European Commission

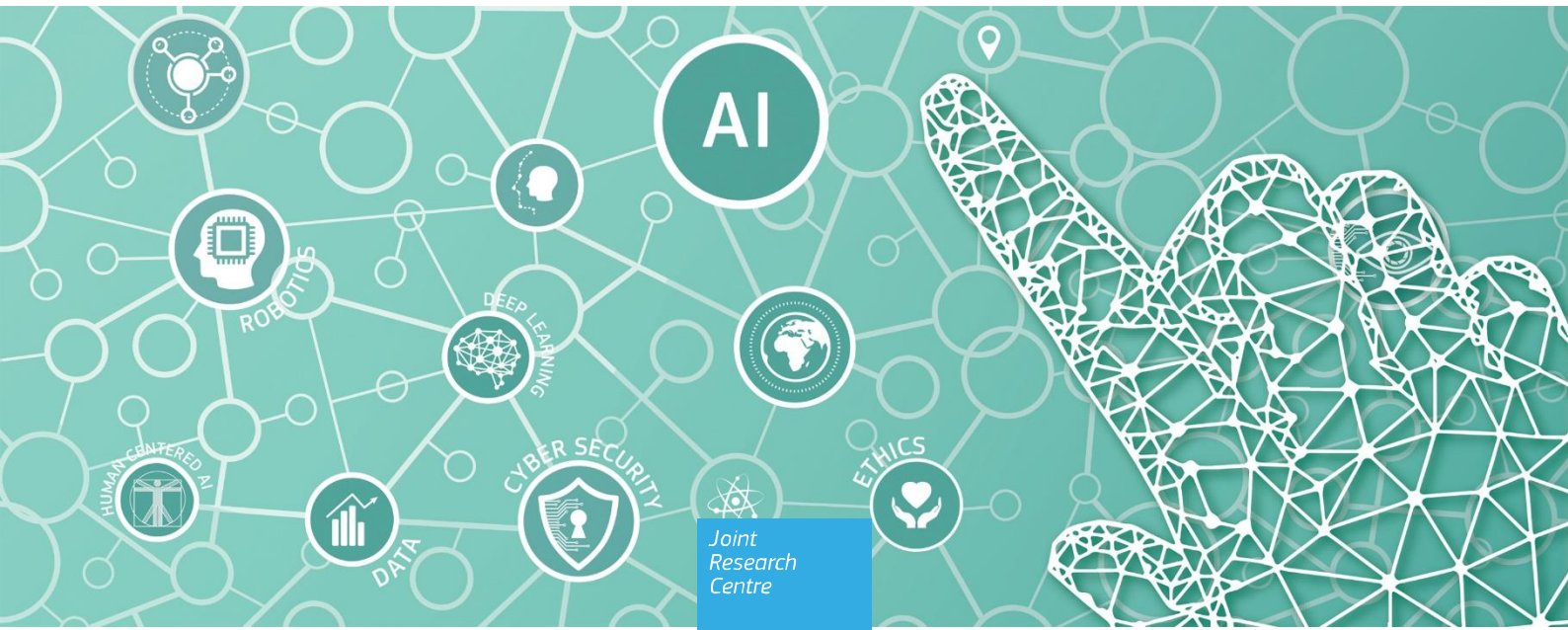
JRC SCIENCE FOR POLICY REPORT

Artificial Intelligence and Digital Transformation: early lessons from the COVID-19 crisis

Craglia M. (Ed.), de Nigris S., Gómez-González E, Gómez E., Martens B., Iglesias M., Vespe M, Schade S., Micheli M., Kotsev A., Mitton I., Vesnic-Alujevic L., Pignatelli F., Hradec J., Nativi S, Sanchez I., Hamon R., Junklewitz H.

2020

EUR 30306 EN



Joint Research Centre

Contact information
Name: Massimo Craglia
Address: European Commission, Joint Research Centre, TP262, Via Fermi, Ispra 21027 (VA), Italy
Email: massimo.craglia@ec.europa.eu
Tel.: +390332786269

EU Science Hub
https://ec.europa.eu/jrc
https://publications.jrc.ec.europa.eu/repository/handle/JRC121305

JRC121305

EUR 30306 EN

ISBN 978-92-76-20802-0 ISSN 1831-9424 doi:10.2760/166278

Luxembourg: Publications Office of the European Union, 2020

How to cite this report: Craglia M. (Ed.), de Nigris S., Gómez-González E., Gómez E., Martens B., Iglesias, M., Vespe M., Schade, S., Micheli M., Kotsev A., Mitton I., Vesnic-Alujevic L., Pignatelli F., Hradec J., Nativi S., Sanchez I., Hamon R., Junklewitz H. *Artificial Intelligence and Digital Transformation*: early *lessons from the COVID-19 crisis*. EUR 30306 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-20802-0, doi:10.2760/166278, JRC121305.

Contents

Abstract

The COVID-19 pandemic has created an extraordinary medical, economic and social emergency. To contain the spread of the virus, many countries adopted a lockdown policy closing schools and business and keeping people at home for several weeks. This resulted in a massive surge of activity online for education, business, public administration, research, social interaction. This report considers these recent developments and identifies some early lessons with respect to the present and future development of AI and digital transformation in Europe, focusing in particular on data, as this is an area of significant shifts in attitudes and policy. The report analyses the increasing use of AI in medicine and healthcare, the tensions in data sharing between individual rights and collective wellbeing, the search for technological solutions like contact tracing apps to help monitor the spread of the virus, and the potential concerns they raise. The forced transition to online showed the resilience of the Internet but also the disproportionate impact on already vulnerable groups like the elderly and children. The report concludes that the COVID-19 crisis has acted as a boost for AI adoption and data sharing, and created new opportunities. It has also amplified concerns for democracy and social inequality and showed Europe's vulnerability on data and platforms, calling for action to address these crucial aspects.

Acknowledgements

The authors are grateful to Alex Zenie, Christine Kriza, Hubert Chassagne, and Claudius Griesinger for their contributions to Section 3 and for reviewing the draft, Anastasios Efstathiou for his contribution to Section 5, and to Chrisa Tsinaraki, Lorena Hernandez, Fabiano Spinelli and Alessandro Dalla Bennetta for their contributions in the analysis of the tracing apps in Section 7.

The authors are particularly grateful to Nicole Ostlander, Carlo Lavalle, Marco Minghini, Nick Nicholson and David Asturio Bofill for their reviews and thoughtful comments that have helped strengthen and sharpen the report.

Authors

Craglia M. (Ed.), de Nigris S., Gómez-González E., Gómez E., Martens B., Iglesias M., Vespe M., Schade S., Micheli, M., Kotsev, A., Mitton I., Vesnic-Alujevic L., Pignatelli F., Hradec J., Nativi, S., Sanchez I., Hamon R., Junklewitz H.

All authors are European Commission Joint Research Centre members of staff except for Emilio Gómez-González from ETSI Universidad de Sevilla, Spain, and Irena Mitton from MITGIS, Croatia.

Executive summary

Artificial Intelligence (AI) is at the centre of an increasing global competition. Europe has recognised the challenge and has been gearing up its policy on AI with major initiatives and ambitious investment programmes. This report explores how COVID-19 is reshaping the direction of technological and policy developments, and what lessons we can learn that may affect the future development of AI and more broadly, the digital transformation.

The **key findings** are that COVID-19 has acted as a **booster**, and as an **amplifier** of potential opportunities and concerns.

As a booster of:

- AI adoption and use in scientific and medical research, and applications like telemedicine, and medical diagnosis,
- Acceptance of robots in the workplace.
- Data sharing practices among commercial companies, and between business and governments
- The switch to online of education, public administration, commerce and business.
- Innovation to cope with the crisis, e.g. in AI methods using existing data to estimate the risk of infection by economic sector.

As an amplifier of opportunities:

- For existing digital companies that adapted better and faster to the lock down (e.g. collaborative platforms, e-commerce, data brokers, cybersecurity)
- For the acceptance of teleworking as part of the normal mix of working arrangements, with potential social and environmental benefits.

As an amplifier of concerns:

- About the potential misuse of personal data collected to respond to the emergency for mass surveillance and reduced democracy.
- About the organised campaigns of misinformation launched to undermine social cohesion and public trust in European institutions.
- About cybersecurity of the European data spaces and applications.
- About the dependency on non-European collaborative platforms, providing valuable intelligence to the platform operators for profiling, targeting, and potential manipulation.

The **most important observation** is that the COVID-19 pandemic, and its response including the lock down and accelerated digital transition, has **widened the gap** between the wealthier and poorer segments in society, hitting particularly hard the more vulnerable groups, the elderly, the young, and people from socially or economically disadvantaged groups.

The **second most important observation** is that in a digitally transformed society, **data** is the core ground on which political, economic, and social battles are fought at all levels from global to local. This includes not just the processes of data collection, integration, management, and use (or misuse), but also the underpinning IT and applications infrastructure, and cybersecurity. **Technological and data sovereignty** are rightly commanding greater political attention in Europe, and the increased cyberattacks and misinformation campaigns which took place during the COVID-19 outbreak as well as our dependency on non-European platforms demonstrate the importance of this attention.

The **initial lessons** we are learning from COVID-19 indicate that the interconnectedness of the challenges requires a strong coordination in the response. Europe can make good use of key instruments such as the European Strategy for Data, the forthcoming Digital Europe Programme, the Horizon Europe research programme, and a Recovery package of unprecedented scale. Connecting these instruments with a particular regard to **strengthening European technological and data sovereignty and reducing the increasing inequalities in society** would address the challenges and exploit the opportunities better, so that the European way towards the digital transformation is more inclusive and supportive of the founding values of the EU. Not just bouncing-back to pre-COVID-19 normality, but bouncing-forward to a more resilient and just society.

1 Introduction

M. Craglia

What lessons can we learn in Europe from the COVID-19 crisis with respect to the future development of AI and digital transformation?

The JRC flagship report on Artificial Intelligence[1] (AI) (Craglia et al. 2018) provided a multi-perspective view of AI from a European perspective just ahead of the launch of the Coordinated Plan on AI in December 2018 (EC, 2018a). The report reviewed the recent developments in AI and situated the position of Europe in the global competitive landscape between the U.S. and China. It explored the ethical debates around the development of AI as well as the legal framework, the supply of relevant skills, the possible economic and cybersecurity impacts, and the need to build resilience in society for the disruptive changes ahead.

The report recognised that we are only at the early stages of the digital transformation of our society, and that within this broader context AI offers many opportunities. To seize these opportunities and reduce the risks we need, as European society including all the stakeholders both public and private, to guide the process of development so that it fosters the ethical and legal principles underpinning European democracies and lying at the base of the European treaties. The report also acknowledged that whilst Europe is well positioned internationally with respect to its research capacities, it needs to ensure it develops a robust computing infrastructure and good quality data to be able to harness the potential of AI for the benefit of Europe.

Since then, the European Commission has adopted the Coordinated Plan on AI in partnership with the Member States to boost public-private investment in AI, develop national AI strategies, foster the diffusion of trustworthy AI technologies and applications, and prepare European society by adapting its learning and training programmes. AI Watch[2], the knowledge service of the European Commission was launched in January 2019 by DG CNECT and JRC to monitor the implementation of the Coordinated plan and assess the adoption and impacts of AI for Europe.

The importance of AI for the future of Europe was recognized at an early stage by the new Commission with President von der Leyen announcing, even as President-elect, that AI would be one of her priorities within the first 100 days of her mandate. Once confirmed as President, the mission letters of Vice President Vestager[3] and Commissioner Breton[4] overseeing the digital portfolios promoted strongly a human-centric and trustworthy approach to AI with an important emphasis on technological and data sovereignty, the importance of which has only grown in light of the recent increased geopolitical tensions between the U.S. and China over technological supremacy and AI.

The commitment towards a European approach to AI has already resulted in the adoption of a Communication in February 2020 on Shaping Europe's Digital Future, including a White Paper on AI launching a broad consultation on a risk-based approach to regulating AI, and a European Strategy for Data establishing a set of European data spaces in key strategic sectors (EC, 2020a, 2020b, 2020c).

---

1 In general terms, Artificial Intelligence (AI) refers to machines or agents that are capable of observing their environment, learning, and based on the knowledge and experience gained, take intelligent action, or propose decisions. The most common applications are machine learning, natural language processing, computer vision and audio processing. For a more thorough definition of artificial intelligence and of its key technologies and applications see Samoili et al. 2020.

2 https://ec.europa.eu/knowledge4policy/ai-watch_en

3 https://ec.europa.eu/commission/sites/beta-political/files/mission-letter-margrethe-vestager_2019_en.pdf

4 https://ec.europa.eu/commission/sites/beta-political/files/president-elect_von_der_leyens_mission_letter_to_thierry_breton.pdf

These policy developments have, like everything else, been affected by the devastating impacts of the COVID-19 virus, which at the time of writing on June 28th reached 10 million confirmed cases and half a million deaths worldwide[5], of which 1.5 million cases and over 176,000 deaths in the EU/EEA and the UK[6].

The crisis has reshaped the direction of technological and policy developments to respond to medical, economic and social emergencies. The boundaries of what European societies considered acceptable in terms of democratic oversight, government intervention and personal privacy have been stretched during the emergency with unknown lasting consequences. The magnitude of the economic and social challenges in the post-COVID-19 crisis often appears daunting, but there are also some opportunities emerging to reset the path of development. As data-driven scientific advice gains prominence, what lessons can we learn in Europe with respect to the present and future development of AI and digital transformation? This report addresses this question from multiple perspectives in line with the original JRC report, with a thread line running through the report focused on data as this is the terrain where we can observe significant shifts in attitudes and policy.

The report is organised as follows: Sections 2 and 3 provide evidence of the increasing attention to AI applications in health, and then focus on the societal impacts of AI in medicine and healthcare in the context of COVID-19. Sections 4, 5, and 6 introduce the tensions in data sharing between individual rights and collective wellbeing, and give examples of how the COVID-19 pandemic has boosted collaboration on matters of intellectual property and data sharing among commercial companies, and between business and government. Sections 7 and 8 focus on the rise of apps for contact tracing as one of the more emblematic examples of a technological response to the pandemic, raising questions on the risk for mass surveillance and loss of democratic control. Section 9 on the other hand, provides a good example of how AI methods can be used creatively on existing official data without trampling on individual rights to support policy, in this case the potential impacts of reopening the economy after the lock down. Section 10 and 11 draw our attention to the resilience demonstrated by the Internet, but also to the dependency on non-European collaborative platforms during the lock down. This dependency adds to the cybersecurity concerns, as the number of cyber-attacks, also deploying AI, increased during the crisis with well-orchestrated misinformation campaigns aimed at undermining social cohesion and trust in the institutions. Section 12 remind us that the impacts of the digital transition during the lock down are increasing existing inequalities, while Section 13 draws the conclusions.

[5] https://coronavirus.jhu.edu/map.html

[6] https://www.ecdc.europa.eu/en/cases-2019-ncov-eueea

2 AI in health

S. de Nigris, M. Craglia, J. Hradec

Access to data is critical to successful AI applications. European health systems are rich in data but exploiting it securely and wisely remains a challenge.

There has been a growing interest in the application of AI in health over the last few years. The COVID-19 crisis has increased the attention even further raising some societal issues which we discuss in Section 3. In this Section we provide some elements of the wider canvas against which the applications of AI in health have to be situated based on the AI Watch report (de Nigris et al., 2020).

Governments in Europe, but also other countries such as Japan and India, are giving AI applications in health a high priority due to factors such as aging population and shortage of health care professionals (McKinsey, 2020). As an example, the national strategies of Belgium, Cyprus, Denmark, Finland, France, Germany, Hungary, Italy, Latvia, Lithuania, Malta, Poland, Spain, Sweden, and the UK all refer to healthcare as one of their priority sectors [van Roy, 2020]. A survey of 200 European AI projects in the public sector (Misuraca and Van Noordt, 2020), found that health-related ones are the third most numerous (35) and, in this cohort, 22 initiatives are geared towards increasing performance and effectiveness of such services. Furthermore, in a survey of 18 European countries, the health sector ranked first as the policy domain to prioritize in the future (Misuraca and Van Noordt, 2020).

Whilst the level of interest and the number of pilot projects and experimentations are growing, the level of diffusion is still relatively low and most projects are just at initial stage to "test the water". As an example, a survey[7] by the Observatory on Digital Innovations in Health of the Politecnico di Milano in 2018 of practitioners and managers of health institutions in Italy revealed that only 20% of the respondents identified AI as a priority and that the overall level of investment in AI was rising but was still very low (€ 7m) against an overall expenditure for digital innovation in health of some € 1.4 bn. in 2018.

Public sector organisations are understandably more cautious in adopting AI, while there is greater interest in the commercial sector as detected by a recent survey of almost 10,000 companies in Europe, mostly SMEs, carried out on behalf of DG CNECT in 2020 (IPSOS, 2020). The key findings are that across all sectors, including health, 42% of companies are already using one or more AI solutions, with an additional 18% planning to adopt within two years, while the remaining 40% indicated that they have not implemented or have not yet intention of implementing AI-based solutions in the near future. We see therefore a high level of interest but with a significant minority yet to be convinced. This is important to ground the discussion which is often characterised by hype and inflated expectations (Topol, 2019a).

