has led to global adoption of a series of emergency measures which has been determined as a considerable, and necessary, suppression of the exercise of fundamental individual and collective freedoms. Notwithstanding this, the fight against the virus has faced greater difficulties in democratic societies due to the prevalence of a recognised sphere of guaranteed rights. These have been impeded by the onslaught of restrictions, otherwise considered the 'beating heart' of constitutional systems. Indeed, the main struggle within this complex epidemiological crisis has been the dynamic compromise among political, economic, and social priorities to be pursued in the medium-short term and the need to preserve the detailed framework of principles, powers, limits, and guarantees that are the foundations and ultimate aim of democratic structures.

In a landscape characterised by continuous digital evolution, the search for such remedies has been inevitably focused on technology tools, whose peculiar characteristics subsequently became great allies against the spread of the Covid-19. Digitalisation has offered strong and effective alternatives to combat the virus which are not necessarily based in maintaining the material difference between people such as the essential use of the masks to prevent the infections, social distancing, and the closure of non-essential activities in the most critical phases of the health crisis. Technology has offered instruments to precisely relax those space barriers which have inevitably emerged following emergency measures adopted by national governments. The emergence of the COVID-19 infection in the East led to experiments in China and South Korea[2] assessing the possibility of adopting contract tracing tools to support the diagnostic activities which has facilitated the emergence of a trend to reconstruct chains of infection.

Digital contact tracing uses mobile applications (apps) to support health authorities in the medical follow-up of patients alongside the activities usually carried out manually. The aim is to alert citizens that they have been in close proximity to an individual who has been confirmed positive for Covid-19

[2] China has almost immediately implemented tracking technologies strengthening traditional medical activities. The monitoring system adopted appears to be broad-spectrum, as it provides facial recognition mechanisms and the use of a 'health code' in QR format to access public spaces. The solution adopted by South Korea is different but no less invasive since it implements processing and cross-referencing of data obtained through geolocation techniques, video surveillance systems, and banking transaction control mechanisms. The legal basis for this tracking system is the Infectious Disease Control and Prevention Act (IDCP Act) adopted by the National Assembly on February 26, 2020. See The Government of the Republic of Korea, 'How Korea responded to a pandemic using ICT (Information Communication Technology' *(*2020) < Flattening the curve on COVID-19: How Korea responded to a pandemic using ICT 상세보기|Bilateral RelationsEmbassy of the Republic of Korea to the Hellenic Republic (mofa.go.kr)> accessed 21 February 2021; Yasheng Huang, Meicen Sun, and Yuze Sui, 'How Digital Contact Tracing Slowed Covid-19 in East Asia' *Harvard Business Review* (April 15 2020) <How Digital Contact Tracing Slowed Covid-19 in East Asia (hbr.org) > accessed 21 February 2021; OECD, 'Testing for COVID-19: A Way to Lift Confinement Restrictions' (2020), <Testing for COVID-19: A way to lift confinement restrictions - OECD (oecd-ilibrary.org)> accessed 27 February 2021.

providing direct guidance to citizens ensuring that all 'play their part' in the control of disease.[3]

The contribution offered by these technologies is particularly relevant. As is known, the so-called "shoe-leather epidemiology" traditionally involves the collection of epidemiological data "by direct inquiry among all or a representative sample of the affected people, for example by walking door to door (wearing out shoe leather in the process, hence the term) to ask direct questions".[4] It relies on three steps: contact identification, where the person confirmed as infected remembers activities and persons who have been in contact with; contact listing and contact follow-up to monitor for symptoms and test for signs of infection.[5] Technology dramatically enhances this process and makes it more efficient in curbing the virus's spread. Thanks to smartphones' ubiquity, indeed, digital tracing can efficiently and quickly manage a more significant amount of data compared to traditional disease surveillance activity, drastically limiting personal contacts between public health operators and citizens.[6] It is also able to overcome the natural limits of human memory since it allows individuals to 'remember' potential exposure to COVID-19 following interactions with acquaintances and relatives, where this also expands to unknown people, accidentally encountered during daily life. It follows that this tool significantly supports the so-called T3 (Test-Treat-Track) strategy that usually takes place during epidemiological outbreaks[7] as it strengthens the crucial phase of tracking infected people to isolate them, reducing the spread of the virus.

However, despite the potentialities described, the digital contact tracing experience has been somewhat disappointing so far. In Europe, none of the twenty-one Member States that adopted this solution has reached the limit of 60% downloads,[8] considered the minimum threshold for the treatment's full effectiveness.[9] On the contrary, during these months, a broad attitude of mistrust

---

[3] eHealth Network, 'Mobile Applications to Support Contact Tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States' (2020) 6.

[4] A Dictionary of Public Health., 'Shoe-leather epidemiology', Oxford University Press (2007) <https://www.oxfordreference.com/view/10.1093/oi/authority.20110803100502769> Accessed 05 July 2021.

[5] World Health Organization, 'Contact tracing' (2011) <https://www.who.int/news-room/q-a-detail/contact-tracing>. Accessed 5 July 2021.

[6] ISS Bioethics COVID-19 Working Group. 'Digital support for contact tracing during the pandemic: ethical and governance considerations'. (Roma, Instituto Superiore di Sanità; 2020); See also Daniel Shu Wei Ting, Lawrence Carin, Victor Dzau & Tien Y. Wong. 'Digital technology and COVID-19'. *Nat Med* 26, 459–461 (2020). https://doi.org/10.1038/s41591-020-0824-5; Priscilla N. Owusu, 'Digital technology applications for contact tracing: the new promise for COVID-19 and beyond?'. *Glob health res policy* 5, 36 (2020). https://doi.org/10.1186/s41256-020-00164-1.

[7] The T3 strategy has been built by the World Health Organization within the scope of the malaria outbreak. On the topic see WHO, 'Universal Access to Malaria Diagnostic Testing – An Operational Manual' (Malta, 2013); OECD (n.3).

[8] An updated list of the States that have adopted digital contact tracing can be found on the MIT Technology Review's blog at the following link: Patrick Howell O'Neil, Tate Ryan-Mosley and Bobbie Johnson, 'A Flood of Coronavirus Apps are Tracking Us. Now it's Time to Keep Track of Them' *(MIT Technology Review,* 7 May 2020) < https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/> accessed 29/6/21

[9] A study conducted at Oxford University showed that, in order for the technological solution to be considered effective and contribute to ending the spread of the epidemic, the contact tracing application must be used by 60% of the population or by at least 80% of smartphone owners. See Luigi Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner,

towards the digital tool has been spreading, emphasised by the idea that this kind of tracking is inefficient for fighting the health crisis. Strong is the belief that digital contact tracing is too pervasive, resolving itself as an unnecessary measure which is disproportionate in a democratic society.