Another important consideration is that in the health sector where clinical AI applications are perhaps the most visible, applications in other areas such as Administrative, Financial, and Operational are often at a more mature stage of development including for example chatbots to support customer enquiries and software to facilitate patient management (AHA,2019b).

2.1 Highlights from the scientific literature

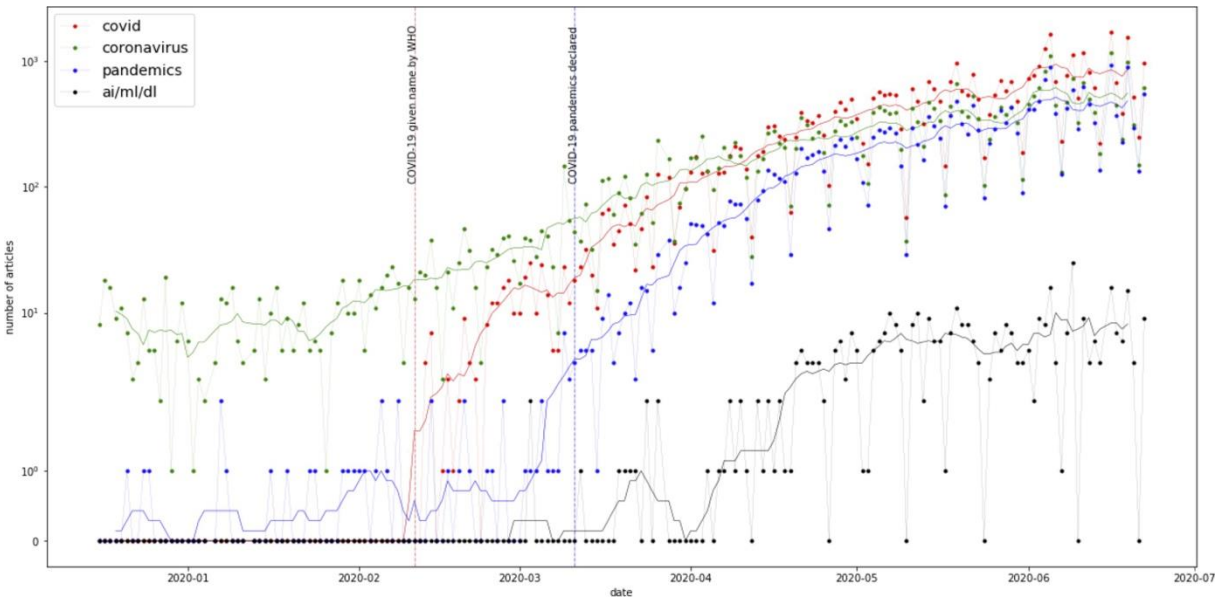
To assess the increased attention in the medical literature to COVID-19 and AI, we have searched for AI or COVID related papers among the 30 million abstracts, keywords, and citations of the papers published since

7 https://www.osservatori.net/it_it/osservatori/comunicati-stampa/spesa-sanita-digitale-italia

2010 in PubMed, the world largest and most up-to-date source of medical scientific articles. Updated several times a day it covers not only the United States but also most other countries for articles published in English. Whilst prior to 2010 AI did not have a visible presence in the articles analysed, since the beginning of 2020 we started to see an upward trend in AI-related papers trailing by about a month the papers discussing COVID, Corona virus and pandemic as shown in Fig. 1.

The graph clearly shows the trend in the number of AI applications related to COVID-19 to be correlated with the interest of the scientific community in the COVID-19 itself. AI seems to become a part of the standard scientific toolbox within the medical community. Being at an early stage however, many studies seem to be affected by problems related to difficulty in accessing the relevant data, small samples, biases in the data or inconsistent labelling of the training datasets (Topol, 2019a, Panch, 2019, Ghassemi, 2019). To counter data paucity, dataset sharing is a desirable practice and, in this regard, the COVID-19 emergency already catalysed the emergence of dedicated platforms. Data Against COVID-19[8], for instance, is an exemplary initiative matching data, brought by practitioners, and expertise, brought by data scientists.

Figure 1: Number of publications on AI and COVID-related topics Jan-June 2020



Source: JRC with data from PubMed

2.2 National and European initiatives

Recognising that access to data is a fundamental pre-requisite for the successful application of AI techniques, many initiatives are under way in Europe both at national and European level to leverage the great wealth of data of the European health systems (McKinsey, 2020).

France, for example, has seen the creation of the Health Data Hub (HDH, 2018) and, in 2016, of the SNDS (Système National des Données de Santé) for the exploitation of medical data. The SNDS tries to overcome the traditional fragmentation of existing datasets[9]: It collates data from medical prescriptions, financial data from the hospitals and causes of death from different systems. Furthermore, it plans to incorporate the regional databases concerning handicapped citizens and, finally, a sample of private insurance reimbursement data (HDH, 2018). This wealth of data, following some 60 million French citizens, is not, however 'AI ready' (Polton, 2018): such datasets were conceived for administrative purposes, and thus require additional work to extract clinical information. Nevertheless, the SNDS is a formidable data source, spanning over 20 years.

The use of these datasets is regulated by the Health Data Hub which grants access to the anonymised data, processing the requests and assessing their eligibility together, if needed, with the CNIL (Commission Nationale de l'Informatique et des Libertés). This lightweight approach produced, during the first year of operation (2017-

8 https://www.data-against-covid.org/
9 https://www.indsante.fr/fr/les-composantes-du-snds

2018), an average of 70 days waiting time for approval when vetting from the CNIL was required (HDH, 2018), which represents a considerable improvement from the 3-6 months waiting time in the previous system.

At the European level, the European Commission already identified in its communication on AI (EC, 2018b) health as a sector where Europe has world-leading industry and a wealth of industrial, research, and public sector data. The richness of this data is the focus of the European Strategy for Data that envisages the establishment of several thematic data spaces, of which one on health to support "advances in preventing, detecting and curing diseases as well as for informed, evidence-based decisions to improve the accessibility, effectiveness and sustainability of the healthcare systems" (EC, 2020c). The strategy builds on the 2018 Communication on eHealth (EC, 2018c) and envisages both sector-specific legislation including greater access to and portability of personal health data by citizens, and dedicated infrastructures and analytical tools in addition to supporting the development and interoperability of national electronic health records.

These are excellent initiatives that need to address the formidable challenge of developing secure pools of good quality and interoperable data accessible for research and development. Health data is sensitive and often personal data may be needed to draw the appropriate samples even if then no personal data is need for the analysis. Intelligent technological and administrative solutions are therefore needed to work within the boundaries of our data protection and legal framework and yet foster the collaboration between data providers and users and arrive at results that are both safe[10] and timely

As shown, the landscape is evolving rapidly and the COVID-19 crisis appears to have added significant urgency to the applications of AI in this sector. The next Sections explore some of the more promising areas of applications and highlights a number of societal issues these raise.

[10] In this respect, the report on safety and liability of AI (EC, 2020m) explains how new technologies challenge the existing frameworks and in what way these challenges could be addressed. Healthcare is identified as a sector that may require particular attention because of the complexity of interacting actors in applications where partially automated AI systems will support human decision-making.

3 Societal impact of Artificial Intelligence in Medicine and Healthcare: key relevant aspects in the coronavirus pandemic

Emilio Gómez-González and Emilia Gómez.

AI can be of great benefit to medicine and healthcare but also carries a number of risks, often related to how the data it needs is collected and used.

As indicated in the previous Section, the advent of Artificial Intelligence (AI) into Medicine and Healthcare is an ongoing revolution combining the potential of disruptive advances and extraordinary benefits with many unknowns and questionable ethical and social issues.

From early 2020, the devastating consequences of the worldwide spread of the SARS-CoV-2 (corona)virus and the associated COVID-19 disease indicate that the post-COVID-19 world is likely to be different at all societal levels, even if the pandemic 'comes to an end' like previous outbreaks of similar coronaviruses (e.g. the SARS-CoV-1 outbreak between 2002 and 2004). In the current situation there are still many uncertainties. They range from clinical questions, short and long-term effects, potentially associated ailments, new waves of contagion and mutations, to economic and cultural changes, alterations in citizen's daily lives and individual and social rights. In this context, the European Union (EU) faces significant challenges from the health, economic, political and societal points of view.

An extensive structured review by the authors (Gómez-González & Gómez, 2020) of over 600 references shows that AI can play a key role in the fight against the pandemic and in the shaping of the post-COVID-19 world at all levels of society. The coronavirus pandemic has fostered AI applications, particularly in medical and clinical areas, as AI-mediated technologies lay at the main core of the response to the worldwide health crisis. There is a growing arsenal of AI-related developments addressing the coronavirus pandemic from many different approaches. Some of these applications can be listed as follows:

- Data-driven knowledge extraction techniques are being exploited in a variety of areas, from direct medical diagnosis, epidemiology, and management and optimization of clinical and logistical pathways. In public health management, the integration of heterogeneous sources of information –including data from personal devices and medical records– with machine learning techniques offers great potential for the detection of patterns and the prediction of future scenarios, and the prevention and forecasting of disease outbreaks and routes of spreading.
- Computer vision techniques already developed for medical imaging are being adapted for image-based diagnosis of coronavirus related features (e.g. through the analysis of chest scans).
- Massive analysis of genetic data is being employed to speed-up the development of vaccines and treatments.
- Data from social media and community-generated platforms is being used to monitor the spread and the public perception of the disease.
- Robotics, telemedicine and virtual doctors are adopted to replace human-human interaction in contaminated environments. Companion robots, for instance, help to reduce the 'human gaps' created by physical and social isolation.
- AI-mediated tools are being used to detect and fight misinformation and fake news.

As recently pointed out in the analysis of AI in Medicine and Healthcare (Gómez-González & Gómez, 2020), applications in these fields become a double-edged sword in the current health emergency: while providing strong benefits and potential to fight the disease, there are controversial societal aspects to be considered and this balance has been strongly affected in the last few months. In a declaration issued at the beginning of 2020, the World Health Organization also highlighted some of these worrying issues as 'urgent health challenges for the next decade' (Ghebreyesus, 2020). We present this tension and the changes it is generating in the societal view of eight AI-related topics that we consider most relevant in the context of the COVID-19 crisis.

3.1 The boost of telemedicine

Telemedicine has experienced a strong boost during the COVID-19 health emergency because of several significant contributions. On the one hand, telemedicine can reduce the number of people visiting medical services, from general practitioners to hospitals, therefore decreasing risks of contagion and spreading of the disease. On the other hand, it serves to optimize the use of medical resources (e.g. imaging scans, lab test) in 'common pathologies', freeing resources for the priority of the pandemic. Since there are patients who fear visiting clinical facilities, telemedicine is also helpful to reduce incidences related to certain diseases which can be managed remotely. Several current technologies have a strong potential for telemedicine that is not yet fully exploited: from wearables and internet-of-things (IoT) devices for health monitoring, to virtual reality environments for human-human interaction.

However, there are also challenges in using telemedicine in the current pandemic. Among them, there is a need for physicians to adapt to a new scenario without the physical presence of the patient. In addition, there is a risk of individuals being remotely guided to perform certain medical procedures that should be carried out by a trained professional. The lack of direct contact with the patient is of particular relevance for a correct diagnosis in many clinical areas, since physicians extract important information from physical contact (e.g. through palpation) and from visual perception (e.g. gait disturbances, skin appearance). The current impossibility of tactile, haptic feedback is an active drawback to be solved for remote diagnosis platforms and tools.

3.2 Benefits and risks of data-driven algorithms

Data-driven algorithms have been widely exploited to fight the pandemic in four main different areas:

1. medical diagnosis based on processing tests and imaging scans (Baraniuk, 2020) and on the analysis of data from personal devices (mobile phones, wearables) (Menni et al., 2020) (Jacobs, 2020);
2. epidemiological studies to predict pandemic outbreaks, temporal and geographical spread and evolution;
3. enhancement of societal and individual welfare, through social networks and recommender systems to promote social bonding, connect isolated patients and provide recommendations such as personal trainers, newspapers and health support tools; and
4. clinical management of the pandemic: data-driven methods support the optimisation of medical resources under very high pressure (Intensive Care Units, ICUs), logistics (Hao, 2020a), help to generate scientific evidence from multiple data sources, and act as a decision support tool for treatments and the use of equipment.

Some of these applications show extraordinary benefits in terms of efficiency, and are being adopted to fight COVID-19. However, we shouldn't forget the related social and ethical concerns as widely discussed in recent analyses (Gómez-González & Gómez, 2020). Among them, the lack of standards for evaluation and international coordination, and the issues of data selection and curation for training of systems. 'Small', biased datasets used to build and train models may have deep consequences in their performance in real-world scenarios. Even well-established AI tools in other areas present abnormal figures when dealing with new, untested behavioural patterns of people under severe restrictions for many daily activities (Heaven, 2020). The consequences of algorithmic bias in health care need to be carefully assessed, especially regarding their detrimental impact on equity, for example as a consequence of racial and gender bias. In the context of a health emergency, the urgency to find solutions may produce a 'reduction of controls'. What are proper benchmarking strategies? Can we trust new, not well-established systems? Should an AI tool for clinical applications be evaluated by a potentially error-prone human or by another potentially more effective autonomous system? (Gómez-González & Gómez, 2020) (McKinsey & Company, 2020).

Given the state of the art, we cannot yet trust an algorithm on its own to support decisions influencing human lives (e.g. deciding on who gets admitted to intensive care units, or taking life or death decisions (Scudellari, 2020)). Such 'limit' to AI applications presents many challenges in terms of human supervision and oversight that still need to be addressed.

3.3 Robotics: from fear to new roles and acceptance

The public perception of robots, seen by many as unwanted substitutes of humans and 'job takers' in the pre-COVID-19 situation, has drastically changed during the current health emergency. Automated machines (robots, drones) were part of equipment used by human physicians (e.g. robotic surgery assistants and devices (Graur et al., 2018)), already performing some relatively autonomous activities in hospital and clinical facilities. However, they were mostly restricted to dangerous tasks (e.g. the disinfection of facilities with toxic chemicals or high-energy ultraviolet lights) and repetitive, physically demanding duties (e.g. displacement or storage of equipment). 'Companion robotics' also started to be tested in certain clinical environments (Shishehgar et al, 2018), proving to be very useful, combined with other assistive devices, to provide human-human communication in situations of physical isolation

Nevertheless, in the post-COVID-19 context, autonomous machines are now seen as useful 'operators' which can replace humans in many other types of tasks (Thomas, 2020). Some of them are close to law enforcement (e.g. monitoring the social distancing or the quarantine orders (Su, 2020)) but others include activities that were traditionally considered to need the 'human touch' but have now become too risky for humans. They include patient control and triage, temperature measurements, and the delivery of tests and medication in virus-contaminated environments. Such new roles may evolve into extended care of functionally-impaired patients (e.g. residents in nursing homes). The change in the public perception of robotic platforms in the COVID-19 context can drastically boost their adoption in many areas in the near future.

3.4 Personalised medicine

In the fight against the COVID-19 pandemic it is critical to improve our understanding of the mechanisms of immunity, how human cells battle the virus and how drugs and vaccines may interact. Artificial Intelligence lies at the core of massive data analysis employed to decipher the genetic features required for successful diagnosis and treatments in the paradigm of 'precision medicine', while advanced data integration and mining call for the concept of 'extended personalized medicine' (Gómez-González & Gómez, 2020). These technologies bring in new powerful tools in the fight against COVID-19 (Wakefield, 2020).

Computational biology and virology accelerate the search for treatments and vaccines exploring drug candidates, risk factors and the prediction of side effects (Health Europa, 2020). AI-enabled tools allow for advanced computational models (Biozentrum, 2020), identifying genetic signatures and studying their interaction in highly complex biochemical and biological environments. Real experiments can be strongly boosted by numerical simulations, saving time and resources in the search for new, effective therapies. Patterns of contagion in cells and the analysis of antibody binding sites can be analysed trying to determine which regions of the viral proteins can be more effectively targeted by drugs and vaccine candidates (Fast & Chen, 2020). However, important questions also persist. Personalised medicine aims to develop targeted treatments at the individual level while currently established methodology to generate and accept 'scientific, clinical evidence' relies on group averages and population statistics (Gómez-González & Gómez, 2020). New methodological, testing and regulatory tools are needed.

3.5 A difficult balance: individual rights vs public health

Living a global, world-wide public health emergency, many countries have restricted individual rights implementing such measures as imposed quarantine, confinement of population and social distancing. In this context AI-mediated technologies have proven to be key elements for the control of individuals (Kim, 2020) and societies. They include tools for massive digital surveillance (e.g. computer vision techniques for facial recognition, traffic cameras for population monitoring, temperature monitoring (Schectman et al., 2020) (Lin & Martin, 2020)), merging clinical and social data (Mickle et al., 2020) (Timberg & Harwell, 2020) to provide information to health authorities, the creation of mobile apps for evaluating the exposure of individuals to the virus and digital contact tracing (Kahn & Hopkins, 2020), the programming of algorithms for citizens disease-tagging, even to evaluate the return to work places (Horowitz, 2020) (Rossignol & Lenoir, 2020), and the use of

wearables to control social distancing (e.g. wristbands (Doffman, 2020) or the app developed by the Robert-Kockh Insitute[11]).

Although such applications of technology are justified by authorities and governments as required to fight the pandemic in a fast and effective way (Chandran, 2020), many controversial aspects arise as related to the limitation of individual rights in democratic regimes during peacetime. Among them, privacy and data-protection concerns are increasingly being raised by scientists (Joint Statement on Contact Tracing, 2020) (Bengio et al, 2020), general media (The New York Times, 2020) and even by European Governments (Albergotti, 2020) and the European Union Agency for Fundamental Rights (European Union Agency for Fundamental Rights, 2020). This agency warns on the effects of an uncontrolled use of technology on individual rights, from privacy to freedom of movement and assembly. It also highlights that the use of data-based technology to overcome the pandemic should safeguard those rights, and raises the question of establishing limits on the time and scope of the extraordinary measures taken by the EU Member States. Many additional questions emerge or need to be revisited in these extra-ordinary times (Gómez-González & Gómez, 2020): Should personal (health, location, contacts) data be anonymised or erased after the pandemic is controlled? Can they be made available to private companies (e.g. for medical research?). In June 2020, considering their low infection rate, but in the midst of a controversy between health and data protection authorities, Norway announced halting its app for track and trace data collection, and erasing all the recorded information, on privacy concerns. Should others follow? (Reuters, 2020) (for further discussion on contact tracing apps and their implications see Sections 7 and 8).

3.6 Psychographics and the control of information

Psychographics is a recently coined term that refers to the extraction of psychological and cognitive attributes of humans as related to their opinions and attitudes, including cultural, religious and political, and the analytical characterisation of values, habits and other figures well beyond those data included in common demographics and economic statistics (CB Insights, 2020b). In recent years, it has become a new tool and target for social influence and control, from tailored advertising and nudging consumer's habits to manipulating political orientation, and it is linked to new modalities of 'digital aggressions' and even (cyber)war (CB Insights, 2018). Psychographics relies on AI-mediated massive data collection and analysis and, in the current situation generated by the coronavirus pandemic, it is at the center of the already mentioned boost of data gathering and the struggle for the control and use of information.

In a context of population confinement or with many restrictions to physical displacement and direct social interaction, digital tools for communication and social networks become preferred channels for massive exchange of data including those related to health in any format files, voice, video and in real-time individual and group interactions. In many cases, they rely on very loose security and privacy settings, being therefore open to 'listening' by external parties and to receiving inputs under many appearances. Moreover, these platforms are almost exclusively non-European (see also Section 10).

Recent studies show that the analysis of data in social media allows for evaluating the psychological situation of societal groups and even the emotions of individual people and entire populations in real time (Jaidka et al, 2020). Simultaneously, massive amounts of data about health status, including genetics, physical location, tracing of contacts and many other topics are being collected and processed. This brings to the public debate some undiscussed, controversial issues about 'old and new' concepts, from data property and inheritance (who is the owner of health, genetic data when a person dies?) to AI-mediated technologies for the common good (in Medicine and Healthcare) and the role of regulation and legislators. How will the collected information (of individuals) be used after the pandemic? Might it be used for 'monitoring' political opponents? Or to 'induce' social demands and changes in certain environments?

3.7 The control of information. The risk of an additional 'infodemic'.

Health-related information is critical at the time of pandemics. The extraordinary capabilities of AI-mediated tools can multiply the beneficial effects of trusted, reliable information but also expand the negative consequences of misinformation (wrong information) and disinformation (purposely false, misleading information) spread in society. A specific term ('infodemic') has been defined as the combination of 'information' and 'pandemic' to describe this new risk (Richtel, 2020; Mooney and Juhász, 2020).

Certain relatively obvious negative uses of the AI tools relate to the online, web-based promotion of unproven even clearly harmful remedies for the coronavirus disease and to the 'digital updates' of health scammers

[11] https://play.google.com/store/apps/details?id=de.rki.coronadatenspende&hl=en&gl=de

(Gómez-González & Gómez, 2020) (Popular Science, 2020). Their extent and impacts, including human lives, of such scams (Spring, 2020) led the United Nations Educational, Scientific and Cultural Organization (UNESCO) to issue a warning stating that 'During this coronavirus pandemic, 'fake news' is putting lives at risk' (UN News, 2020) and the European Commission to step up its work addressing health concerns and warning consumers against rogue traders (European Commission, 2020d).

The motives for spreading malicious digital content about the virus and COVID-19 disease to citizens can be many, and include the intention of generating social divide and discontent (Hao, 2020b), disturbances (Cimons, 2020), cyberespionage and cybercrime (Canadian Centre for Cyber Security, 2020), and bioterrorism (Council of Europe, 2020) (see also Section 11)

The heterogeneous mixture of real-world concerns and the multitude of false, misleading information available throughout the Internet creates a strong demand for transparent, reliable information from public authorities about the pandemic itself and explaining the need for, scope and duration of the controversial measures applied during the crisis. Some of the new threats derived from disinformation related to the COVID-19 pandemic have been identified by the European Commission as instigated and supported by foreign state actors opposing the basic pillars of the European Union, and a definite response has started towards a stronger and more resilient EU (European Commission, 2020e). There is an essential role for governments to provide the population with reliable information, avoiding the spread of fake news, misinformation and disinformation, while keeping the fundamental principles of individual and social freedom

3.8 New opportunities for AI.

The current health emergency has generated novel opportunities for AI technologies in many different contexts and unexpected applications have emerged. Some relate to monitoring of physical distancing of people in public spaces, from streets and commercial areas to recreation spaces, even in natural environments (parks, beaches). Other AI-mediated tools play new roles in addressing needs related to healthcare and wellbeing as meditation apps (Cummins, 2020) to reduce stress and anxiety, particularly of patients and caregivers.

Moreover, AI-based technologies offer a strong way forward to explore new methods to fight this and, perhaps, other potential pandemics. Innovative approaches include diagnostic tools based on Internet searches of symptoms or the analysis of voice and sounds (Lubell et al., 2020), and imaging techniques to detect contaminated surfaces and reduce the risks of contagion. Within an international push to promote research and innovation at all societal levels (CB Insights, 2020a) and a number of expanding platforms to foster international cooperation in clinical, scientific, and technological advances to fight the pandemic, Europe is playing a leading role in many of them (European Commission, 2020f) (ELLIS Society, 2020)

3.9 Conclusions

The COVID-19 crisis has created new needs and scenarios at all levels of society, and will produce some paradigm shifts with significant changes in daily life. The development and adoption of AI-mediated technologies has boosted many areas related to Medicine and Healthcare, and we need to take advantage of their benefits, carefully navigating the balance with the associated risks and the expected societal impact that they will bring. As the way data is generated, collected, analysed and used is central to many issues we have highlighted in this Section, the next one discusses some of the economic aspects of access to private data.

4 Some economic aspects of access to private data for use in the COVID-19 crisis

B. Martens

COVID-19 shifted the balance in data sharing from individual rights towards the public good.

The COVID-19 crisis illustrates how data can often have social value that exceeds the private value that persons and firms can extract from it. Pooling of contact and location data can be useful for the management of public health policy responses to the crisis. At the same time, individuals have legitimate rights to data protection under the EU General Data Protection regulation (GDPR) (EC, 2016) and may prefer not to participate in data pooling schemes.

Economists have estimated the gap between the private and social cost of COVID-19 infections. For the US economy (Bethune and Korinek, 2020), the private cost of a COVID-19 infection is estimated at $80k while the social cost is around $286k. This wide gap provides a stark illustration of the social desirability to reduce freedom in private behavioural choices, through social distancing and confinement measures, to avoid high social costs. Mitigation policies also raise equity concerns because of strongly diverging interests between age groups (Glover et al, 2020). How and to what extent to bridge that gap is a moral, cultural and political choice for society, not an economic choice. Individual liberties, including privacy rights, are derived from fundamental human rights, not from economic considerations. A society that emphasises individual liberties will therefore put fewer restrictions on individual freedoms and have more tolerance for a gap between private and social costs. A society that emphasises collective and social values will put more restrictions on individual freedoms, possibly including data privacy rights, to the point where private and social costs are equalised. Economics can accommodate both societal choices: The Pareto social welfare criterion emphasises private freedoms. Social welfare can only be increased to the point where no individual suffers a private cost from public policy measures. The Kaldor-Hick social welfare criterion emphasizes social welfare and accepts policy measures that reduce private welfare provided the overall social benefit that it produces for society could "theoretically" compensate the private losses. However, some researchers argue against the negative trade-off between privacy and social welfare goals (see for example Milusheva, 2020 and Cho, Ippolito and Yu, 2020).

The report of the Expert Group on B2G data sharing (EC, 2020g) discussed many examples where private data sharing with public policy institutions, including health data, would be "in the public interest" or social welfare enhancing. The report advocates voluntary data sharing and stops short of recommending mandatory data sharing. An economic case for mandatory health data sharing could nevertheless be made in the case of data market failures, for example when individuals have no incentive to voluntarily share useful data. According to the European Commission's "Better Regulation Guidelines" (EC, 2017) regulatory intervention is justified in the case of market failures and social welfare concerns, and the European Commission's "Data Strategy" (EC 2020c, p 13) advocates voluntary data sharing but where appropriate compulsory sharing can be introduced in specific circumstances of market failures. Some EU Member States have already put in place a legal framework for mandatory health data sharing to overcome these market failures, with adequate data protection measures consistent with the GDPR. This is the case for example of Finland that adopted a law in 2019 that makes it mandatory for private and public health service providers to pool their patient data on a government server[12].

[12] https://stm.fi/en/secondary-use-of-health-and-social-data

Various projects are under way at EU level and in EU MS that seek to use personal data for COVID-19 crisis management. A first type of project collects mobile phone data to monitor mobility and population movements[13] (see Section 6). The added value of aggregation across EU MS for epidemiological modelling resides in the comparison of country experiences with regard to different mitigation policies. A second type of project seeks to build contact tracing apps for smartphones to trace exposure to infected individuals (see Section 7). Notwithstanding their limitations, these projects show how a major international crisis like COVID-19 can quickly recast the terms of the debate on sharing data between public sector, the commercial sector and civil society in ways that did not seem possible before. Whether these new possibilities will survive beyond the crisis is an open question.

[13] Mobile phone operators do not transmit the original location data for each individual user but only an aggregate dataset. These applications of mobile phone data are not new. Many mobile phone operators sell anonymized and aggregated data for commercial purposes, at a price.

5 Intellectual property considerations on data sharing for AI COVID-19 related tools

M. Iglesias

The legal framework for data is complex but COVID-19 has shown excellent examples of voluntary sharing of data and intellectual property.

Beyond privacy, the sharing of data may also have intellectual property (IP) and other legal implications. Recent initiatives have been launched to encourage the pooling and sharing of IP to accelerate the discovery of treatments or vaccines, to cope with the shortage of supplies and/or to ensure that cures reach all those in need, globally, quickly and at affordable prices. At the International level, the WHO[14], the Medicines Patent Pool and other public actors[15] are discussing the creation of technology pools to share knowledge, IP and data to ensure global equitable access to medical technologies. The industry has also taken steps to increase collaboration on IP sharing and permissive licensing. The Open COVID Pledge has made available licences that allow free, temporary access to patents, copyrights and other IP rights. The pledge has been endorsed mostly by big IT companies and universities. In a similar vein, a number of innovators have renounced the enforcement of their rights, disclosed their relevant know-how, or agreed to share their IP under flexible licensing. Within this context, some stakeholders have called for open access to publications and data, as well as for affordability clauses, to apply to the results of projects funded by public money. The Commission is exploring ways to secure open access to data, and facilitate timely and equitable access to the results of EU funded COVID-19 research projects[16].

The rapid sharing of scientific and research data, in particular of genome data has greatly supported research efforts to fight the outbreak (Guilou, 2020). Other efforts towards open data sharing are the early Wellcome (2020) statement on sharing research data and findings relevant to the novel coronavirus (COVID-19) outbreak, the EC COVID-19 Data Portal[17] allowing researchers to upload, access and analyse COVID-19 related reference data and specialist datasets, or, in the US, the CORD-19 COVID-19 Open Research Dataset[18], that makes available an extensive machine-readable coronavirus literature collection for text and data mining.

At the regulatory level, international and national laws allow for compulsory licences for patents, that under certain conditions and against a fair remuneration allow making use of inventions without the rightsholder's authorisation. Some countries have recently invoked or accommodated their laws to ensure fast track procedures to make use of this exceptional regime if needed. Overall, compulsory licensing is generally perceived as a last resort. As highlighted in the AI flagship report (Craglia et al. 2018) the legal regime related to the access and use of data is intricate. Data as such is not protected by IP, although, when certain circumstances concur, IP protection may be triggered: this is the case of the *sui generis* right of database

[14] Last May, the WHO and Costa Rica have launched the COVID-19 Technology Access Pool (C-TAP), to share knowledge, IP and data necessary for COVID-19.

[15] https://japan-forward.com/editorial-japan-should-lead-global-effort-to-make-covid-19-vaccine-available-to-the-world/

[16] Open access to research data is recommended in Horizon 2020, and is even mandatory for certain projects. H2020 projects working on COVID-19, SARS-CoV-2 and related topics have been urged to provide immediate open access to research outputs, https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/oa-pilot/h2020-guidelines-oa-covid-19_en.pdf. The second call for expression of interest on COVID-19 research published in May requires the beneficiaries to license results on a non-exclusive basis and at fair and reasonable conditions, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/sc1-phe-coronavirus-2020-2a

[17] https://www.covid19dataportal.org/ This portal is the primary point of access of a platform being set up by the European Commission and the and EMBL's European Bioinformatics Institute (EMBL-EBI), together with EU Member States and research partners such as ELIXIR. The European COVID-19 Data Platform will enable the rapid collection and comprehensive data sharing of available research data from different sources for the European and global research communities.

[18] https://www.semanticscholar.org/cord19

makers, the protection granted to trade secrets, or the exclusivity rights to clinical data. No compulsory licences are explicitly foreseen for the *sui generis* right on databases. Although new changes brought by the Directive on Copyright in the Digital Single Market introduce more flexibility in the way data can be used (allowing for text and data mining under certain conditions), the issue of access was not in the scope of the Directive.

During recent years, there has been lot of discussion on the legal regime of access to data and the most appropriate framework to ensure an agile data economy. As discussed in Section 2, access to good quality data is essential to develop appropriate and trustworthy AI applications. For this reason, the recent European Strategy for Data (EC, 2020c) establishing common data spaces including one for health is important. The strategy also envisages possible legislative actions to provide incentives for horizontal data sharing across sectors. Either through licences and agreements for voluntary sharing, or through compulsory sectorial or horizontal regimes, data sharing mechanisms need to consider the multiple legal dimensions that may be attached to the data, as well as the appropriate safeguards to ensure that the legitimate interests of the parties concerned are preserved, including provisions on allocation of rights on the potentially protectable results derived from insights obtained from these data. Ultimately, in case of access to data to fight a public health emergency, the interest of society for an efficient and rapid response raises additional challenges.

6 B2G data sharing at the time of COVID-19: Lessons learned from working with Mobile Network Operators

M. Vespe

COVID-19 shows that companies can set aside their concerns for commercial confidentiality and share data securely to fight the emergency.

In April 2020, the European Commission wrote to the Mobile Network Operators (MNOs) requesting access to anonymised and aggregate mobility data to help fight COVID-19. This marked the beginning of an unprecedented B2G data sharing initiative involving about 20 operators across Europe, with the aim of covering EU Member States with at least one MNO. Given the fast development of the pandemic and the scale of the crisis, MNOs agreed to share data on the basis of the letter, which at this stage replaces a formal agreement with the European Commission. Nevertheless, given the commercial sensitivity and privacy concerns, the Commission committed to put in place security and de-anonymisation safeguards, as well as non-disclosure and data retention measures.

The data request was designed to give insights into mobility, providing input to epidemiological and economic models to understand the dynamics of the spread, the impact of containment measures on mobility and on the reproduction number of the virus (EC, 2020j). The initiative is ultimately expected to inform de-escalation strategies as well as provide forecasting capacity for future re-escalation policies to address prospective second waves of the virus. Nevertheless, it is the European scale of the initiative that will allow the understanding and sharing of best practices across countries, understanding what mobility policies are the most effective to fight COVID-19. The level of granularity of the data, and the attributes that can be captured through them, will provide the European Commission with the possibility of a transparent tool for obtaining indicators specifically designed to meet the needs of JRC researchers, the ECDC, EC policy makers and Member States[19].

The unique nature of the initiative lies not only in its geographical scope, but also in the relatively rapid and in many cases unconditional support offered by the companies. Thanks to continuous dialogue with the Commission, MNOs have shown concrete interest in being active and supportive, irrespective of the different levels of maturity in producing the required data; some were already collecting and delivering similar data to National authorities, others had to develop ad hoc processes to be in a position to respond to the data request.

This initiative could result in speeding up future B2G processes as it potentially shows how actors at the interface between the private sector, science and policy can play a key "trusted intermediary" role in ensuring that the use of data takes place responsibly and is aimed at effectively responding to pressing policy questions. Based on the results obtained, this initiative could also help to simplify the use of private sector data for policy in a systematic way, providing concrete channels to the private sector in providing support to address societal issues.

[19] https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/european-roadmap-lifting-coronavirus-containment-measures_en

7 Shifting sands in data gathering: COVID-19 and contact tracing apps

S. Schade, M. Micheli, A. Kotsev, I. Mitton

Governments need to earn citizens' trust and account for inequalities in access and use of technologies to develop effective digital solutions.