In a pandemic scenario where the technological tools' potentialities could be a crucial weapon to fight the virus, the European experience highlights the need for an in-depth analysis of the actual relationship between democratic evolution and new technologies.

II. Balancing of Interests During the Emergency

Democracy is an evolving process,[10] the principles and values on which it is based represent not only the origin that legitimised the fulfilment of this order but it is ultimate aspirations which are the protection and guarantee of rights and freedoms which are of their essence. From an evolutionary perspective, these systems are characterised by an ongoing tension aimed at progressively balancing, various conflicting interests to ensure that there is no hierarchy of rights where one cannot be seen to prevail in an absolute manner.[11] In ensuring this, a harmonious, peaceful coexistence composition of rights is realised.

This structure also operates during times of crisis. Indeed, it is precisely in the darkest moments that the balance between interest's deemed worthy of protection becomes fundamental for the survival of democratic societies. When the system finds itself in trouble and is more easily exposed to attacks on its democracy, the legislator must strengthen its attention so that contingent needs do not distract from the common interest by favouring decisions that could compromise the future of democracy. Facing social, political, and legal challenges in democratic societies, therefore, implies a continuous effort to protect the values and principles that represent the essence of the rule of law.[12]

This is clearly exemplified in the current health crisis scenario. In an attempt to save as many lives as possible whilst guaranteeing the sustainability of national health systems, in initial stages of the spread of the Covid-19 virus, traditionally democratic states have adopted necessary restrictive measures on fundamental freedoms, such as the freedom of movement, residence, freedom of assembly, as

---

Michael Parker, David Bonsall, Christophe Fraser, 'Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing' (2020) Science 368 (6941); Robert Hinch et. al., 'Effective Configurations of a Digital Contact Tracing App: A Report to NHSX' (2020) <Report_-_Effective_App_Configurations.pdf (theconversation.com)> accessed 27 February 2021.

[10] Norberto Bobbio, *The Future of Democracy: A Defence of the Rules of the Game* (Cambridge UK, Polity Press, 1987) VII.

[11] See, inter alia, Gustavo Zagrebelsky, *Il diritto mite. Legge diritti giustizia*, (Einaudi 1992); Roberto Bin, *Diritti e argomenti. Il bilanciamento degli interessi nella giurisprudenza costituzionale* (Giuffrè 1992); David Altman, *Direct Democracy Worldwide* (Cambridge University Press, 2010); Gino Scaccia, 'Il Bilanciamento Degli Interessi come Tecnica di Controllo Costituzionale' (*Consulta Online,* 1998) 6, p. 3953; Vittorio Angiolini, *Libertà e Giurisprudenza Costituzionale* (Giappichelli 1993); Andreas Kulick, 'How to Balance the Conflicting Interests: Proportionality Analysis', *Global Public Interest in International Investment Law* (Cambridge University Press 2012); Roland Axtmann, *Balancing Democracy* (Continuum International Publishing Group 2001).

[12] Council of Europe, 'Respecting Democracy, Rule of Law and Human Rights in the Framework of the COVID-19 Sanitary crisis: A Toolkit for Member States' *(SG/Inf11 2020)* 3.

well as fundamental economic freedoms. However, over time, the need to reactivate the democratic balance to allow for the gradual loosening of the restrictions in a future vision of returning to normality has emerged. To achieve this aim, during the pandemic States have been experimenting with different solutions to protect their communities and at the same time prevent the right to health, multifaceted and prodromal to the life in a society, to turn itself into a 'tyrant' right.[13]

This view takes on particular importance as a democratic system, in order to survive over time, must be able to deal with inevitable situations of crisis, sudden and unpredictable, through the implementation of emergency measures. However, such decisions must always be proportional, necessary, and temporary in order to avoid that the emergency could undermine the system by drifting it away from its purposes.

The choice to adopt contact tracing systems as an instrument to address the virus inevitably inserts itself into this continuous and delicate process. Indeed, the potential that accompanies technological innovation must necessarily be canalised along the tracks of the democratic evolution of modern societies to prevent it from acting as an obstacle to its path. To make this happen, digital development must always be realised in full respect of the principles and values that constitute the system's fundamental pillars, operating as an instrument of reinforcement not of detriment to the exercise of freedoms and fundamental rights.

This is particularly necessary with technological tools such as IoT and Artificial Intelligence that have now surpassed the boundaries between the analogue and digital sphere, encouraging the creation of a dimension, so called 'on life',[14] in which the two areas are closely interdependent, often seamless. As is known, nowadays, complex algorithms are able to analyse and match data provided by different sources and datasets in order to find unexpected correlations and patterns and realise more efficient decisions.[15] That is particularly relevant in a pandemic context in which intervening promptly in the spread of infections is vital. However, precisely the extraordinary ability to predict behaviours and processes with unprecedented accuracy represents the new digital landscape's most dangerous and delicate aspect. One of the more significant issues connected with the diffusion of new technologies is the lack of transparency in the algorithms' functioning. More and more often, AI operates as a black box: the related decision-making process is often opaque and potentially harmful to the beneficiaries.[16]

---

[13] *Ilva case* (2013) Corte Costituzionale 85. The Italian Constitutional Court, in this famous case law, has emphasised the existence of a mutual integration relationship between fundamental rights, a relationship that prevents a right from having absolute prevalence over the others. On the contrary, there would be an unlimited expansion of one of the rights that would become a' tyrant 'against other juridical situations that are constitutionally recognised and protected'.

[14] Luciano Floridi, *The Onlife Manifesto. Being Human in a Hyperconnected Era* (Springer 2015).

[15] Daniela Messina, 'Online platforms, profiling, and artificial intelligence: new challenges for the GDPR and, in particular, for the informed and unambiguous data subject's consent' (2019), Medialaws - Rivista di diritto dei media 2 159,161.

[16] See, inter alia, Viktor Mayer-Shönberger, Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt 2013); Andrea Simoncini, 'L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà' (2019) *Biolaw Journal* 1; High-Level Expert Group on Artificial Intelligence, *A definition of AI: Main*

Since it is large proved that without strict rules, AI could embed prejudices based on sex, age, race, disability, or other irrelevant characteristics[17], there is no doubt that the smaller is the logical-deductive contribution that humans make in presence of automated activities, the greater is the risk of obtaining results capable of compressing the individual's capacity for autonomous and independent choice.[18] Making decisions based on sophisticated profiling activities, often without human interventions, indeed, risks leading to the extreme consequence of exacerbating discriminations, inhibiting the exercise of fundamental freedoms, or limiting the provision of essential services.

This is particularly dangerous in the presence of wide-ranging digital tracing systems to which activity of prevention and limitation of the spread of the virus is correlated, but also a definite possibility of accessing more quickly to health care or, on the contrary, being able to access workplaces or to participate in social events once the absence of the disease has been ascertained.