This section identifies some of the key features of COVID-19 related mobile applications (apps) and presents a broader reflection on the shift in perception and policy actions on surveillance/tracking, privacy, and personal data sharing and processing, complementing other Sections of the report.

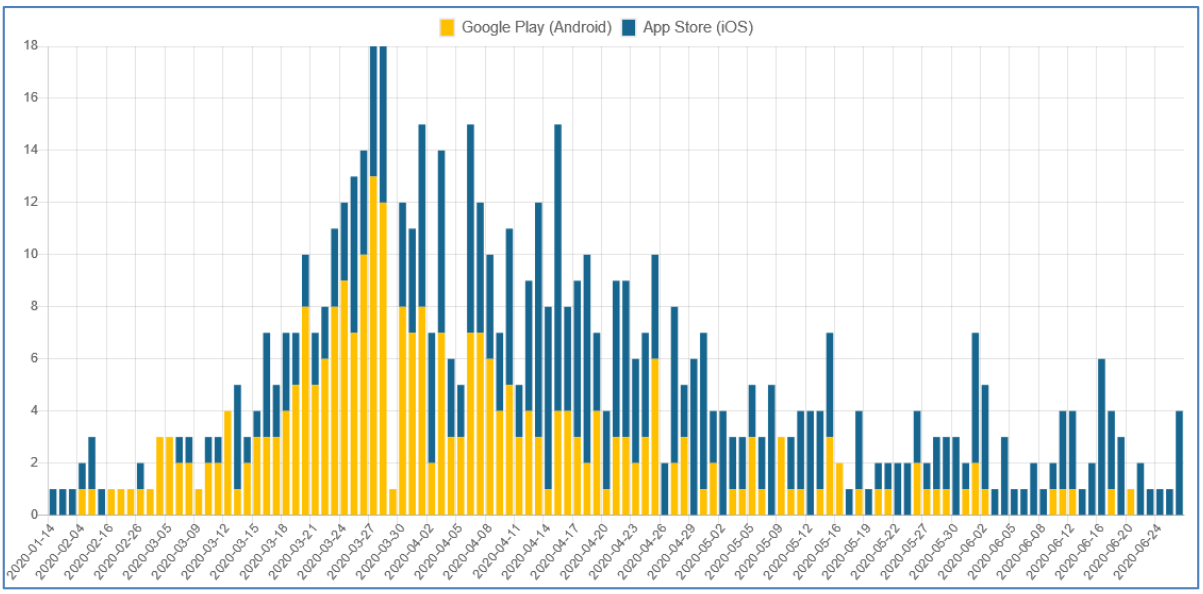
Apps to fight the pandemic receive most societal attention when it comes to their '*contact tracing*' functionality. Contact tracing apps are designed to complement manual contact tracing efforts, normally done by health authorities, which consist of in person interviews with positive cases to identify and contact those who may have been exposed to the virus and provide adequate guidance. Contact tracing apps are thought to facilitate such tasks through the recording of location data or Bluetooth communication data, as a means to automatically detect if a user may have been exposed to the virus. Such contact tracing apps are seen as an important tool to help mitigate the negative impact of the outbreak and many countries have launched or are currently developing them. Within this context, however, many questions are still open concerning these apps accuracy, safety, privacy, but also their effectiveness in helping to fight against COVID-19 and reduce the severity of the confinement measures.

Apps developed in response to COVID-19 also include many other functions beyond contact tracing, such as symptom checkers and self-diagnosis tools, trustworthy information and guidelines to the public, data donation initiatives to provide scientific and policy knowledge about the virus, live maps and info graphics, telemedicine and quarantine/lockdown monitoring. We analysed these COVID-19 related apps from the Google and Apple app stores in order to understand the overall landscape. We covered all kinds of COVID-19 related apps and categorised them according to their functions. We saved daily the newly emerging apps (and investigated if some disappeared) and derived an overview table together with a few basic statistics. Figure 2 provides an impression of the evolution of apps availability derived from Google Play and Apple App store.

The release of new COVID-19 related apps reached its peak between the end of March and mid-April. In conjunction, considerable attention and public debate were mounting around the emerging approaches for collecting and processing data for contact tracing apps (Ada Lovelace Institute, 2020; Criddle and Kelion, 2020; Howell O'Neill et al. 2020; Floridi, 2020). The first proximity-tracing framework was the Pan-European Privacy Preserving Proximity Tracing (PEPP-PT)[20] that foresaw a centralised mechanism of data collection and processing by governments receiving constant streams of data through Bluetooth from mobile phones tracking near-by contacts. Subsequently, a consortium composed of several international experts from academia and research institutions, including several former members from the PEPP-PT initiative, proposed a decentralized alternative: the Decentralised Privacy-Preserving Proximity Tracing (DP-3T) (Troncoso et al. 2020). In the DP-3T data about people who had been in close proximity in the previous weeks is stored on the mobile devices and not saved on a central server. Finally, Google and Apple partnered and proposed a joint solution named Exposure Notification, which also follows a decentralised approach and was inspired by DP-3T.

[20] https://www.pepp-pt.org/

Figure 2: Temporal overview of COVID-19 related apps published on official app stores (status 30 June 2020)



Source: JRC

The first approach (PEPP-PT) was promoted by those arguing that it would give a more comprehensive picture to the authorities about the spread of the virus and greater reassurance to the public that the data was handled ethically by governments. The counter-argument was that it would stress already fragile public sector servers to handle millions of transactions per day, expose them to greater cybersecurity threats, and eventually lay the ground for invasive forms of state surveillance (Clarke, 2020). The second approach (DP-3T) appeared technologically simpler, and was promoted by researchers and activists as more privacy-preserving than the first one, which became a prominent factor in the vibrant debate concerning government accessing personal data. The debate especially exposed a certain lack of trust in how data would be handled, and in general revealed a concern about creating a "precedent" that could also be used in other circumstances (see Section 8).

Many European governments initially favoured the first centralised approach, but when Apple and Google announced on 10th April[21] that they would team-up to develop interoperable APIs (Application Programming Interfaces) based on the second approach and indicated that they might not support alternative solutions on their platforms (i.e. allowing apps to work and collect Bluetooth data while running in the background), this swung the debate. Germany and Italy switched from the PEPP-PT to DP-3T with Finland, Austria, Latvia, Estonia, Ireland, the Czech Republic and Switzerland also adopting a decentralised approach (Criddle and Kelion, 2020; Howell O'Neil et al. 2020). At the moment, other countries are waiting to take a decision or do not plan to develop such an app due to skepticism about its effectiveness (e.g. Belgium and Sweden). Whilst the European Commission issued useful guidelines and recommendations on the developments of the tracing apps emphasising the importance of privacy and security, and the compliance with EU Fundamental Rights, while ensuring that apps are used on a voluntary basis (EC, 2020h, 2020j, 2020k), this episode showed the role that web giants play in relation to governments' decisions. At the same time, it also illustrated how the active promotion of solutions by researchers and activists can connect to the public debate, and how this might influence public decision making on a national scale.

Regardless of the chosen technological solution, a key issue for the effectiveness of these apps is the extent of their download and consequent use. The estimates of what is the minimum share of the population needed to make the use of the app effective vary, but it is noticeable that Singapore - one of the first countries to develop such app - argued that a 20% use was totally inadequate. If only one in five people have the app downloaded and working, this means that the chance of tracing an individual who has been in contact with somebody found positive is only 4% (20% X 20% or 0.2 X 0.2). Therefore, the government of Singapore argued that it was necessary for at least 75% of the population to use the app in order to have at least a 50% chance of tracing people who had been in contact with a positive case (Yee, 2020). Similarly, in the UK it was argued that it was necessary for at least 60% of the population to have and use the app to make it effective (Hearn and Sabbagh, 2020).

[21] https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

It is worth then considering that according to the Eurobarometer survey of December 2019 (Eurobarometer, 2020), across the whole of the EU 27% of the population does not consider itself to have sufficient digital skills (only a 2% improvement over 2017) rising to more than 30% in 12 of the EU countries, with between 12 (EU average) and 25% (worst case) considering they have no digital skills at all. Furthermore, among the younger and the older segments of the population the percentage of people who do not own a smartphone or do not use one for accessing the Internet is notably higher than in the rest of the population. Therefore, these groups would be excluded by default from access to COVID-19 apps. Aside from the purely quantitative dimensions of this phenomena casting doubts on the effectiveness of the tracing apps, these figures also raise the issue that these apps are likely to benefit most the higher income groups leaving poorer segments of society further exposed. Finally, even among those with the necessary skills and devices, it is necessary to consider their propensity to download and use the apps. Survey results currently available regarding European citizens' perspectives about COVID-19 contact tracing apps show that not all citizens are willing to use them. For instance, a survey conducted in the UK, Germany, Italy, France and the USA in March shows that around three quarters of those surveyed said they would "definitely" or "probably" install such an app, while other national surveys, in Italy and Switzerland, showed lower percentages, close to 60% (Milson et al. 2020; Rossi, 2020). Among the main reasons for not wanting to use these apps are: privacy and security concerns over personal data handling by public bodies and/or private companies, as well as skepticism towards these apps accuracy and their efficacy in addressing the spread of COVID-19 (Rossi, 2020; Redmiles, Kaptchuk, and Hargittai 2020).

In the light of the considerations above, we saw how important it is for governments to earn trust from citizens when implementing solutions that deal with their digital data. We may conclude that whilst the COVID-19 crisis may have increased governments legitimacy in collecting and processing data for the benefit of society, we still need to improve the overall level of societal readiness in terms of skills, distributional impacts for those left behind, and public trust. Finally, the dependency on tech giants for implementing large scale digital solutions that pursue the public interest emphasises the overarching influence of the commercial sector in setting the agenda and in creating the infrastructure used by governments to collect and use data.

8 Privacy, democracy and the public sphere in the age of COVID-19

L. Vesnic-Alujevic and F. Pignatelli

Government access to personal data is an area of concern for potential misuse. Democratic accountability is therefore crucial.

The COVID-19 crisis has raised a number of societal, ethical and policy challenges. Some of them are connected to increased use of digital tools in our everyday life during the confinement (e.g. for telework whenever it is possible, for being connected to other people, being informed especially about the spread of the virus, for leisure, shopping), as well as the use of AI, apps and consequently, data. As already mentioned, COVID-19 apps have been developed for surveillance and monitoring of disease spread through the so-called contact tracing. Monitoring and tracking of movements is considered to have the potential to be effective in the situation of medical emergencies, even more when non-anonymised data are used (Long, 2020).

While technology can give us powerful tools in the treatment and monitoring of a disease, offer solutions to save lives or get us out of the confinement, we should not assume that it can replace medicine. It is often believed that every solution for problems we face nowadays can be solved by technology (Klein, 2020; Vesnic-Alujevic et al, 2016; Dubal, 2020). In the COVID-19 context, that would mean that technology is "the only possible way to pandemic-proof our lives, the indispensable keys to keeping ourselves and our loved ones safe." (Klein, 2020). Similarly, Fuchs (2020), for example, argues that "technological fixes to political problems because of the complex interaction of technology and society, can never work" (Fuchs, 2020, p. 262). In this context, for example, it is interesting to observe that although 38% of the Islandic population already use a contact tracing app, the estimations are that the real impact is rather small, especially compared to manual tracing techniques (Johnson, 2020). As discussed in Section 7, one would need a 75% uptake to have a 50-50 chance of getting some useful information. Even if technology were a key to protect public health, should it be in hands of private entities or should it be controlled by public ones (Klein, 2020)?

While apps are built to be used for medical purposes, they can in parallel be used to monitor their behaviour and movements all the time (Harrari, 2020). Through a combination of apps and facial recognition, new mass surveillance systems based on biometric data are born and could give legitimacy to the use of such systems outside of emergency states. The interlacing of public health goals with mass surveillance can be potentially alarming. In this way, surveillance can be repurposed for public/social good but could have broader antidemocratic and discriminatory consequences in a longer term and at a broader scale (Dubal, 2020).

Although in Europe installing the app will not be compulsory, and the evidence is mixed on the extent to which citizens are under pressure to install the apps, the question remains whether we might be trading our social isolation for "being imprisoned by the for-profit use of our data" (Klein, 2020), i.e. the so-called "cage" of surveillance capitalism (Cliffe, 2020; Zuboff, 2019)? A somewhat similar "experiment" of making a "smart" city in Toronto waterfront with the increased use of technology and surveillance through a "sensor-laden vision" was rejected by its residents who objected to enormous amount of personal data that could be collected by a private company, approach to privacy and intellectual property and dubious benefits for the city (Hawkins, 2020; Klein, 2020).

In circumstances such as a pandemic, the State needs all of its citizens to obey the rules and can monitor and sanction those who break them (Harrari, 2020). The concepts of bio-surveillance, biopower, as well as disciplinary society were developed almost half a century ago by French philosopher Foucault. An alternative

framework was later developed by Gilles Deleuze (1990) through the concept of societies of control leading to Zuboff's (2019). surveillance capitalism. With the rise of digital health and AI, scholars (e.g. Lupton, 2014; Van Dijk, 2014) have warned that digital technologies used in healthcare change power relations and allow for new digital inequalities and spaces of surveillance. One of the long-term worries is that through the idea that our health and safety depend on technology, the technology becomes integrated into the basics of social functioning. An example of such approach can be a kindergarten in Varese, Italy, currently experimenting with 150 children that will wear electronic bracelets to trace their contacts and vibrate if social distance is not respected, as a "sort of a game" (ANSA, 2020).

As presented in Section 7 current debates focus around centralized vs. decentralized app models where key matching information are stored only on the phones, instead of centralized archives. While a preferred model to many is a decentralized one because of privacy, Bluetooth that needs to be used in a decentralized model also creates potential privacy problems (Naughton, 2020). One of the risks of the introduction of surveillance systems in our democracies is democratic backsliding in the longer term and the loss of privacy as a human right (Arnould, 2020). Human Rights Watch and similar civil society organisations have already warned about these practices especially in central and eastern Asia. State-collected especially non-anonymised data on people's health or immunity status creates many health privacy concerns (Long, 2020). Therefore, there is a need for a strong democratic control on data access and societal "aim" of digital technologies and the use of data, while respecting normative and constitutional principles (EDPS, 2020). We should not forget that these are all sensitive data: biometric data, health data, location and movement data, that will be combined with our social contacts, and given to government and private companies.

Location data, for example, not only shows where an individual is, but also what their interest and preferences are. Although general data protection principles can be applied to location data privacy (Keßler, and McKenzie, 2018) there is a need for some specific considerations (Pignatelli et al., 2020). With contact-tracing apps in a post-pandemic world, location will certainly be a key piece of the data infrastructure. However, location data privacy needs to remain one of the key public concerns. Although privacy and data protection legislation is generally enacted on a country to country basis, the overarching logic and contents are comparable. The European Union General Data Protection Regulation (GDPR) (EC, 2016) is generally regarded as the most robust and mature data protection framework in the world. The GDPR states that location data privacy is the individual's right not to be subjected to unauthorized collection, aggregation, processing and distribution (including selling) of his location data. It is the right to be protected by the ability to conceal information of whereabouts, which can be derived from personal location data. Anonymization of such sensitive data in Europe should, thus, be paramount.

Despite the need to contain the pandemics, government must remain transparent and accountable to its citizens, while protecting their health. In other words, this cannot mean infringing citizens' rights in order to protect them but acting in the interest of the public and citizens. The crisis cannot be an excuse to advance authoritarianism or not respect human rights such as privacy (Zahuranec & Verhulst, 2020). It is important to have an oversight and governments need to be clear about the purpose of the app. Unnecessary information (in terms of pandemic) should not be gathered and/or stored longer than the duration of the crisis. The accountability is important to strengthen the trust of citizens both in government as well as in technology, as effective deployment of technology to support the transition to a post-COVID-19 society depends broadly on trust in both (Ada Lovelace Institute, 2020).

Ten of the Council of Europe's 47 Member States (Albania, Armenia, Estonia, Georgia, Latvia, Moldova, North Macedonia, Romania, San Marino and Serbia) announced derogations from the provisions of the European Convention on Human rights, possible under Article 15 in the period of "public emergency threatening the life of a nation". In a period of emergency, the state can take measures derogating from their obligations to protect fundamental rights and freedoms. Six of these countries included Article 8 (right to privacy) in the list of derogating articles (Siatitsa & Kouvakas, 2020). In Hungary, the emergency measures introduced a possible prison sentence for spreading false information about COVID-19. The Bulgarian president partially vetoed a similar law that could have repercussions on free speech (Verseck, 2020). The use of such apps could have a long-lasting impact on democracy and changes to everyday lives, as surveillance and use of data in such way could become permanent. This could also impact social and political cohesion (Long, 2020; Naughton, 2020). Ada Lovelance Institute (2020) recommends a comprehensive legislation "to regulate data processing in symptom tracking and digital contact tracing applications. Legislation should impose strict purpose, access and time limitations."

With the increased use of digital technologies and apps, as mentioned (Craglia et al. 2018) it is crucial to consider ethical issues that could emerge from the use of such technology. As discussed in Section 7 tracing

apps raise important issues about the distributional impact of their use given the different levels of skills in society and access to the right equipment. The app might restrict not only privacy but also other human rights (e.g. liberty of movement, right to self-determination, freedom of association), while its accuracy and contribution to tracing infections is questionable. As with other ethical issues connected with the use of AI, this also leads to the question of who is responsible and liable for potential errors (in connection with the identification of people or areas of high risk) that should be minimized (Craglia et al, 2018). The app could also lead to further discrimination in hiring based on our health status as well as social isolation due to lack of confidence in other human beings (Lauwaert et al, 2020).