It follows that within an increasingly data-centric system, enriched by progressively more intense profiling activities, the protection of individuals' dignity requires the provision of more significant safeguards and guarantees aimed at strengthening the self-determination of the individuals. Their protection can no longer disregard the provision of measures to face situations of unlawful or unconscious treatment of personal information and avoid phenomena of limitation of liberties and fundamental rights.

Therefore, within such a dynamic and complicated panorama, the introduction of new technological instruments, especially given their collective interest, requires an *ex-ante* assessment of their compliance with the system of principles and guarantees and their mandatory inclusion in the democratic balancing.

In the case of digital tracking tools, this analysis inevitably includes evaluating the instrument's proportionality and the scheduling of a time limit beyond which the processing is no longer legitimate. A 'sunset clause' is needed[19] to prevent the crisis from stabilising, allowing digital contact tracing to exercise illegitimate interference in the full and conscious exercise of fundamental rights. Since it is unpredictable, the exceptionality of the emergency allows interventions that can be justifiable due to the provisional nature of the regime of necessity compared to the normality of the rule of law. However, it should be emphasised, such decisions must always and in any case be adopted in view of a return to normality, in order to avoid 'breaks' within the democratic order that can lead to an unacceptable point of no return.[20] In the absence of such a perspective, the risk

capabilities and scientific disciplines (2019); Dan L. Burk, 'Algorithmic Fair Use' (2019) *The University of Chicago Law Review*, (86) 283; Bart van der Sloot, Sascha van Schendel, 'Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study', 7 (2016) JIPITEC 110.

[17] Edward Santow, 'Can Artificial Intelligence Be Trusted with Our Human Rights?' *AQ: Australian Quarterly* (2020) 91 (4) 10. See also paragraph 3.

[18] See Alessandro Acquisti, Jens Grossklags, 'Privacy and Rationality in Individual Decision Making' (2005) IEEE Security and Privacy Magazine 3(1) 26; Anna Papa, 'La Problematica tutela del diritto all'autodeterminazione informativa nella Big Data society' (*Consulta Online* 2020) <Consulta OnLine - Anna Papa,La problematica tutela del diritto all'autodeterminazione informativa nella big data society; (giurcost.org)> date accessed 20 February 2021.

[19] Council of Europe (n 9) 3.

[20] See, inter alia, Alfredo Fioritto *L'amministrazione dell'emergenza tra autorità e garanzie* (Il Mulino 2008); Giovanna De Minico, *Costituzione, emergenza e terrorismo* (Jovene 2016); Diletta Dima, Uso e abuso degli strumenti emergenziali. Alcune (ulteriori) distorsioni in tempo

that emerges is that technologies could transform themselves from a support tool to a means of prevarication, exacerbating discrimination and limiting the exercise of pre-existing essential freedoms.

In light of these considerations, the European experience of digital contact tracing takes on particular importance in the study of the current relationship between society and new technologies: it suggests a wealth of considerations offering two important lessons for the future digital evolution of democratic societies.

III. The Legal Basis for Digital Contact Tracing

'The systematic and large-scale monitoring of location and/or contacts between natural persons is a grave intrusion into their privacy'.[21] This is the starting point of the guidelines which have addressed the Member States' choice to adopt digital contact tracing systems to help fight Covid-19. It is unquestionable, that the introduction of particularly pervasive technologies within democratic societies inevitably requires a prior assessment that allows the instrument to be grafted into the framework of the principles and values shared and enshrined in the European constitutions.

Sophisticated profiling activities can exacerbate already existing discriminations or stereotypes,[22] intense profiling activities can penalise individual inclinations.[23] Furthermore, an incomplete or incorrect data set can fatally lead to inaccurate or incorrect predictions, generating biased and potentially harmful results for users. Security issues can determine, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy.[24] Without adequate guarantees, data mining and data analysis can invariably impact the right to self-determination, limiting the variety of information, knowledge, and opinion that an individual can access. This process is likely to curb pluralism, a vital cornerstone of the democratic order.[25]

Consequently, within the digital scenario, protecting individuals from losing control over their personal data has become crucial since, without proper

---

di crisi (2014) 22 Federalismi.it.; Massimo Luciani, Il sistema delle fonti del diritto alla prova dell'emergenza (2020) 2 Rivista AIC 1.

[21] The 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' (2020) 7

[22] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (17/EN WP251rev.01 2018).

[23] Viktor Mayer-Shönberger, Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt 2013); Ira S. Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 (2) IDPL 74.

[24] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1, recital 75.

[25] See Anna Papa (n 12); Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018 17/EN WP251rev.01); Andrea Simoncini, 'L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà'(2019) Biolaw Journal <L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà | Simoncini | BioLaw Journal - Rivista di BioDiritto> accessed 20 February 2021

guarantees, data analysis can lead to the extreme consequence of inhibiting the exercise of fundamental freedoms or limiting the provision of essential services.

In this light, the protection of personal data, especially in a digitally oriented society, has become a fundamental right, as expressly stated by Regulation (EU) 679/2016 (hereafter GDPR) and guaranteed by the Charter of Fundamental Rights of the European Union Art. 8, paragraph 1,[26] as well as Article 16, paragraph 1, of the Treaty on the Functioning of the European Union.[27] It follows that this legal situation is not only worthy of protection by placing a duty of intervention from public authorities through the provision of appropriate and specific guarantees, but at the same time, it is inevitably subjected to that irrevocable work of balance between conflicting interests, which represents an activity inextricably linked to the very essence of all democratically advanced societies. These considerations assume relevance in the presence of tracking activities that require the involvement of special categories of personal data according to Art. 9 of the GDPR. As stated by the former Working Party Article 29, the processing of health data is always an activity that presents a high risk and therefore necessarily requires the implementation of a data impact assessment to prevent such tracking from leading to discrimination.[28]

Consequently, the possibility of implementing such extensive tracking tools to address Covid-19 has inevitably required a deep and reasoned reflection on the need and the opportunity to adopt such a solution within democratic societies. In particular, the need to assess the extent to which the epidemiological emergency can justify the introduction of potentially invasive technological measures within democratic societies and what guarantees need to be adopted have been arising in order to avoid that the use of these tools results in unacceptable damage to the sphere of the dignity of the individuals who decide to use them.[29]

This is the reason that has led the European Union to address the digital contact tracing along the tracks of the principles and values defined in the field of data

---

[26] Charter of Fundamental Rights of the European Union (2012) OJ C 326/391.

[27] Consolidated version of the Treaty on the Functioning of the European Union (2012) OJ C 326/47.

[28] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Pocessing is 'likely to result in a high risk' for the purposes of Regulation 2016/679' (2017 17/IT WP 248 rev.01) 18.