Data and new technologies should be used to empower citizens and help them make more informed personal choice rather than "all-powerful government" or private companies (Harrari, 2020). This is why more debates in public are needed. Some countries tried to organize public debates in connection to the development and use of apps (e.g. Netherlands), but many are trying to make decisions quickly and thus bypass democratic processes and input from the public (Mello & Wang, 2020). For these and other issues, it is important that solutions do not come top-down but are explored through a broader debate (Lauwaert et al, 2020). Deciding on the direction our societies should go and how democracies should be preserved and enhanced need to be explored through enhancing individual and collective agency (Waltner-Toeuws et al, 2020). Because without public trust and participation, these strategies have little chance of success.

9 Using data effectively to support post lock-down re-opening.

J Hradec

Innovative uses of AI methods can extract useful intelligence from existing administrative data without interfering with data protection.

The running thread of this report is that data is at the heart of AI applications: being able to access and effectively use the data we have is essential for every company, public organisation or state. In Section 8, we have raised a number of important issues with respect to the potential negative uses and consequences of the data generated and collected in a crisis like COVID-19. In this Section, we report a more positive example based on work at the JRC to support the European Commission and the EU Member States to assess the relative risks of reopening different economic sectors after the lock-down period. As we have seen, during lock down, which was more or less stringent in different EU countries, only essential services were kept running at all times (e.g. utilities, food production and distribution, pharmaceuticals, essential infrastructures). As the peak of contagion passed, there was a need to identify which economic sectors to open first to allow the restart of the economy whilst reducing the risk of a second wave of infections.

To answer this question, we followed the steps below:

1. Create a model of the likely number of daily contacts of each person based on both economic and social activities,
2. For the economic activities, identify the relative number of daily contacts of each worker by economic sector, also considering the potential for telework and the proportion of workers commuting daily by public transport in "normal" circumstances.
3. Assess the socio-economic impact of risk (by gender and income)
4. Assess the spatial distribution of risk, based on socio-economic characteristics of different regions, and commuting patterns.

For 1) EU statistics on income and living conditions (SILC) 2015 data were used to extract data on individuals and households and data were combined with data on cultural participation[22] and enriched by remodelled data on regular use of public transport (also from SILC) only available for 2014.

The data were aggregated to obtain personal archetypes (e.g. male 50-59 living in a household of 5 people in highly populated statistical area NUTS AT3 of Austria, working as a manager in agricultural workplace with 20-50 coworkers who has a car in the household and meets relatives daily while going to cinema and concerts at least once a month). All together 505,493 of such profiles were generated representing 520.5 million people in the EU, Norway, Switzerland and Serbia.

For each archetype, the number of daily contacts (DC) was estimated as follows:

- Household size: all people in household meet daily, added to DC

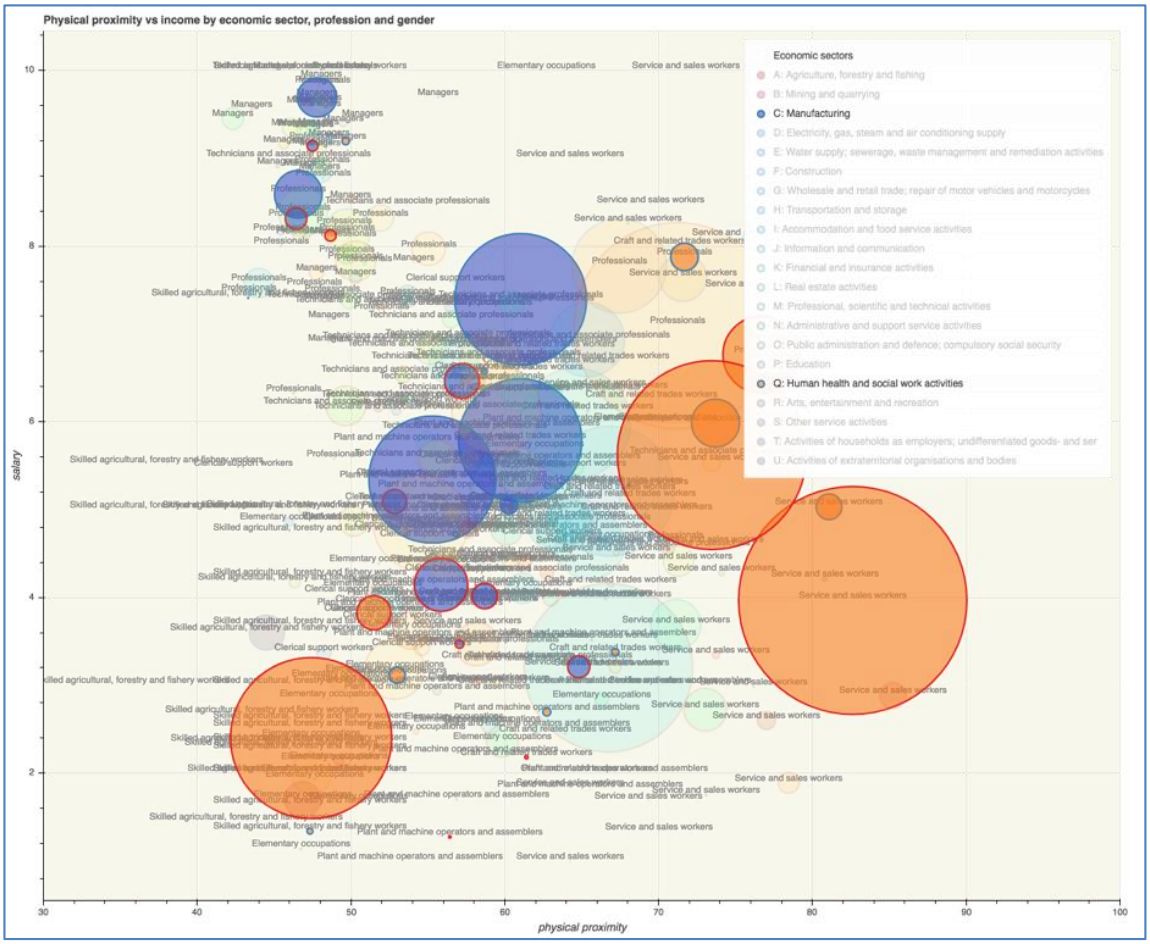
[22] https://ec.europa.eu/eurostat/statistics-explained/index.php/EU_statistics_on_income_and_living_conditions_(EU-SILC)_methodology_-_2015_Social/cultural_participation_and_material_deprivation

- Apartment block housing adds 5 (3 for smaller apartment blocks) to DC, detached houses add 0
- If schooled: 50 contacts added for all types of school
- Public transport: 50 contacts added to DC if in densely populated area, 30 for medium population, 10 for scarcely populated areas.

Meeting relatives/friends, other social and cultural activities, and voluntary activities: added a number of contacts based on the available European data.

For 2) and 3) data from the European Union Labour Force Survey (EU LFS 2019) database were extracted on professions and economic sector, by sex/gender, and country. In total, data covering 218 million economically active people were used in the study. Data on physical proximity by economic sector, and therefore daily contact potential, was estimated based on Dingel and Neiman (2020). Figure 3 below shows as an example the physical proximity (X axis is Index of proximity based on Dingel and Nieman) vs. income (Y axis = weighted average of income deciles) by economic sector, profession, and gender (blue ring around blob = men, red= women). The figure clearly shows that healthcare and social workers (in orange) are at greater risk of infection having a larger index of physical proximity than workers in the manufacturing sector (in blue). They are also almost exclusively female and paid less than their predominantly male workers in manufacturing. COVID-19 does not affect people equally but exacerbates existing inequalities in society. We return on this in Section 12.

Figure 3: Physical proximity vs income for all sectors with Manufacturing and Health highlighted.



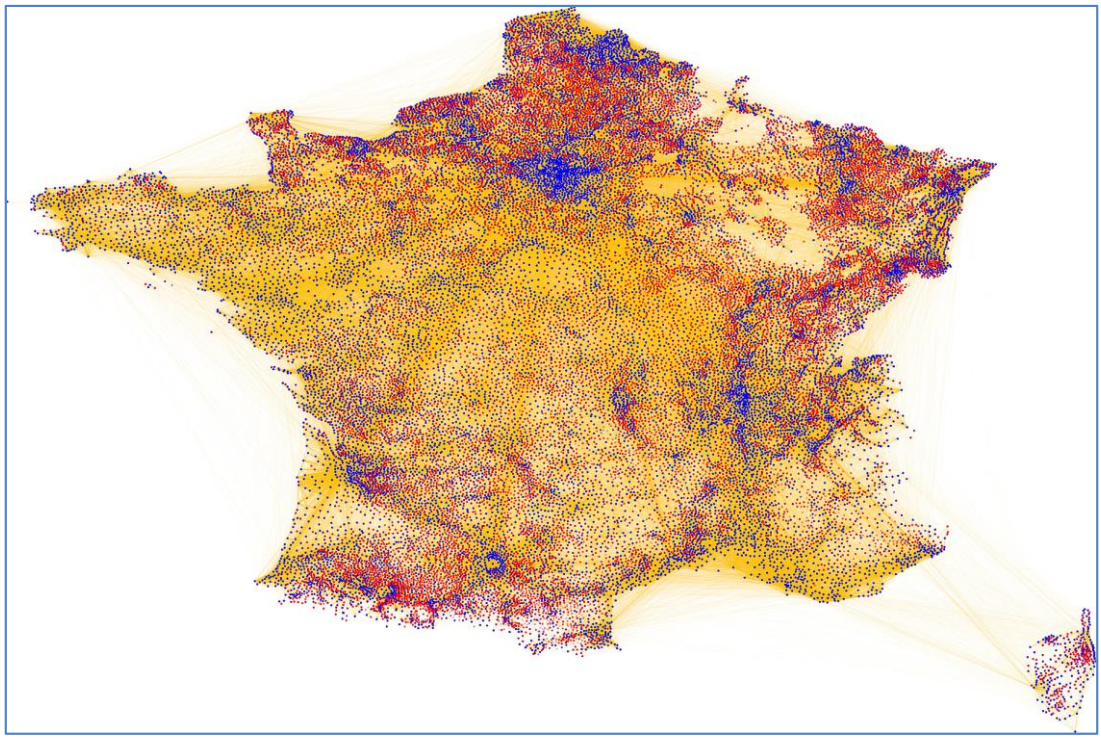
Source: JRC

To address 4) we leveraged the concept of synthetic population developed in the JRC's Digitranscope[23] project. In this project we took the lowest level of spatial data at which official statistics are released (typically the census track that has a population of 300-500 people depending on country and location) and used machine

[23] https://ec.europa.eu/jrc/communities/en/community/digitranscope

learning methods (iterative proportional fitting) to create a synthetic population (Lenormand and Deffuant 2012, Gargiulo et al. 2010), i.e. to distribute all the official data available for these areas (gender, age, family composition, conditions of the buildings) to a set of "statistical" individuals so that when aggregated into families and households at the area level they return the same data as that of official statistics[24]. If data from the official cadastre is available on building characteristics it is also possible to assign these "statistical" individuals and families to individual properties so as to have an even more fine-grained spatial distribution of official data. This method is potentially very powerful to estimate needs and design policy interventions targeted to specific groups and neighbourhoods. In the context of this project, it was possible to model the synthetic population of 63 million people, in 35 million households allocated in 10 million houses in France using data from their official statistical office[25] to model their travel to work behaviour, also estimating the proportion of people using public transport by economic sector. The figure 4 below shows the model of the commuting patterns of 26 million French in 2016. Areas in blue show increased daytime population concentration as people commute in, while areas in red show decrease as people commute out.

Figure 4: Influx-outflux of French commuters 2016



Source JRC

Assuming the same commuting patterns by public transport by sector as those of France (because of lack of data in other countries) it was possible to arrive at a cumulative estimation of the relative risk of reopening the economy by sector, and the social and geographical distribution of potential impacts. Ultimately, the choice of what to open, where and how is political as it needs to balance the health vs. the economic and social risks, but this example shows the opportunities offered by the application of AI methods on available official data to support policy. Beyond this specific example, the possibility of creating synthetic populations and remodeling available data to identify the specific needs of groups and categories opens the door to the design of more "personalised" and responsive policies that put individuals at the centre of the policy intervention as discussed in Craglia, Hradec and Troussard (2020).

[24] We also used fitness-based synthesis to avoid having a low-entropy population where the distribution of attributes concentrates around the mean (Ma and Srinivasan, 2015)

[25] https://inseefr/en/statistiques?debut=0&theme=1

10 How COVID-19 exposed the European fragility of networks, technology, and data strategies

S. Nativi

The lock-down exposed the dependency on non-European platforms and the gaps in European technological sovereignty.

In a digitally transformed society, the COVID-19 crisis has shown that digital platforms have become strategic resources even for non-traditionally digital sectors, such as public administration systems (including the healthcare one), fresh food retail, personal care retail, administrative intermediations, education, and business (e.g. Marr, 2020; Nicolls, 2020). In Asia many application platforms (largely mobile based, such as *WeChat*) had already developed spanning many different applications areas and market sectors to serve customers/citizens with their daily tasks, from food retail to insurance and banking services, using a single entry point. The COVID-19 crisis gave these platforms a unique opportunity to provide users (e.g. consumers & suppliers, advertisers, intermediaries, audience, educators & students, public authorities & citizens, employer & employee, etc.) with the only "safe" instrument to come together and exchange goods, services and information. As a result, these platforms have had an extraordinary chance to reach out to new users and collect valuable big data, in particular on the behaviour of "non-traditional" users, reinforcing their own position and creating valuable intelligence.

This has accelerated the process of market polarization on big digital platforms. In fact, while data is replicable customers are not. COVID-19 represented an important opening for those digital platforms that could scale up in a few days i.e. big ones, to attract new users/customers on different sides of the market by offering them good network connectivity and a rich user experience for their new daily tasks. To attract new customers and keep old ones, several platforms and ecosystems offered free data and services including the well-known tracking apps. Platforms can be seen as planets with a gravity; once "landed" on a planet, it's difficult to escape its gravitational attraction.

The rest of the section will briefly investigate some COVID-19 implications from a European perspective, on infrastructure and software applications of platforms. We focus in particular on two software application areas which have become iconic of the COVID-19 crisis: videoconferencing and educational platforms, while a third one, personal tracking apps, is addressed in Section 7 of this document.

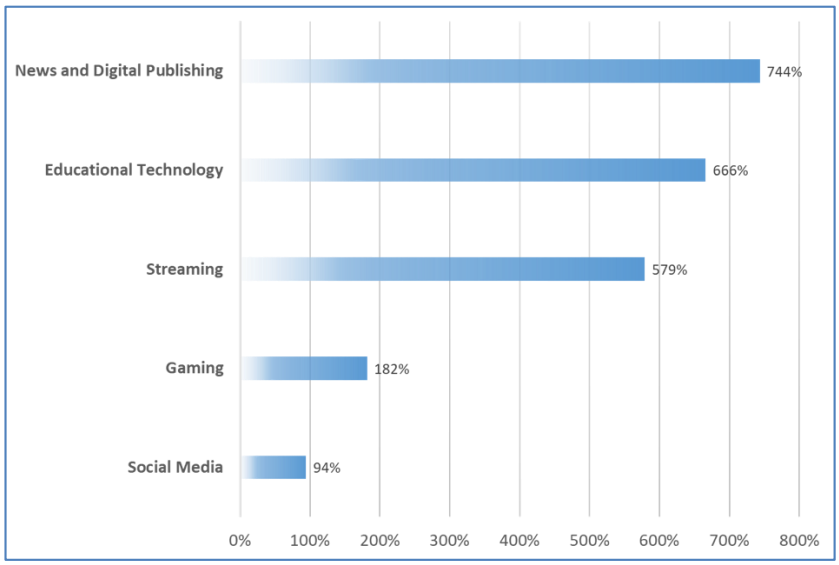
10.1 COVID-19 effect on Network services

Most of the big companies providing services for networking, cloud computation, and media and content delivery, reported an impressive jump in their traffic a few days before and/or just after the lockdown measures taken worldwide, more than 70% for Italy and UK, about 40% for Spain, France and Poland, around 20% for USA (DE-CIX, 2020), (Bergman & Iyengar, 2020), (McKeay, 2020) (Bhak, Bayulgen, Blum, Ford, & Van de Weyer, 2020). Interestingly, an important traffic increment (estimated to be between 10% and 30% worldwide) has remained even in the de-confinement phase, largely anticipating the growth forecasted for the end of 2020. Naturally the amount of data generated by the Internet (potentially to be processed for working out intelligence) augments along with the traffic growth.

Indeed, telecommunication companies have been under enormous pressure to continue delivering critical infrastructure and services during the coronavirus outbreak. In particular, in March, video usage increased more than 40%, VPN usage more than 60%, and there has been a tenfold increase in collaboration tool usage

(Cooney, 2020). Over February and March, Fastly[26] analyzed traffic by vertical industries, looking at average percentage increases of requests per second (RPS) comparing the expected RPS growth before COVID-19 and the actual growth during the COVID-19 crisis, an elaboration of these data is showed in Figure 5.