[29] See, inter alia, Sofia Coffa, 'The Infection of Privacy at the Height of COVID-19' (*Media Laws*, April 30 2020) <The infection of privacy at the height of COVID-19 (medialaws.eu)> accessed 22 February 2021; Benjamin Boudreaux, Matthew A. De Nardo, Sarah W. Denton, Ricardo Sanchez, Katie Feistel, Hardika Dayalani, 'Strengthening Privacy Protections in COVID-19 Mobile Phone–Enhanced Surveillance Programs' (2020) Research Brief RAND Corporation <https://www.rand.org/pubs/research_briefs/RBA365-1.html.> accessed 22 February 2021; C. Carlo Colapietro e Antonio Iannuzzi, 'App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa tra tutela del diritto alla salute e protezione dei dati personali' (2020) 2 Dirittifondamentali.it <Colapietro-Iannuzzi-App-di-contact-tracing-e-trattamento-dei-dati-con-algoritmi.pdf (dirittifondamentali.it) > accessed 22 February 2021; Oreste Pollicino, 'Fighting Covid-19 and Protecting Privacy. A Proposal in the Light of the Roots of European Constitutional Law' (*Media Laws* March 25 2020) < Fighting Covid-19 and protecting privacy. A proposal in the light of the roots of European Constitutional law (medialaws.eu) > accessed 22 February 2021; Giorgio Resta, 'The Protection of Personal Data in the COVID-19 Emergency Law' (*Giustiziacivile.com* 5 March 2020) <La protezione dei dati personali nel diritto dell'emergenza Covid-19 | Giustizia Civile> accessed 22 February 2021; Tamar Sharon, 'Blind-sided by privacy? Digital contact tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers' (2020) 18(1) Ethics and Information Technology [Online] [Accessed 29/6/2021] Available from doi: 10.1007/s10676-020-09547-x.

protection, establishing *a priori* measures and guarantees to implement this tool in a proper way.

The implementation of digital tracking solutions derives its legitimacy in the GDPR, which legalises the processing of personal data if it is necessary to protect the vital interests of the data subject or of another natural person (Art. 6 paragraph 1 lett.d). Similar evaluation acts when processing is necessary for humanitarian purposes, including the monitoring epidemics and their spread or in situations of humanitarian emergencies, in situations of natural and man-made disasters (Recital 46).

In addition, concerning special categories of personal data ex Art. 9, GDPR allows processing for reasons of public interest in relation to public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical device, as well as for health security, monitoring, and alert purposes, the prevention or control of communicable diseases, and other serious threats to health (Recital 52).

The technological solutions implemented in Europe were created in compliance with the essential requirements established in two main documents: The Common EU Toolbox for Member States[30], realised by the eHealth Network and the Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak[31], adopted by the European Data Protection Board. To ensure a common approach, the national apps are voluntary and make use the of the Bluetooth technology instead of the more invasive geolocation technique. In this way, they can guarantee the simple 'memorisation' of the codes associated with the devices encountered during the day, without allowing the more insidious reconstruction of the movements made by the subjects being traced. In addition, the data transmitted must include only unique and pseudonymous codes which minimises the risk of a possible re-identification of the tracked user. The apps are also designed to strictly comply with the essential principles of the GDPR, namely the purpose limitation, the proportionality, and transparency of the processing, as well as the minimisation of the data collected, and the identification of a specific time limit for the conservation of the information.

By respecting these parameters, the European apps guarantee - or should guarantee - an appropriate balance between the protection of individual and collective health through more effective and fast identification of possible outbreaks as well as the reconstruction of the infection chain, and protection of personal data, so that such a solution can be used 'to empower, rather than to control, stigmatise, or repress individuals'.[32]

However, albeit the protection of personal data has been playing a central role in the European experience of digital contact tracing, the poor results obtained so far show, especially in a moment of crisis, that the lawfulness of a new technological instrument is a necessary but not sufficient condition for its full acceptance in a democratic society.

The widespread climate of mistrust and opposition to the technological remedy has indeed highlighted, perhaps for the first time in recent history, that the mere

[30] eHealth Network (n.4).
[31] The European Data Protection Board (n.15).
[32] Ibid 3.

implementation of technology tools to solve issues is not a general panacea. This is true even in the context of a health emergency. In an increasingly digitalised world in which technologies are more and more grafted into the fabric of people's daily and working activities, the implementation of new technologies, mostly of significant interest for communities, requires a step forward which consists both in a simultaneous and coordinated action of all public and private actors involved as well as in overcoming of individualisms.

IV. The Need for a Trustworthy Ecosystem

Almost a year after the first trials of digital contact tracing in Europe, the tool's criticalities have not so much concerned the legitimacy and proportionality of the treatment, which, in the light of the GDPR, have been identified in reasons of public interest in the area of public health and epidemiological contrast. The most significant issues, instead, have concerned a general attitude of diffidence and distrust among the recipients. An approach rooted in the widespread weakness of the organisational and security architecture created to support data collection that has limited the digital measure to be successful.

During the emergency, many examples have been emerged in this regard. The Italian 'Immuni' app, for example, has suffered from the lack of a detailed strategic plan involving the national health system in a clear and timely manner.[33] This disorganisation has generated a sense of bewilderment and distrust among users[34], who in many cases have had to face the typical consequences of the automated decision-making processes according to Art. 22 of the GDPR. The absence of specific protocols able to guarantee the healthcare staff's fast involvement in order to compare the outcome of the notification with the actual conditions of the patient or proceed with a diagnostic for SARS-CoV-2 has determined, indeed, cases of 'discrimination from Covid-19'.[35] Many alerted users have been forced to self-isolate, without certain times, with obvious consequences in terms of workplace accessibility, circulation on the territory, and personal relationships management. This is despite the fact they were only potentially positive individuals waiting for a test.

In the United Kingdom, the 'NHS Covid-19' app has also encountered several problems. After shifting from a centralised to a decentralised system to store

[33] On the necessity and limits of digital tracing in Italy see Francesco Pizzetti, 'Pandemia, Immuni e app di tracciamento tra GDPR ed evoluzione del ruolo dei Garanti' (*Media Laws,* 2020, 2) 11; Giovanna De Minico, 'Virus e algoritmi. Impariamo da un'esperienza dolorosa' (*la Costituzione.info*, 1 April 2020) <Virus e algoritmi. Impariamo da un'esperienza dolorosa – laCostituzione.info> accessed 20 February 2021; Giusella Finocchiaro, 'Il punto sull'app Immuni: bilanciamento tra diritti' (*Media Laws,* 9 June 2020) <Il punto sull'app Immuni: bilanciamento tra diritti (medialaws.eu) > accessed 20 February 2021.