Figure 5. Percentage growth of the request per second (RPS) measured in March per application platforms, calculated in respect of the expected RPS increment as calculated in February, before the COVID-19 crisis.



Source: JRC based on elaboration of data reported by Fastly, Bergman & Iyengar (2020)

Internet and the Web survived COVID-19 emergency leveraging their resilience and elasticity by-design nature (Cooney, 2020; Graham-Cumming, 2020; Scott, Cerulus, & Delcker, 2020; McKeay, 2020). In particular, the Internet Protocol (IP) design, the Internet peer-to-peer structure, and the elastic nature of modern websites and Internet applications that still work even if webpages may take a bit longer to load. The Internet builds on the connections of backbone networks at peering points (which are neutral facilities often owned by third parties and non-profit organizations); they had to face the most important congestions in the network to move traffic among the peers, as recognized by CISCO (Davidson, 2020). The peering points and the whole backbone infrastructure rely on the fastest computer networking devices (switches and routers) made by vendors that are predominately American and Chinese e.g. Cisco, Extreme, Huawei, and Juniper. Although the Internet showed a good scalability, a set of important collaborative measures, noticeably with American and Japanese companies, had to be taken to govern the network traffic and avoid major disruptions. The general effect of these measures was to reduce the quality of service e.g. the decrease of downlink speed observed by Fastly, and limit the behaviour of some specific applications, in particular:

- The European Commission invited streaming platforms (in particular the American Google, YouTube, and Netflix) to follow the lead of telecom providers and consider adapting the throughput of video streaming and temporarily moving to SD (Standard Definition) rather than HD (High Definition) streaming, at least for the most critical working hours of Internet activities on impacted geographies (Lomas 2020).
- Some content delivery companies (e.g. the American Akamai) (McKeay, 2020) worked with partners (e.g. the Japanese Sony and American Microsoft) (Giret, 2020), to limit the impact of patches to games and other software downloads by using off-peak hours for downloads.
- The European Commission also asked telecoms operators that provide Internet services to take steps to prevent and mitigate the impacts of impending network congestion, by inviting them to make use of "possibilities" offered by EU net neutrality rules, most outages have been limited to digital services like videoconferencing (Scott, Cerulus, & Delcker, 2020).

[26] Cloud computing services provider and Google partner.

- The European Commission finally called for Internet users to make responsible use of online recreational activities, including using Wi-Fi (rather than mobile data) and choosing lower resolution for content whenever possible (Lomas, 2020).

Fastly analyzed the Internet traffic of France, Italy, Spain, a few USA states deeply affected by COVID-19, UK, and Japan, observing that the traffic growth caused a common deterioration of the quality of service (i.e. decrease of downlink speed), with the exception of Japan and California. The deterioration was more remarkable in Europe (Bergman & Iyengar, 2020). It is also worth noting that the current regional-based governance of the Internet may in the future be affected by corporate initiatives providing global Internet access via constellations of satellites (Mann, 2020) or high-flying balloons (e.g. Loon[27] project by Google)

10.2 COVID-19 effect on Software applications: Videoconferencing and Education frameworks

During the COVID-19 crisis, the popularity of video-conferencing technology has grown exponentially. Large numbers of people turn to video-teleconferencing platforms to stay connected; enterprises and government organizations started using video conferencing as an effective solution to connect with remote workers, customers, and employees. Like many other Web and Internet software applications, the leading service providers in this area are largely American (e.g. CISCO WebEx, Microsoft Skype and Teams, Google Meet, Zoom VideoCommunications, 8x8 Video Meetings, LogMeIn, GoToMeeting)[28]. All the platforms saw a considerable increase in usage taking the opportunity to connect further with their customers and attract new ones (Carter, 2020). Soon after the lockdown in Europe, in March, Webex reported that more than 30% of its top global enterprises had asked to help them scale remote work, and Microsoft reported that its Teams collaboration platform has seen a 500% increase in meetings, calls, and conferences. To face such huge demand, compete in a crowded sector and avoid being seen as avidly opportunistic, many market players offered their services for free (or at minimal cost) to enterprises and government organizations e.g. in February, Zoom lifted the 40-minute limit on video calls for its free version in China.

Unquestionably, the image of videoconferencing explosion due to COVID-19 is represented by Zoom. The company was already a *unicorn*[29] at the beginning of 2017, but it was with COVID-19 outbreak that the company has taken off. In March, Zoom reached more than 200 million daily meeting participants (Yuan, 2020) and surpassed 300 million in April (Zoom, 2020) compared the 10 million meeting participants at the end of December 2019. Zoom was also emblematic for a couple of challenges that emerged with COVID-19: the rise in cyberattacks and the re-evaluation/definition of privacy. In March, Zoom had an important privacy and security backlash (i.e. videoconferences hijacking, also called "Zoom-bombing") (FBI Boston, 2020), which led the CEO and founder of Zoom to apologize (Yuan, 2020). The Citizen Lab of the University of Toronto found that the company was using a questionable definition of 'end-to-end encryption' (Marczak, 2020). Besides, Zoom was sending unauthorized data to Facebook (Cox, 2020). At the end of April, Zoom claimed to have resolved all these issues (Zoom, 2020), and was reported by Okta 2020 to be the 2020 top videoconferencing App.

According to the World Economic Forum (Li and Lalani, 2020), 1.2 billion children in 186 countries are out of the classroom. Where possible, in response to COVID-19 measures, schools and teachers had the difficult task to convert in-person courses into virtual ones. The market of online education (including language apps, virtual tutoring, video conferencing tools, and online learning software) have received a significant surge in usage since the COVID-19 crisis. As for the videoconferencing applications, this market sector (estimated to reach $350 billion by 2025, before the COVID-19 boost) (Research and Markets, 2019) is dominated by the United States and China. Due to COVID-19 lockdown, in Asia several companies saw the explosion of their learning apps (Li & Lalani, 2020), including the Indian BYJU's, the Singapore-based collaboration suite named Lark, the Chinese Tencent classroom and Alibaba distance learning solution, DingTalk. Google offered its Classroom suite to schools, the online platform that allows teachers to post videos and assignments, while, the University of Bologna in Italy (with an enrollment of over 80,000 students) switched 90% of its courses online using Microsoft Teams (Spataro, 2020). Finally, in March, Zoom offered free access to video conferencing tools to K-12 schools during COVID-19, and 90,000 schools in 20 countries were among the new users of the app. School administrations had to face three important challenges: the scalability of their digital infrastructures (see cloud

[27] https://loon.com/

[28] An example of open source videoconferencing platform is Jitsi https://jitsi.org/

[29] A privately-held startup company with a value of over $1 billion.

infrastructures), the often limited preparation of the staff to run courses online and the increased digital divide (i.e. the spread, use and availability of technology) affecting their students.

10.3 Conclusions

The Internet and the web are resilient by-design but three other factors were important to face the traffic explosion due to the COVID-19 lockdowns: (1) a peer-to-peer structure relying on neutral (often non-profit) exchange points (aka peering-points), (2) an effective collaborative governance of the network, and (3) the degradation of non-critical services as well as a general acceptable deterioration of downlink speed. As to European technological and data sovereignty, the sectors to be monitored are: fast computer networking devices, distributed computing platforms, content delivery networks, and media streaming networks.

Technology and data sovereignty must include software applications. The vast majority of the software online applications utilised by old and new users/customers in the COVID-19 period, are American and Chinese. This means that these companies have been able, through their platforms, to gather additional intelligence about every aspect of the European economy and society.

Society is moving its economic and social transactions more and more from the physical to the virtual world, which is, once again, largely dominated by American and Chinese companies. For Europe, it is of paramount importance to strengthen its presence in this world whose development has received an important acceleration due to the COVID-19 outbreak.

Profound crisis periods, like the one generated by COVID-19, have shown in the past to create also opportunities for digital innovative solutions giving birth to new unicorns and to some of the present big Web giants. However, it is important to have a supporting ecosystem for this to happen, as in the Zoom case, and there are lessons here for a European perspective.

- The re-evaluation/definition of privacy is a clear challenge of a post-COVID-19 digital society as discussed in Section 8, and IP issues discussed in Section 5 may need to be re-evaluated in the context of the current increased use of collaborative platforms.
- Cybersecurity: Zoom security and privacy shortcomings reconfirmed the general belief in Europe that a stronger regulatory framework is needed also for non-European companies operating in Europe. The discussion of cybersecurity issues in Section 11 may have further implications for a European technological and data sovereignty perspective.
- Internet is a strategic infrastructure and the future Internet (the transformative internet) will be even more. The present regional-based governance of the network might be significantly affected by innovative technologies that promise a global Internet access in a low-latency broadband way.

11 AI-related cybersecurity considerations for the COVID-19 situation

R. Hanon, H. Junklewitz and I. Sanchez

AI can strengthen cybersecurity but also be exploited for cyberattacks. Either way, it is a key technology for the digital integrity of society.

11.1 Cybersecurity context of the COVID-19 crisis

The current COVID-19 pandemic has significantly affected the landscape of cybersecurity risks faced by European governments, businesses, and citizens. Threat actors are taking advantage of the multiple opportunities resulting from the public health and economic implications of the crisis. In particular, malicious actors profit from the much-increased reliance on digital instruments for both professional and personal activities (as discussed in Section 10), and from great pressure put on governments and state actors to handle the consequences of the crisis, which limits their capacity to respond to the emerging cybersecurity threats.

Various cybersecurity organizations have reported (Europol 2020), (CERT-EU 2020a) a significant increase of cyberattacks. For instance, within a matter of weeks of the outbreak, ransomware attacks had increased by almost 150 % above the baseline levels in February 2020 (Upatham und Trainen 2020). This increase in attacks was especially targeted against the organizations that are at the forefront of government responses against the pandemic in the first weeks of the crisis, even though this trend seemed to fade out as governments started adapting to the situation. For instance, the World Health Organization has been the target of constant cyberattacks since the beginning of the pandemic (Ahmed 2020). These attacks are not innovative in the way they are carried out, as they mostly rely on the same range of approaches traditionally employed in the past Rather, they show a change in purpose, with a shift of targets towards key actors in the fight against the pandemic (CERT-EU 2020b), such as national health organizations, hospitals or pharmaceutical companies. The motives of attackers include, amongst others, targeting crisis-relevant infrastructure, such as hospital networks, to extort money or cause chaos (Interpol 2020), threatening the leakage of personal data (Goodwin 2020), conducting scams on short supply medical equipment (Europol 2020), running cyberespionage campaigns to steal valuable information for the elaboration of a vaccine or even conducting state-sponsored attacks on research facilities (Goud 2020; Glyer, Perez und Jones 2020; Stubbs und Bing 2020; CERT-EU 2020c).

Corporations and individuals are also prime targets for cybercriminals as the crisis has intensified the use of digital systems, as discussed in Section 10. Firstly, this has led to an intensive use of teleworking that has migrated business activities from corporate networks and equipment to domestic ones, creating numerous opportunities for attackers to exploit the weaker security of personal devices and the lack of caution of users, in order to infect devices and compromise business secrecy. Secondly, the situation has also contributed to a significant increase in the usage of digital communication tools, and more generally of online platforms for entertainment or domestic activities, providing new opportunities for attackers (Abrams 2020). Finally, threat actors have also leveraged the justified fear of citizens with respect to this exceptional situation to deceive them for their own ends (Tidy 2020). This may explain the observed proliferation of attacks exploiting the COVID-19 theme (CERT-EU 2020d; Muncaster 2020), including intrusions into personal computers, email phishing and malware distribution campaigns, and intensive diffusion of misinformation to undermine the communication of national institutions.

11.2 Impact of AI in the cybersecurity landscape of the COVID-19 crisis

Artificial intelligence, as a driving force of the current digital revolution, also plays a significant role in the cybersecurity of digital systems, as it is a vector of innovation for both cybersecurity companies to design better products and services, and threat actors to develop more sophisticated attacks (Craglia et al. 2018). The COVID-19 situation is no exception, and although AI is not yet a key component of most cybersecurity software, tangible elements of the use of machine learning techniques have been identified during the COVID-19 crisis, both on the side of actors that attack digital systems and on the side of those who protect them.On the one hand, cybercriminals are integrating more and more AI techniques in their toolkits to increase the range of their attacks. A striking example of this is the growing use of deepfakes to conduct cyberattacks, for instance to induce fraudulent transactions, as in a prominent fake phone call case in 2019 (Stubb 2019). Deepfake (Kietzmann, et al. 2019) is the term used to refer to fake content generated using deep learning, a set of techniques that rely on large volume data to automatically generate original but realistic content. The term is generally employed for images, videos, audio recordings, and text, however, it could be extended to other kinds of content. The democratization of software to generate deepfakes has opened the way to their exploitation by threat actors in cyberattacks, to mimic content that is usually deemed to be hard to falsify by individuals without substantial means at their disposal. A recently published business analysis indicated that an increase in the use of deepfakes has been reported by companies (NCCGroup 2020) in scams relying on the impersonation of an authority figure. While there is not yet explicit evidence of the use of deepfakes for cyberattacks specifically during this pandemic, it is expected they will become a standard technique in the toolkit of threat actors to deceive users into taking actions to the benefit of malicious parties. As a matter of fact, recent examples of video deepfakes directly linked to the COVID-19 crisis (Galindo 2020; Priyardashini, 2020) in other contexts than cyberattacks, highlight the potential damage that could be provoked, when used in support of attacks such as business email compromise, phishing, identity theft, or cyberextortion.

Deepfakes also have a strong potential to cause serious harm in creating fake news and misinformation, even though first surveys seem to indicate that their use is not yet significant in misinformation campaigns (Brennen, et al. 2020). Finally, the high flexibility of deep learning techniques enables the production of fake content in contexts other than impersonation, like in medical imaging where threat actors could compromise sensitive information such as medical images to their advantage (Savevski 2020; Finlayson, et al. 2019). Generally, with their potential to create more targeted and automated cyberattacks, deepfakes are part of a larger picture where the introduction of AI tools leads to further automation and increased potential of cyberattacks (Bundage 2018). On the other hand, AI can help to fight these cyberthreats, exploiting its flexibility to detect new forms of attacks and adapt to new trends. For example, email screening and phishing detection solutions based on online learning can learn to address new COVID-19 related threats adapting to the rapidly evolving situation (Kan 2020). Similarly, AI can be used to combat misinformation campaigns monitoring media for fake news and detecting and preventing deepfakes. While AI has not yet reached its full potential for the protection of digital systems, it can be noted that companies offering digital services advertise the use of AI to strengthen the security of their platforms, especially in the light of the recent security vulnerabilities that have been discovered in many products and services with the emergence of mass remote working. As a response to this trend, threat actors are already integrating mechanisms to take advantage of the limitations and weaknesses of AI-powered detection systems, in particular, their vulnerability to adversarial attacks, a type of attack where the attacker adds additional content to the code of the malware, with the objective to make it look benign for the security engine. This approach has been detected for Trojans, with the use of text in relation to the COVID-19 crisis [30].

11.3 Conclusion

The COVID-19 crisis has already had a major impact on many sectors of our modern societies, and more consequences are likely to materialize over time. Cybersecurity is vital to ensure the resilience of the digital infrastructure, which supports an ever-increasing part of our societal activities. Rather than a radical overhaul, the crisis acts more as an amplifier of known cybersecurity issues. This is happening in a context where AI is becoming increasingly important as a new technology, a trend being amplified with increased digitization during the crisis. While AI is not yet a groundbreaking technology for cybersecurity, this crisis gives a glimpse of what is likely to happen in the next few years. Considering the potential of this technology for cybersecurity applications, as well as its potential for being exploited and misused by cybercriminals, AI will be a key element in the capacity of our societies to preserve their digital integrity in the next crisis to come.

[30] https://www.bleepingcomputer.com/news/security/trickbot-emotet-malware-use-coronavirus-news-to-evade-detection/

12 Regional perspective

M. Craglia

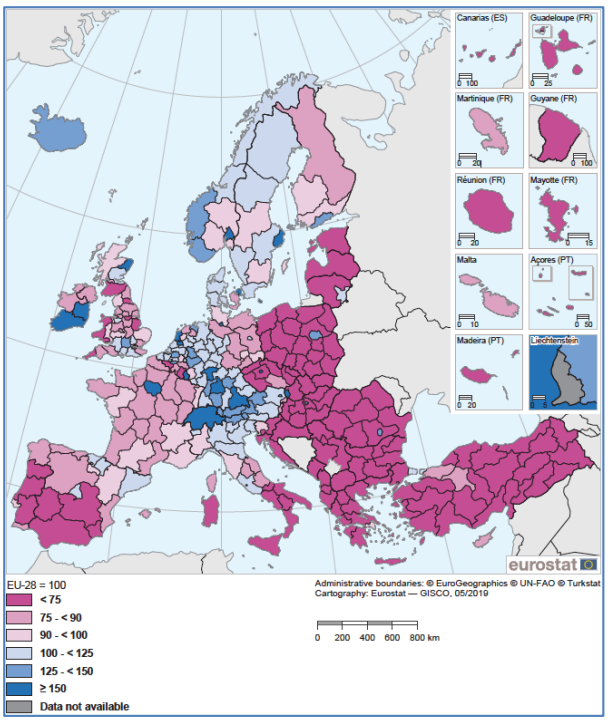
COVID-19 and the accelerated digital transition have widened social inequality and hit hard the elderly, the young and the socially disadvantaged.