[34] Editorial, 'L'app Immuni mi ha avvisato a quarantena finita. Ora ho capito perché si tarda: segnalarsi positivi è un'impresa' *Corriere della Sera, (*Milan, 1 november 2020) <«L'app Immuni mi ha avvisato a quarantena finita. Ora ho capito perché si tarda: segnalarsi positivi è un'impresa»- Corriere.it> accessed 10 February 2021; Luigi Garofalo, 'Sanità digitale, cosa va (ricetta via sms) e cosa non va (Immuni sconosciuto a molte Asl)' *(Key4biz,* 15 October 2020) <Sanità digitale, da Immuni sconosciuto a molte Asl alla ricetta via SMS (key4biz.it)> accessed 10 February 2021.

[35] Daniela Messina, 'Sistemi di Contact Tracing nell'emergenza Covid-19: Alla Ricerca di un equo Bilanciamento ra diritto alla salute, tutela dei dati personali e dovere di solidarietà' (2020) 3 Nuovo Diritto Civile 459.

data, in line with Italy and Germany, according to some analysts, the test and trace project was 'managed chaotically and became the subject of bureaucratic tussles. The result was overspending, wasted effort, and—worse—wasted time'.[36]

The English digital tracing, indeed, has been strongly affected by the overall tracking strategy's continuous redefinitions. The consequential national poor results have led to re-evaluating a localised approach with contact tracers focused on specific areas to provide a more tailored service.[37] The aim is to mimic the traditional tracking known as 'shoe-leather epidemiology', which involving 'painstaking direct inquiry among all or a representative sample of the affected people, for example by walking door to door'[38] seems to be anachronistic within a digital landscape.

Security problems, instead, have occurred in Spain and Germany. The Spanish government has declared with an official statement that it has been necessary to update the app 'Radar Covid-19' in October 2020 due to a breach in the tracking system that allowed to trace easily COVID-positive individuals' identity. Unauthorised third parties, indeed, were able to monitor data traffic, associate the transfer of encrypted information to a unique user and indirectly associate the positivity status.[39] The security issue, which was mitigated by sending fake positives,[40] has started a heated discussion due to a delay in making the problem public since it was deemed not of such seriousness as integrating a breach of personal data security Art. 33 of the GDPR.[41]

---

[36] James Ballarchive, 'The UK's Contact Tracing App Fiasco is a Master Class in Mismanagement' (*Mit Technology Review,* 19 June 2020) <https://www.technologyreview.com/2020/06/19/1004190/uk-covid-contact-tracing-app-fiasco/> accessed 20 February 2021.

[37] See Anne-Lise Sibony, 'The UK COVID-19 Response: A Behavioural Irony?' (2020) 11 EJRR, p.350; Laura Hughes, Anna Gross, Andy Bounds, 'UK Government abandons Centralised approach to Contact Tracing in England 'Ringfenced' Teams to Work with Local Councils after Successful Trials' *Financial Times* (London, 10 August 2020)<https://www.ft.com/content/b1f0fe23-a8e0-4c6c-b484-d55d6893ef6f> accessed 28 December 2020;
Leo Kelion, 'Coronavirus: UK confirms plan for its own contact tracing app' *BBC* (London, 12 April 2020) <Coronavirus: UK confirms plan for its own contact tracing app - BBC News> accessed 20 January 2021.

[38] John M. Last, A *Dictionary of Public Health* (Oxford University Press 2007).

[39] See Jordi Pérez Colomé, 'La 'app' Radar Covid ha tenido una brecha de seguridad desde su lanzamiento' *El Pais* (Madrid, 22 October 2020) <La 'app' Radar Covid ha tenido una brecha de seguridad desde su lanzamiento | Tecnología | EL PAÍS (elpais.com)> accessed 23 January 2021.
Pablo Rodríguez, Santiago Graña, Eva Elisa Alvarez-León, et al. 'A population-based controlled experiment assessing the epidemiological impact of digital contact tracing' (2021) *Nat Commun* 12, 587.

[40] 'Identification and deanonymization of COVID-19 positive users that upload Radar COVID TEKs to the Radar COVID server' (*GitHub*, 13 November 2020) <Identification and deanonymization of COVID-19 positive users that upload Radar COVID TEKs to the Radar COVID server. · Advisory · RadarCOVID/radar-covid-backend-dp3t-server · GitHub > accessed 23 January 2021; .

[41] As proof of the relevance of what happened from the point of view of the security, the Spanish Secretary-General has nevertheless communicated the incident to the *Agencia Española de Protección de Datos* (AEPD), that has announced to be working on the procedure but not has expressed its opinion on the gravity of the breach yet. Jordi Pérez Colomé , 'The Governement finally Gives the Details of the Radar Security Breach. The Vulnerability, Considered "High Severity", was definely Resolved on October 30', *El Pais* (Madrid, 20 november 2020) <El Gobierno da finalmente los detalles de la brecha de seguridad de Radar Covid | Tecnología | EL PAÍS (elpais.com) > accessed 28 February 2021.

Similarly, the German application 'Corona-Warn-App', commissioned by the government and created by the technology companies SAP and Deutsche Telekom, recently has shown a technical vulnerability. According to the opinion of one of the researchers who helped to detect it, this issue 'had the potential to affect the integrity of Germany's COVID-19 response'.[42]

In France, the limited spread of digital contact tracing has forced the government to release a second and improved application significantly named 'Tous Anticovid' to underline the need and the inevitable participation of all citizens to limit the expansion of the virus. The most recent version provides a series of new features related to the health crisis and the state of alert due to the pandemic, such as 'MesConseilsCovid,' a questionnaire through which it is possible to obtain personalised support in the event of symptoms, and 'DepistageCovid' which provides an updated map of the screening centres with waiting times information.[43]

Finally, in Spain the uniform spread of digital tracking has undergone a significant slowdown which can be attributed to the peculiar regional articulation of the form of State.[44] The creation of a shared digital front in the fight against the virus, at least in the first phase of the pandemic, was hindered by the implementation of digital applications at the regional and local level. Although initially justified by the organisation in autonomous communities of the Spanish health system,[45] this fragmentation not only slowed down the path of digital contact tracing at a national level but also had consequences on the adoption of the 'Radar Covid' app since the various monitoring and code sharing systems implemented by the autonomous communities have undermined the correct and timely communication of both the usage data and the effectiveness of the application, generating a sense of bewilderment and confusion among the population.[46]

---

[42] Alvaro Muñoz, 'Securing the fight against COVID-19 through open source' (*GitHub*, 19 November 2020) <https://securitylab.github.com/research/securing-the-fight-against-covid19-through-oss > accessed 25 January 2021; Jens Helge Reelfs, Oliver Hohlfeld, and Ingmar Poese, 'Corona-WarnApp: Tracing the Start of the Official COVID-19 Exposure Notification App for Germany'(2020) ACM Special Interest Group on Data Communication (SIGCOMM '20 Demos and Posters).

[43] Décret n. 2020-1310 du 29 octobre 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire; Ministère des Solidarités **et** de la Santé**,** TousAntiCovid: réponses à vos questions (21 October 2020) < TousAntiCovid: réponses à vos questions - Ministère des Solidarités et de la Santé (solidarites-sante.gouv.fr)> accessed 25 January 2021.

[44] As is well known, the Ley Orgánica 4/1981, while giving to the executive body the power to declare the state of alert in case of 'crisis sanitarias, tales como epidemias y situaciones de contaminación graves' (Art. 4, par. 1, lett. b) contemplates the opportunity to act in a coordinated manner with the autonomous. In this perspective, following the declaration of the pandemic, the Real Decree 463/2020 assigned to the government the task of managing the emergency, but at the same time confirmed the maintenance of the competencies of local authorities in the areas covered by their distribution, including explicitly the health sector according to Articles. 148 and 149 of the Constitution.

[45] See Federico Spagnoli, 'L'emergenza Covid 19 in Spagna e negli Stati Uniti: un bilancio comparato' in Rolando Tarchi, *L'emergenza sanitaria da COVID-19: una prospettiva di diritto comparato* (Gruppo di Pisa. Dibattito aperto sul Diritto e la Giustizia Costituzionale 2020).

[46] Jordi Pérez Colomé, 'El Gran Misterio de Cuánta Gente ha usado Realmente Radar Covid'*, El Pais (*Madrid 15 November 2020) <https://elpais.com/tecnologia/2020-11-14/el-gran-misterio-de-cuanta-gente-ha-usado-realmente-radar-covid.html> accessed 23 February 2021.

The above-mentioned experiences prove that several factors have impacted the European digital contact tracing. The absence of rational and wise strategies implemented by governments and national health systems, the various delays in the communication of people who have tested positive, the presence of security issues, as well as organisational systems jeopardised by the territorial fragmentation of the power that have indeed limited its successful application. These problems have led to the creation of a psychological barrier that has pushed a large part of the European population to mistrust a tracking system that made the voluntary use of its strong point.

The lack of trust that emerged during the pandemic has highlighted the existence of a critical issue in the digital evolution of democratic societies. The health crisis has demonstrated that the new digital tools to be affirmed are dependent on the creation of a trustworthy ecosystem,[47] especially if there is a public interest dimension. Despite the essential nature of a legitimate basis in the use of new technology, lawfulness alone cannot achieve a universal atmosphere of trust. As underlined in the field of AI, building a trustworthy scenario means inserting new technologies within a system based on all public and private subjects' joint collaboration, variously involved in innovation. Far from evoking a generic reliability of new technologies, a trustworthy ecosystem, through the correct identification of the stakeholders' roles and responsibilities and the provision of intervention and protection measures for users, aims to generate trust towards the entire value chain that revolves around technology.

To reach this purpose, once the instrument's legitimation basis has been identified, attention should be focused on two other aspects represented by ethics and robustness. It is only the collective and coordinated action of these elements together with lawfulness that ensures that technological innovation establishes itself within society, positively reinforcing its development in a democratic way. If lawfulness guarantees that the technology has been developed with regard to the shared principles and values of the community, ethics progresses thereby requiring that technology be fundamentally human centric. This parameter operates to ensure that new digital tools support or integrate individuals' activities and knowledge rather than inhibiting the exercise of fundamental rights and freedoms.

---

[47] The need to create a trustworthy ecosystem has emerged among the studies on Artificial Intelligence. It represents the pillar around which the European Union has intended to build its digital strategy because of the increasingly intense use of sophisticated applications and 'intelligent' platforms. Faced with these instruments, the need to convey this epochal revolution along the tracks of the essential principles and values that characterise democratically advanced societies has emerged. With this goal, in April 2019, the High-Level Expert Group on Artificial Intelligence drew up the Ethics Guidelines for Trustworthy Artificial Intelligence in April 2019 and the Assessment List for Trustworthy AI (ALTA) in July 2020. See, inter alia, Thomas Wischmeyer, Timo Rademacher, *Regulating Artificial Intelligence* (Springer, Cham 2020); Harry Surden, 'Artificial Intelligence and Law: An Overview' (2019) 35 Ga.St.U.L.Rev , Ira S. Rubinstein (n 17); Viktor Mayer-Shönberger, Kenneth Cukier (n 17); Bart van der Sloot, Sascha van Schendel, Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study, (2016) 7 Jipitec 110; Kevin D. Ashley, *Artificial Intelligence and Legal Analytics New Tools for Law Practice in the Digital Age* (Cambridge University Press 2017); Maryam Ashoori, Justin Weisz, *In AI We Trust? Factors That Influence Trustworthiness of AI Infused Decision-Making Processes* (2019) ArXiv Accessible at: abs/1912.02675; Francesco Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione* (Giappichelli 2018); Paul Nemitz, 'Constitutional Democracy and Technology in the Age of Artificial Intelligence' (2018) Phil. Trans. R. Soc. A 376.

Ultimately the aim is to prevent innovations from inflating progress beyond the ethically acceptable limits in modern society.[48] This robustness is principally linked to the prevention of harm,[49] and operates both in a technical and social perspective. A crucial element, this principal hinges on the need for new technologies to be designed and implemented - borrowing a well-known term in the field of data protection - 'by design and by default' to prevent potential risks. The aim is to minimise unintentional, unforeseen damage and to react resiliently in the event of vulnerability or criticality. In this respect, technologies should not only be technically safe (in the case of contact tracing, examples are the choice of Bluetooth, the creation of encrypted data to avoid the recognition of people tested positive and the decentralised system) but also socially whereby its creation and dissemination considers the context and ends in which it is implemented thereby preventing unwanted consequences for the community. It is crucial that for robustness to be concretely realised, the potential risks associated with the use of new technologies must be understood, assessed, and predicted by those who are physically required to implement the related prevention and protection measures.

In other words, the more highly technical soul must widely deal with the legal and ethical ones in order to create a proper virtuous circular process based on the simultaneous and coordinated action of all the various stakeholders.

Such a wide-ranging involvement that concretely expands to all those directly involved in technological innovation is also contemplated in the Guidelines on artificial intelligence and data protection.[50] On the same ideal line, indeed, the text, approved in Strasbourg on 25 January 2019, not only reiterates in Art. 1 that the protection of human dignity and fundamental freedoms, in particular the right to the protection of personal data, assumes an essential role in the development and adoption of AI applications, but underlines the need to establish a direct dialogue between legislators and various decision-makers, as well as with developers, producers, and service providers. The purpose is fostering 'to adopt a human rights by-design approach and avoid any potential biases, including unintentional or hidden, and the risk of discrimination or other adverse impacts on the human rights and fundamental freedoms of data subjects.'[51]

It follows that the European yearning for a trustworthy ecosystem arises from the belief that new technologies, especially when a high level of automaticity characterises them and whose decisions may impact the exercise of fundamental rights and freedoms, always require in addition to a clear and strong basis of legitimacy, also a reliable, safe, and ethically sustainable scenario to be inserted in. If this does not happen or even just one of these elements is missing, the risk of exposing the user to consequences that can affect the full and conscious development of his/her person, either as an individual or as a member of a community, fatally emerges. Furthermore, the lack of reliability of the system supporting the technology can lead to a widespread distrust, preventing public

[48] See European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2017) OJ C 252/239.
[49] The European Data Protection Board (n 15) 16
[50] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) Guidelines on Artificial Intelligence and Data Protection (2019).
[51] Ibid 2.

interest instruments from making their own positive contributions to society's evolution. That is exactly what happened with European contact tracing.