In the previous Sections of this report we have considered the emerging applications of AI in medicine and healthcare and some of the broader lessons emerging from the COVID-19 crisis. Whilst taking a European perspective, we must not forget that there are many differences in Europe among and within the Member States, so opportunities and impacts are not equally distributed.

12.1 National and regional variations

The starting point is to remember that there are significant variations across Europe in terms of socio-economic characteristics, of which the Gross Domestic Product represents a crude but recognized indicator. According to Eurostat (2019) if the average GDP per person in 2018 was almost €31,000, only about one third of the European NUTS2 regions were above the European average, with a large number in the post-industrial regions of Northern and Eastern Europe and the peripheral regions of Southern Europe well below 75% of the European average as shown in Figure 6.

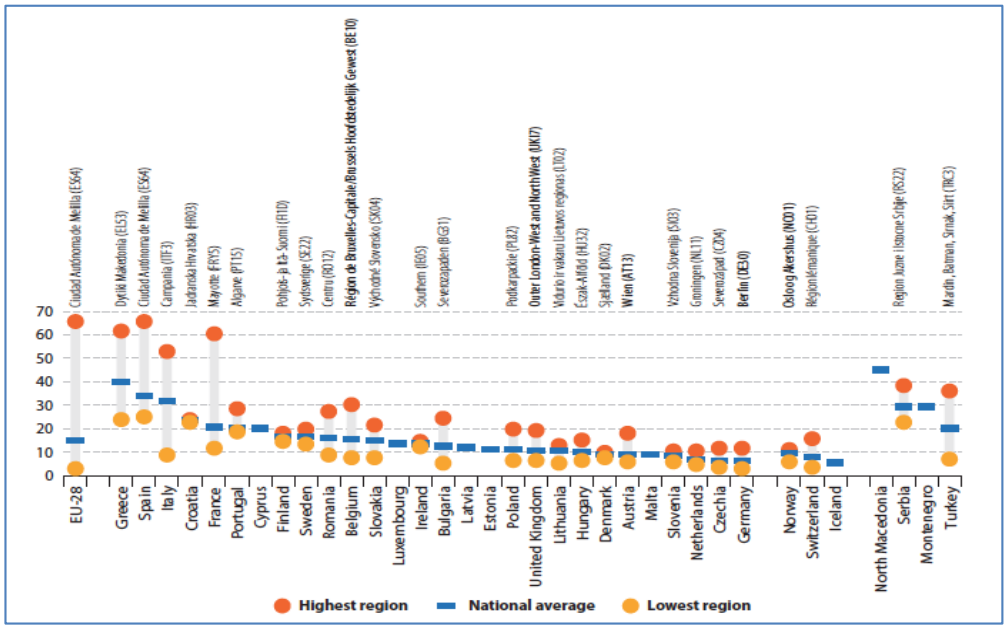
Figure 6: GDP per inhabitant 2017 by NUTS2 region



Source: EUROSTAT 2019

These differences reflect those in education and skills, and availability of opportunities for personal development. For example, the proportion of 15-24-year-olds not in education, employment or training was just under 17% across Europe in 2017, but ranged between from a low of 5.4% in the Netherlands to a high of 25% in Southern Italy. Similarly, youth unemployment, which for the EU stood at 15.2% in 2017, over twice the level for the adult population, varied very significantly, particularly in 16 regions of France, Italy, Spain Greece where it was higher than 50% as shown in Figure 7.

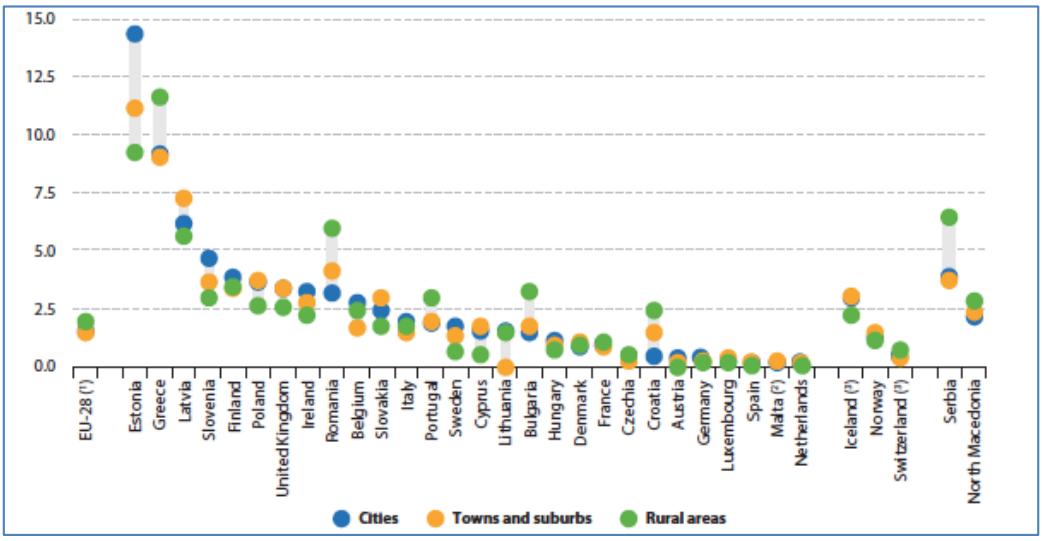
Figure 7: Youth unemployment rate, 2018.



Source: EUROSTAT, 2019

It is now widely accepted that GDP is not a good measure of wellbeing and a broader set of indicators is needed, including subjective measures of inequality and wellbeing (OECD, 2018). Given the focus of this report on the lessons learned from COVID-19, it is therefore important to recognize the differences in Europe across other domains such as the provision of healthcare. As an example, Figure 8 shows the European variations in the percentage of the population aged 16 and over with unmet medical needs, as well as the in-country variations between urban and rural areas.

Fig 8: Percentage population with unmet medical examinations



Source: EUROSTAT, 2019

It is interesting to note that against an EU average of 1.7% of the population with unmet medical needs, about one third of the countries score higher with significant urban-rural differences particularly in Estonia, Greece, and Romania. Italy and Spain in particular, feature much better in the comparison of healthcare than in socio-economic indicators.

12.2 Sub-regional variations

Whilst the section above starts unpacking the European perspective reminding us of how varied the European landscape is, it is equally important to acknowledge the variations within Member States. Italy for example, had a national unemployment rate of 10% in 2019. Seventy percent of its 110 provinces were below the national average, twenty percent had unemployment levels between 10% and 20%, and ten percent more than twice the national average. The lowest value was less than 3% and the highest almost 30% (ISTAT, 2019).

Youth unemployment in Italy in 2019 stood at almost 30%, split almost 50-50 between provinces below and above the average. The lowest level was 8.4% and the highest 68.5%, so more than twice the national average. 10% of provinces had more than half their 15-24 years old unemployed, with consistently higher numbers among females (ISTAT, 2019). These numbers exemplify the range of inequalities still existing in many European countries between different regions, and between rural and urban areas, and the policy challenges to give equal opportunities to all, but in particular to the European youth.

12.3 The socio-economic impacts of the COVID-19 crisis.

The economic impact of the COVID-19 crisis is as yet unknown but has been estimated by the OECD to range between -6% and -7.6% of GDP for the world as a whole under a more positive scenario of no resurgence of the infections in the Autumn, and a more pessimistic one including a second wave. For the OECD countries the estimates range between -7.5% and -9.8% under the two scenarios respectively, with Spain, France, Italy and the UK as the worst hit countries with estimates between -11% and -14% (OECD, 2020).

The social implications of this massive world-wide down-turn in the economy in terms of lost lives, and human suffering is also difficult to estimate but is likely to disproportionally affect the most vulnerable groups including the elderly, people with disabilities, the youth, indigenous people, migrants and refugees, and the homeless according to the United Nations (2020), which calls member countries to step up to the challenge with an inclusive approach.

From a European perspective, the European Commission has recognized the magnitude of the challenge and proposed a comprehensive recovery package[31] being negotiated with the Council and the European Parliament at the time of writing.

Against this background, previous sections of this report discussed the implications of the massive shift towards online communications resulting from the lock down. These included increased dependency on (non-European) platforms (Section 10) and the increased cybersecurity threat this poses (Section 11). Another important thread of the discussion related to the increasing adoption of technological means including, AI powered-ones, to trace people and alert authorities and individuals about the risk of new infections (Section 6).

The broad socio-economic differences in Europe, highlighted in previous parts of this Section, also affect the nature, extent and geographical and social distribution of the impacts of life online. We highlight below two aspects in particular: access to technology and knowledge, and impacts on education.

12.4 Everybody online?

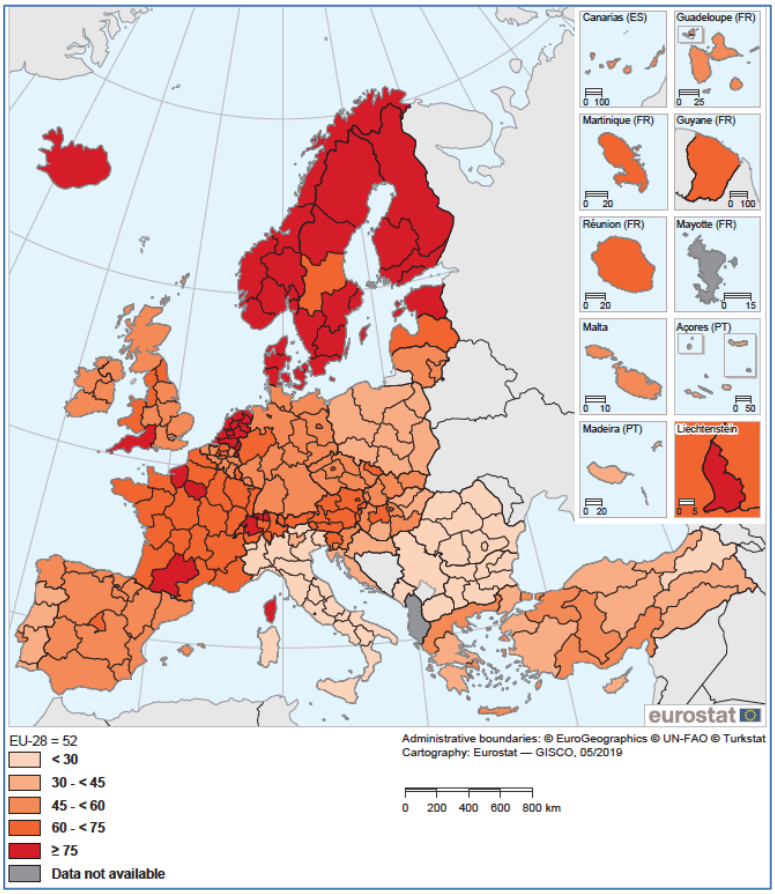
Whilst digital technologies have provided enormous help during the lock down it is important to recognize that even in the EU not everyone is able to afford or master digital technology. For example, the Special Eurobarometer Survey[32] of December 2019 indicated that almost 30% of EU citizens do not feel that they have sufficient skills to use digital technologies in their daily life. This varies from 12-13% in the Netherlands and the Nordic countries, to 40% in Italy and Greece. People in lower income groups, the elderly, women and people living in rural areas are at a greater disadvantage in the use of digital technologies. What is particularly worth noting is that compared to the survey in 2017, the proportion of people who consider themselves to be sufficiently skilled in the use of digital technologies in their daily life has declined in 19 countries, particularly Italy (-11%), France and Lithuania (both -6%). This may mean that people in these countries feel increasingly

[31] https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/recovery-plan-europe_en
[32] https://data.europa.eu/euodp/en/data/dataset/S2228_92_4_503_ENG

less equipped to cope with the speed of technological development. Whilst lack of time is cited by the majority of people in work for their inability to upgrade their skills, cost is the main reason for those who are unemployed.

Access to technology (computers, phones, broadband) and skills are two key components in the ability of people to cope with work, education, and access to services, but national policies also have a role to play. According to EUROSTAT (2019), just over half of the EU population interacted regularly with public authorities over the Internet. As shown in Figure 9, the regional distribution sees the population of Bulgaria, Italy and Greece particularly penalised with less than 30% able to interact with their public authorities via the Internet, which at a time of crisis such as COVID-19 may have caused particular strains.

Figure 9: Percentage people interacting with their public authority over the Internet, 2018.



Source: EUROSTAT, 2019

12.5 The lock down and education

In most countries, governments closed schools temporarily to try and reduce the spread of the COVID-19 virus. This affected more than 1 billion pupils, almost 70% of the world student population according to the UNESCO[33]. Policies varied between countries that implemented a national closure, or a localised closure. The length of closure also varied between a few weeks to three months. There is an increasing body of research on the impact of these closures on learning and future earning potential. For example, Burgess and Sievertson (2020) argue that even a relatively short period of missed school will have consequences for skill growth, while Porter (2020) argues that if the return of investment of an additional year of education is approximately 8-10%, and the average student misses one quarter of the school year, then one might estimate a permanent impact on earnings of 2% to 2.5%.

Impacts are not uniformly distributed, affecting poorer families most, thus exacerbating inequalities. For example, Bol (2020) through a panel survey in the Netherlands found that families from poorer backgrounds have fewer resources for home schooling such as independent space for studying and access to PCs or tablets

[33] https://en.unesco.org/covid19/educationresponse

(34% of pupils in primary education), and fewer capabilities to help with homework, particularly for secondary level students. Moreover, parents seem more able to support girls than boys who tolerate less well home work. He concluded that "the first results of this data collection provide strong indications that the school shutdown caused by the COVID-19 pandemic will increase existing inequalities in education. Children from disadvantaged families received much less support from their parents, which is likely to have impeded the learning during this period" (Bol, 2020, pg. 15).

Similar findings are reported by Montacute (2020) for the UK indicating that according to previous research by the Sutton Trust just over one third of parents with children in the ages 5-16 reported that their child does not have access to their own computer, laptop or tablet to use for accessing the Internet at home. Lack of independent space to study among poorer children living in cramped conditions is an additional factor affecting learning outcomes. Likewise, the Italian national statistical agency (ISTAT, 2020) reports that one third of Italian families do not have a computer or tablet at home, rising to over 40% in Southern Italy. Moreover, four out of ten minors live in overcrowded accommodation.

The combined effect of limited access to infrastructure, the Internet, lack of adequate skills, and independent space to study as well as more limited support from parents is likely to have indeed increased social inequalities and may have long lasting consequences if remedial action is not put in place. Moreover, it should also be considered that teachers and schools were also caught unprepared in many countries to move all their teaching online. Most managed to address the challenge with remarkable commitment and ingenuity, but now need support to institutionalise the digital transition. For a fuller discussion of the impact of COVID-19 on education see Di Pietro et al. 2020.

13 Summary and conclusions

M. Craglia

In this report we have explored the potential contribution of AI to the challenges posed by the COVID-19 crisis as well as the multiple issues that are raised in the interplay between technology, data, and society at stress times like these. We summarise below the key findings and then compare them to those of the JRC report on AI (Craglia et al. 2018) to draw some conclusions and lessons learned.

In Section 2, de Nigris and Craglia reported on the increased attention towards the applications of AI in healthcare by both governments and companies, with a significant increase in the research domain since the beginning of 2020 in response to the COVID-19 crisis. We are nevertheless at the early stages of AI adoption and use, particularly in the public sector and in health, due to the sensitive nature of medical data, the difficulty of bringing this data together and the major organisational and cultural changes needed in such a complex sector. The establishment of a common European data space for health (EC, 2020c) may help to address these issues, but "all other things being equal", it is likely to take some time for AI to become a major contributor in this domain.

The COVID-19 crisis has changed the landscape as argued by Gómez-González and Gómez in Section 3, and may act as a boost to the adoption of AI. Areas of application singled out as benefiting from AI are telemedicine with remote consultation of patients by physicians, data driven algorithms to support medical diagnosis, epidemiological studies, social interaction and support, and clinical management of patients, personalized medicine and the increased acceptance of robots to support remote handling in contaminated environments as well as patients in isolation. Each of these very promising areas of application boosted by the COVID-19 crisis, carries some risk particularly with respect to the way sensitive medical data is collected, analysed and used. Who controls the information generated and for what purpose are key issues as we live in a society in which misinformation is used tactically and strategically to achieve economic and political aims. In addition, the COVID-19 crisis has highlighted the inherent tensions between individual rights and social good.

These tensions are analysed by Martens in Section 4 in the context of access to private data from two perspectives: individual citizens and companies. With respect to the former, the COVID-19 crisis has emphasized the role of the State in leading the response and taking measures that have restricted individual liberties for public good. As Martens argues, different societies will take different views of what is legitimate or appropriate: those that emphasise collective and social values will put more restrictions on individuals, those that emphasis individual liberties will put fewer. We have seen these variety of approaches with respect to the modalities of lock down and access to individuals' data within Europe, and between Europe and other parts of the world. With respect to the relationship between governments and the commercial sector, there has been increasing discussion at the European level on access to commercial data for the public good. These discussions had in the past been rather difficult on the grounds of commercial confidentiality but have been given a boost by the COVID-19 crisis, as exemplified in Section 6.