V. The Lack of Solidarity in the Pandemic Scenario

The second lesson that emerges from the experience of contact tracing concerns the bond that connects members within an organised society. The right to health, as is well known, is a multifaceted legal situation that consists of a double soul: one individual, the other collective. Its protection is intended not only to guarantee the psycho-physical well-being of the individuals, but also the wealth of the whole community, ensuring security and prosperity. This double dimension, which requires a continuous balancing between the two areas so that no one will prevail in an absolute way over the other, is clearly evident in the Italian Constitution in which Art. 32 explicitly states; 'The Republic safeguards health as a fundamental right of the individual and as a collective interest.' The same perspective also underlies the definition of the World Health Organization (WHO). The Ottawa Charter for Health Promotion, indeed, describes health as 'a state of complete physical, social and mental well-being, and not merely the absence of disease or infirmity. [...] a resource which permits people to lead an individually, socially and economically productive life.'[52]

In this light, the right to health undertakes a central role in the evolutionary path of contemporary societies since its protection is not only reconnected to human dignity, becoming an immediate expression of it, but also affirms itself as prodromal to the exercise of all those fundamental freedoms that characterise the life of an individual as a member of an organised community. The collective interest underlying the protection of health inevitably requires the overcoming, especially in this field, of individualistic or sectoral choices that assuring advantages for a limited number of people, can determine negative consequences for the whole present and future community. In this sense, the provisions of the Constitution of the World Health Organization are relevant since they state that the 'health of all peoples is fundamental to the attainment of peace and security and is dependent upon the fullest co-operation of individuals and States.' [53]

Therefore, the protection of health cannot leave out a duty of common solidarity that directly involves individuals and the State for the whole community's well-being.[54] It is the solidarity that generates a feeling of connection and sharing of

[52] WHO, Ottawa Charter for Health Promotion (Geneva, 1986) The whole definition describes health as 'a state of complete physical, social and mental well-being, and not merely the absence of disease or infirmity. Within the context of health promotion, health has been considered less as an abstract state and more as a means to an end which can be expressed in functional terms as a resource which permits people to lead an individually, socially and economically productive life. Health is a resource for everyday life, not the object of living. It is a positive concept emphasising social and personal resources as well as physical capabilities.'

[53] WHO, Preamble to the Constitution of the World Health Organization as adopted by the International Health Conference (New York 1946) 1.

[54] See, inter alia, Danilo Campanelli, 'Solidarity, Principle of', (eds) in Max Planck *Encyclopedias of International Law* (2011); Federico Veronica, Christian Lahusen, 'Solidarity as a Public Virtue?' (2018) 1 Law and Public Policies in the European Union < www.jstor.org/stable/j.ctv941sdc.> accessed 20 February 2021; Vezio Crisafulli, La Costituzione e le sue disposizioni di principio (Giuffrè 1952); Gøsta Esping-Andersen, *Three Worlds of Welfare Capitalism* (Polity 1990); Robert Leonardi and Raffaella Y. Nanetti, *Making Democracy Work* (Princeton University Press 1993); Valentina Tamburrini, 'I doveri costituzionali di solidarietà in

common interests and objectives within a group. It represents that essential 'glue' that connects the principles and values of societies allowing a mutual responsibility among individuals (horizontal solidarity) and between the State and citizens (vertical solidarity). Horizontal and vertical solidarity, indeed, shape the boundaries of democratic systems allowing the reach of shared aims as the principle of equality in a substantive way and the protection of the citizens' rights and needs[55].

Aware of this relevant role, the European Union has always placed solidarity at the foundation of its present and future system. This principle, indeed, has been enshrined in Schuman's declaration in which the building of a *de facto* solidarity was considered an indispensable step for the creation of the Union.

Aware of this crucial role, the European Union has always placed solidarity at the basis of its legal system, also in the perspective of protection between generations[56]. This principle, indeed, has been enshrined in the Schuman Declaration (1950) since the construction of a *de facto* solidarity has always been considered an indispensable step for the creation of the Union[57]. In this perspective, Art. 2 of the TFEU includes this special bond among the European society's pillars[58]. Furthermore, in the TFEU, solidarity, together with the fair sharing of responsibilities, represents the basis for the implementation of Union policies (Article 80). Finally, the Charter of Fundamental Rights of the European Union dedicates to it the entire Chapter IV, placing this principle among the fundamental values of the Union such as human dignity, freedom, and equality.

Therefore, solidarity innervates European society, and by requiring the joint intervention of all citizens, public authorities, and States, it becomes a fundamental element of European society's democratic aspiration.

Despite its relevant role, however, precisely this dimension, which is rooted in a deep sense of belonging to the community, has been the most affected by the critical issues of the organisation behind the implementation of the contact tracing system.

The troubles concerning the absence of a trustworthy ecosystem, fostering an atmosphere of widespread distrust towards the technological application, have prevented the solidarity from emerging and inspiring the use of tracking apps, especially in a health crisis scenario. Therefore, the opacity of information, the absence of a strategic plan shared with the national health systems, and the issues related to safety inevitably led to a prevalence of an individualistic attitude that negatively impacted the tracking systems' success.

Moreover, the use on a voluntary basis has also played an unfavorable role because the essence of this decision has not been fully understood among the population. The choice for the apps' voluntary nature has been inevitably mandatory because strictly connected to the protection of individuals' right of

---

campo sociale: profili generali e risvolti applicativi con particolare riferimento alla tutela della salute' (2018) 18 Ianus 25; Stefano Rodotà, *Solidarietà* (Laterza 2014).

[55] See Adriana Apostoli*, La Svalutazione del Principio di Solidarietà. Crisi di un Valore Fondamentale per la Democrazia* (Giuffrè 2012).

[56] Consolidated version of the Treaty on European Union (2012) OJ C 326/12 Art. 3, par.3.

[57] Declaration of 9th May 1950. Regarding the solidarity principle the Declaration states that: 'Europe will not be made all at once, or according to a single plan. It will be built through concrete achievements which first create a *de facto* solidarity.'

[58] TFEU (n 20).

self-determination from the potential interferences of digital technologies. However, in the absence of a legal obligation, the need to safeguard themselves and, consequently, public health should have brought out the moral obligation to adopt the digital contact tracing. It is especially during a crisis, in fact, that solidarity reveals itself assuming the character of an unconditional duty of the individual for the community. It is the peak moment in which a person participates in society not as an individual but as a citizen, activating that social interdependence that is crucial for pursuing a peaceful coexistence.

Therefore, the lack of consent to a digital technology aimed at fighting a common battle together means that the sphere of duties inextricably linked to the full exercise of rights and freedoms within a democratic society has not been activated. Despite the consideration that the duties of economic, political, and social solidarity represent instead, exactly that 'dark side of the moon' that allows the rule of law to be fully realised. In their absence, society lacks a fundamental aspect for its full realisation in a democratic perspective.[59]

VI. Concluding Remarks

For a democratic regime, being in transformation is its natural state.[60] The imperishable passage of time, bearer of inevitable changes within democratic societies, requires the continuous search for new balances between different interests that come into conflict in front of increasingly complex protection needs. Among the elements that have an impact on this process, technological evolution has a relevant role. Far from being a transitory phenomenon, new technologies' contribution is increasingly permanent and inevitably influences modern communities' progress.

A proof of this involvement also came from the current health crisis. The pandemic has demonstrated to be a potent accelerator of the changes already underway, highlighting the relevance of technology in dealing with a crisis. As is well known, during the apical moments of the infections, a relevant number of working activities have had the chance to continue only through their relocation in the digital universe.

However, the pandemic has also brought to light some critical issues that still characterise digitisation within democratic advanced societies.

As underlined in the article, the future of new technologies, especially the 'intelligent' ones, within democratically advanced societies, will be played on their reliability to be accepted by the communities. Despite its potential in fighting the virus, the failure of digital contact tracing, indeed, has highlighted that innovation, in order to be truly at the service of the community, requires strong coordination among the various stakeholders (public and private) and needs to be grounded in a solid architecture founded on the values and guarantees that outline the horizon of democratic systems.

---

[59] See Alessandro Morelli 'I Principi Costituzionali Relativi ai Doveri Inderogabili di Solidarietà' (*Forum Quaderni Costituzionali*, 20 aprile 2015) < (Microsoft Word - MORELLI-I principi costituzionali relativi ai doveri inderogabili di solidariet\340 \(FORUM\) \(1\)) (forumcostituzionale.it) > accessed 20 February 2021.

[60] Noberto Bobbio (n 7).

To reach this aim, it is crucial to improve the simultaneous action of three elements: lawfulness, ethics, and robustness. Trust, indeed, is a complex idea, irreducible to just one 'thing'.[61] It is a multifaced concept that relies on multiple factors. Within an ever-changing digital scenario, this principle is inevitably linked to the transparency of new technologies and the systemic measures provided to face security problems and assure that they are always proportional and respectful of fundamental rights. In this perspective, new technologies need a holistic and systemic approach encompassing the trustworthiness of all actors and processes that are part of the system's socio-technical context throughout its entire life cycle.[62]

However, building a trustworthy digital scenario is not easy to achieve. To realise this goal, indeed, the legal experts must be able to understand the 'reasons' of the technicians to identify rules that allow the full utilisation of technologies without compromising common values and principles and, at the same time, the technicians must know the 'reasons' of the jurists to effectively understand the extent of the risks potentially connected to these tools and to intervene proactively in order to minimise them. Without this intense 'dialogue' among sphere traditional separated, technology runs the risk of not being completely reliable.

Furthermore, in some cases a trustworthy scenario also demands the support of solidarity principle, that represents a pivotal element for the society's evolution since it constitutes the bond that connects community members in view of common interests. If the digital instrument is of the public interest, indeed, the less confidence there is in it, the more difficult it is for the spirit of solidarity to emerge.

This is what happened with the European contact tracing experience. The absence of an organised system in terms of healthcare, safeguards of fundamental rights, and protection from technical issues able to assure an appropriate balance between the right to health and the protection of personal data, especially in an emergency scenario, have impacted the decision to use the applications. The resulting attitude of mistrust and opposition has prevented the activation of the vital mutual assistance that should connect community's members. Once the legitimacy of the technological instrument's diffusion had been guaranteed, indeed, the fundamental spirit of solidarity should have emerged. In this way, the tracking app would have really achieved its purpose by contributing to the full realisation of the right to health that imposes in a democratic community 'the overcoming of an abstract individuality, taking place in an individual perspective (claiming to receive care) and at the same time collective ones (protecting public health)'[63].

Therefore, the European experience in digital contact tracing demonstrates that even the diffusion of a technology that could play a vital role in the community's well-being needs to be supported by a strong social cohesion and inserted in a reliable scenario. In the lack of these elements, it is sadly doomed to fail.

---

[61] Maryam Ashoori, Justin Weisz (n 37) 7.

[62] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy Artificial Intelligence* (2019) 6.

[63] Carla Acocella, 'L'epidemia Come metafora della sospensione e Della Compressione delle Libertà Fondamentali. Rileggendo La Peste di Camus' (2020) 1 Diritti regionali. Rivista di diritto delle autonomie territoriali 377.

Trustworthiness and solidarity represent two crucial lessons that stem from the pandemic scenario, and that will have a relevant impact on the future development of the digital evolution in democratic societies. The crisis has shown that technology can represent a considerable instrument to boost the well-being of the community, but at the same time, it is not always able to express its full potential. Within a scenario characterised by the increasing presence of digital tools capable of influencing the exercise of fundamental freedoms and rights and causing new discrimination, democratic evolution requires a further step forward in regulating new technologies. The level of the pervasiveness of these technologies, indeed, requires them not only to be respectful of the principles and values that constitute the pillars of democratic communities but also to be ethically sustainable and robust. They need to put the individual at the centre of innovation, preserving the capacity to consciously act like a human being and member of a community without suffering undue interference from the outside. It follows that, within the digital scenario the protection of fundamental rights cannot be fully realised unless who exploits data for its own benefit realises how dangerous data processing could be and consciously accepts related responsibilities. In this perspective, therefore, 'actors variously involved in the supply chain of personal data are required to leave a passive attitude and to be proactive in order to guarantee appropriate protection of data subjects'.[64] Furthermore, in the case of technologies that impact the evolution of society, they must be reliable to be supported by a widespread animus of social solidarity. Only by promoting these aspects, new technologies will play a decisive role in the democratic evolution, in full compliance with that system of values, principles, and guarantees that constitutes the real essence of a State of law, even - and above all - in times of crisis.

[64] Daniela Messina, 'Online Platforms, Profiling, and Artificial Intelligence: New Challenges for the GDPR and, in particular, for the Informed and Unambiguous Data Subject's Consent' (*Media Laws* 2019, 2) 159.