The COVID boosting effect is highlighted also by Iglesias in Section 5 with examples of how companies and governments are making considerable efforts to increase their collaboration and the sharing of Intellectual Property (IP) and data to fight together the crisis, speed up research and innovation, and facilitate global and equitable access to vaccines, therapeutics and medical devices. Future action to facilitate data access and sharing, either through voluntary or compulsory mechanisms, should aim at providing incentives as well as safeguards to the parties concerned and ensuring there are no unjustified obstacles to data sharing, in particular in case of a public health emergency.

Vespe in Section 6 gives a practical example of this new willingness to work together by introducing the collaboration between mobile phone network operators and the European Commission. A letter by the European Commission to the CEOs of these companies requesting access to anonymized and aggregate data to help fight the pandemic was accepted by some 20 companies that provided the requested data without delay. The scale and rapidity with which this data was provided to the JRC for analysis in a dedicated infrastructure are rightly underlined by Vespe because past efforts in this field had often failed on grounds of commercial confidentiality and data sensitivity.

Schade, Micheli and Kotsev analyse, in Section 7, one of the more emblematic data-related aspects of the COVID response: contact tracing apps on mobile phones. These apps are supposed to complement manual efforts to trace individuals who may have come into contact with individuals or environments found to be infected in order to alert them, test them and contain further spread of the virus. Most European governments started developing these apps with an approach designed to collect all the data centrally to increase their ability to monitor the evolution of the pandemic. The alliance of Google and Apple for a decentralized solution that instead stores all the data on the mobile phone on the grounds of increased privacy for the users has forced most governments to change their plans and follow this approach. This shows the power of big tech, leveraging privacy concerns to force governments to change policy. Ironic given past events, such as the Cambridge Analytica scandal, that had put big tech under increased scrutiny on those same grounds.

Privacy and ethical concerns raised by the use of technology, including tracing apps, are the focus of Vesnic-Alujevic and Pignatelli in Section 8. They caution us against the widespread use of technology and the collection of personal data, including location, to fight the pandemic without due democratic scrutiny and societal debate. Necessary measures of surveillance taken to respond to an emergency could turn into a threat to democracy if they became institutionalised beyond the emergency. There is cause to raise the issue and the level of vigilance as some European countries have announced derogations from the European Convention on Human Rights, or have declared a state of emergency including limitations of free speech. Deliberative public participation and agency should instead remain at the base of the European project and we should collectively protect these rights.

A good example of how AI can be applied to administrative data without intruding into people's privacy is provided by Hradec in Section 9. The context of this application is work supporting the JRC Coronavirus Task Force, which was set up at the JRC to provide analyses and models informing the action of the European Commission. The analysis he describes used an approach developed in the Digitranscope research project of the JRC's Centre for Advanced Studies. It uses machine learning methods to distribute all the official data available for statistical areas (gender, age, family composition, conditions of the buildings) to a set of "statistical" individuals so that when aggregated into families and households they return the same data as that of official statistics. Using this fine-grained distribution of official administrative data, it was possible to model the relative risk of reopening the economy by economic sector, and the social and geographical distribution of potential impacts. Beyond the contingent usefulness of this application to inform governments, its value is to show how it is possible to get new insights from existing data through AI methods.

The ability of the Internet to scale up to the challenge of a massive shift to online life is discussed by Nativi in Section 10. The architectural design of the Internet protocols, technology, and governance arrangements made it possible to support the sudden jump in demand resulting from the lock down. This was also supported by open collaboration among key providers supporting, for example, the request of the EC to downgrade the level of service to ensure connectivity. The positive result of this unexpected stress test of the network is mitigated by Nativi in pointing out that as every business, government, education, research, and social activity moved online, we all came to rely exclusively on non-European collaborative platforms. This should be of concern from the perspective of technological and data sovereignty in view of the large amount of intelligence provided to these platforms about European business and social structures, processes, and organisations. This suggests that future European policy should also consider the sovereignty and security of software applications.

The increased cybersecurity risks arising from the increased reliance on digital instruments during the lock down are analysed by Hamon, Junklewitz and Sanchez in Section 11. They focus in particular on two aspects: the increased number of cyberattacks, which do not appear to have had severe consequences on critical infrastructure or the health system according to initial evidence, and the increasing use of AI in both cyberattacks and cybersecurity. They underline the increased number of coordinated disinformation campaigns and deepfakes to advance political aims by undermining trust in European governments and the EU. The potential of AI in supporting cybersecurity applications, as well as its potential for being exploited and misused by cybercriminals, indicate that AI will become even more critical in the capacity of our societies to preserve their digital integrity.

Whilst previous Sections have taken a European perspective of the opportunities and potential impacts of AI emerging from the COVID-19 crisis, Section 12 reminds us that Europe has a great deal of variety. This is one of its charms and a great source of strength and inventiveness, but needs to be considered carefully with respect to the geographic and social distribution of both benefits and impacts. This is important because the economic and social consequences of the economic down-turn caused by the COVID-19 are likely to be long-lasting, and affect disproportionately more the vulnerable groups in society, including the elderly, and the young. For example, some 30% of Europeans do not feel they have sufficient skills to master digital technologies in their daily life. This affected in particular the elderly and the poor during the crisis when most interactions, even with local public administrations, moved online. Likewise, emerging research shows that children from disadvantaged backgrounds suffered more the impacts of school closures and online teaching as they often lacked computers or tablets to do their homework, independent space to study, and sufficient parental support. These impacts could be long-lasting if no remedial action is taken and is targeted to those who need it most.

In the JRC report on *Artificial Intelligence: a European Perspective* (Craglia et al. 2018) we concluded that AI is a general-purpose technology entering our every-day lives and increasingly deployed in industry, government, commerce and research. As Europeans we need to be mindful of the global competition on AI focused on technology, data, and skills and find our own way to develop and use AI so that it strengthens the founding values of the EU such as democracy, and non-discrimination, and is based on a robust ethical framework and trust. In the report we noted that if no positive action was taken, it was likely that the adoption and use of AI could exacerbate existing social and economic inequalities. For this reason, we argued that in addition to the legal and ethical framework and a robust computing infrastructure, there was a need to develop rich ecosystems of data at European and local level to strengthen the resilience of society and build trust with applications responding to the economic and social needs of all levels, from local to European.

Only eighteen months have passed since the publication of that report and much has happened since. The new European Commission took office in December 2019 and identified the digital and environmental challenges as its top priorities. Within the former, AI as well as technological and data sovereignty play a key role. The Commission enacted a European strategy for data establishing several common European data spaces in key areas, has launched a broad consultation on a regulatory framework for AI and is preparing to invest in key infrastructure, cybersecurity and skills through the Digital Europe Programme. The new Horizon Europe research programme will also contain many actions supporting this digital agenda.

…..and then came COVID-19.

It may have been circulating in Europe since November or December 2019, but it was only recognized as a pandemic in March 2020. Four months into this global crisis we can recognize from the contributions to this report that COVID has acted as booster to the adoption of AI and as an amplifier of potential opportunities and threats.

As a booster, we noted increasing adoption and use of AI in scientific and medical research, in applications like telemedicine, medical diagnosis, epidemiological studies, and clinical management of patients as well as greater acceptance of robots in the workplace. During the more acute phases of the crisis, there also seemed to be a shift in public attitudes towards a greater acceptance of data collection for research and monitoring of the spread of the infection. Similarly, we noted how the COVID-19 crisis made it possible to overcome previous barriers in the sharing of data between commercial entities, and between business and governments. This pulling together for the collective benefit of society is a very positive outcome of the crisis, and it will be interesting to see in the future the extent and the ways in which it will continue after the crisis is over.

COVID has also boosted the digital transition of companies, public administrations, and educational establishments. Plans that had maybe dragged on for years, had to be implemented at very short notice, overcoming many technological, organisational, skill gaps, and cultural barriers. How this transition will be institutionalized, what proportion of leisure, education and work will continue to take place online in the post-COVID period is an open question.

As an amplifier of pre-existing concerns, the COVID-19 crisis has underlined the absolutely critical role of the governance of digital data in modern societies. Without well-structured and semantically rich data it is not possible to harness the opportunities afforded by AI. How data is collected, by whom, for what purpose, how it is accessed, shared and re-used have become central questions during the COVID-19 crisis. As shown in this report, we have seen positive examples of pulling resources together by commercial organisations and the public sector for collective benefits, but we have also noted the increasing risks of mass surveillance without adequate public scrutiny, as well as the increasing use of organised misinformation campaigns to undermine

social cohesion and democratic values. Data sovereignty through well informed, transparent public action and active social engagement emerges therefore as a crucial issue.

A particular aspect of sovereignty relates to security. The increasing use of AI for cyberattacks including the creation of deepfakes that could deliberately alter data used to train algorithms, alerts us that we need to pay additional attention to the security of the many data spaces the EU prepares to establish in the key domains of health, environment, mobility, manufacturing, finance, energy, agriculture, and public administration under the European Strategy for Data (EC, 2020c).

Another aspect of sovereignty exposed by the lock down is the dependency on non-European collaborative platforms. These platforms have become a critical layer of the digital infrastructure connecting users, processes, organisational structures, applications and content. Through their use we provide valuable intelligence to the platform operators that can use it for profiling, targeting, and manipulation. Technological and data sovereignty needs to include this technological layer as well. Worrying about the foreign ownership of the physical digital infrastructure and not about the platform layer would leave a big security gap.

A final dimension amplified by COVID-19 is the extent to which the AI and the digital transformation exacerbate existing social, economic, and geographical inequalities, affecting in particular the most vulnerable in society: the elderly, youth, and people from social or economically disadvantaged groups. The report has given evidence of this concern suggesting a proactive approach by public policy to support these groups. In Craglia et al. (2018) we had argued for support to local data ecosystems bringing together public administrations, local companies, education establishments, and civic society, addressing local problems whilst providing increased training and local job opportunities. In this report we have also seen that AI methods can also be used effectively to model need at a very fine-grained level. These methods can be developed further to design and deliver policy intervention where it is needed most.

In conclusion, the COVID-19 pandemic has caused something akin to a natural experiment. It has exposed us to unforeseen and unprecedented conditions, forcing us to react in ways unimaginable just six months ago. With respect to AI, data, and the digital infrastructure, which have to be considered all together as a socio-technical package, the pandemic is acting as a boost to AI adoption and the digital transition, creating new opportunities but also amplifying concerns over data governance, security, and increasing inequalities.

Recognising these early signals, we can use the many policy initiatives already in the making to strengthen the European technological and data sovereignty and address the increasing inequalities so that the European way to digital transformation is more inclusive and supportive of the founding values of the EU. Not just bouncing-back to pre-COVID-19 normality, but bouncing-forward to a more resilient and just society.

References

Abrams, L. *Over 500,000 Zoom accounts sold on hacker forums, the dark web*. April 13. 2020. https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/

Ada Lovelace Institute. *Exit through the App store?* 2020 Retrieved from https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf

Ahmed, D. *Hackers are actively targeting WHO amid Coronavirus pandemic*. hackread.com. March 25. 2020. https://www.hackread.com/hackers-are-actively-targeting-who-amid-coronavirus-pandemic/

Albergotti, R. European government officials call for tech companies to loosen grip on contact-tracing technology. *The Washington Post*. 2020. https://www.washingtonpost.com/technology/2020/05/29/apple-google-contact-tracing/

ANSA. In un asilo di Varese il braccialetto per il distanziamento a 150 bimbi. *Legalita' e scuola*, 6 May 2020. Retrieved from https://www.ansa.it/canale_legalita_scuola/notizie/scuole/2020/05/06/in-asilo-varese-bracciale-per-bimbi_74775209-5ce4-428c-ac0a-f3418d674c52.html

Arnould, V. Human rights matter more than ever in the COVID-19 era, *Egmont*, 17 April 2020 http://www.egmontinstitute.be/human-rights-matter-more-than-ever-in-the-covid-19-era/

Baraniuk, C. The groundbreaking way to search lungs for signs of COVID-19. *BBC News*. 2020. https://www.bbc.com/news/business-52483082

Bengio, Y., Janda, R., Yu, Y. W., Ippolito, D., Jarvie, M., Pilat, D., Struck, B., Krastev, S., & Sharma, A. The need for privacy with public digital contact tracing during the COVID-19 pandemic. *The Lancet Digital Health*. 2020. https://doi.org/10.1016/S2589-7500(20)30133-3

Bergman, A., & Iyengar, J. How COVID-19 is affecting internet performance. Retrieved from *Fastly* 8 April 2020: https://www.fastly.com/blog/how-covid-19-is-affecting-internet-performance

Bethune Z. and Korinek A. Covid 19 infection externalities: trading off lives vs livelihoods, NBER Working Paper 27009, April 2020.

Bhak, A., Bayulgen, O., Blum, H., Ford, F., & Van de Weyer, C. Telcos and Coronavirus: Three Steps to Manage the Crisis. Retrieved from *Bain & Company* 25 March 2020: https://www.bain.com/insights/telcos-and-coronavirus-three-steps-to-manage-the-crisis/

Bol, T. Inequality in homeschooling during the corona crisis in the Netherlands. First results from the LISS panel, SocArXiv 2020.

Brennen, J.S., Simon F. M., P. N. Howard, and R.K. Nielsen. Types, sources, and claims of COVID-19 misinformation. *Reuters institute*. 2020. https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation

Bullock, J., Luccioni, A., Hoffmann Pham, K., Sin Nga Lam, C., & Luengo-Oroz, M. *Mapping the Landscape of Artificial Intelligence Applications against COVID-19*. 2020. https://arxiv.org/abs/2003.11336

Bundage, M. et al. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, OpenAi. 2018.

Burgess, S and H. Sievertsen. "Schools, skills, and learning: The impact of COVID-19 on education", VoxEU.org, 1 Apri 2020.

Canadian Centre for Cyber Security. *Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threat Activity*. 2020. https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-impact-covid-19-cyber-threat-activity .

Carter, R. COVID-19: Ultimate Guide to Free Video Conferencing & Collaboration. Retrieved from *UCTODAY* 16 March 2020: https://www.uctoday.com/collaboration/video-conferencing/covid-19-ultimate-guide-to-free-video-conferencing-collaboration/

CB Insights *What Is Psychographics? Understanding The Tech That Threatens Elections*. 2020b. https://www.cbinsights.com/research/what-is-psychographics/

CB Insights. *How Covid-19 Is Pushing Healthcare Stakeholders, Governments, And Tech Giants To Innovate*. 2020a. https://www.cbinsights.com/research/covid-19-healthcare-initiatives/

CERT-EU. *Threat Landscape Report* Executive Summary-v1.0. CERT-EU. 2020a.

CERT-EU. CERT-EU-MEMO *Attacks on Healthcare* CERT-EU. 2020b. https://media.cert.europa.eu/static/MEMO/2020/TLP-WHITE-CERT-EU-MEMO-Attacks-on-Healthcare.pdf

CERT-EU. *COVID-19, Threat Memo* - TM 20-033, Version 3.0, 25 March 2020. CERT-EU. 2020c

CERT-EU. *CERT-EU THREAT ALERT: Coronavirus cyber exploitation:* CERT-EU. 2020d. https://media.cert.europa.eu/static/MEMO/2020/TLP-WHITE-CERT-EU-THREAT-ALERT-Coronavirus-cyber-exploitation.pdf

Chandran, R. Analysis: Pragmatic" Asia fast-tracks hi-tech coronavirus solutions. *Reuters*. 2020. https://www.reuters.com/article/us-health-coronavirus-tech-trfn/analysis-pragmatic-asia-fast-tracks-hi-tech-coronavirus-solutions-idUSKBN2132ZP .

Cho H., Ippolito D. and Yu Y.W. *Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs*. 2020. https://arxiv.org/abs/2003.11511

Cimons, M. Disinformation during a pandemic can be deadly. *Popular Science*. 2020. https://www.popsci.com/story/science/disinformation-pandemic-disasters/

Clarke L. PEPP-PT vs DP-3T: The coronavirus contact tracing privacy debate kicks up another gear. *New Statesman Tech*. Retrieved 15 July 2020. https://tech.newstatesman.com/security/pepp-pt-vs-dp-3t-the-coronavirus-contact-tracing-privacy-debate-kicks-up-another-gear

Cliffe, J. The rise of the bio-surveillance state. A grim choice faces 21st-century societies: panopticons or pandemics? *New Statesman*, 25 March 2020. Retrieved from https://www.newstatesman.com/science-tech/2020/03/rise-bio-surveillance-state

Cooney, M. Why didn't COVID-19 break the internet? Retrieved from *NETWORKWORLD*: 30 April 2020 https://www.networkworld.com/article/3541357/why-didnt-covid-19-break-the-internet.html

Council of Europe. *The Council of Europe continues working to enhance international co-operation against terrorism, including bioterrorism*. 2020. https://www.coe.int/en/web/counter-terrorism/-/covid-19-pandemic-the-secretariat-of-the-committee-on-counter-terrorism-warns-against-the-risk-of-bioterrorism .

Cox, J. Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account. Retrieved from *Vice Media Group* 26 March 2020: https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account

Craglia M. (Ed.), Annoni A., Benczur P., Bertoldi P., Delipetrev P., De Prato G., Feijoo C., Fernandez Macias E., Gomez E., Iglesias M., Junklewitz H, López Cobo M., Martens B., Nascimento S., Nativi S., Polvora A., Sanchez I., Tolan S, Tuomi I., Vesnic Alujevic L., *Artificial Intelligence: A European Perspective*, Publications Office, Luxembourg, 2018. https://ec.europa.eu/jrc/en/publication/artificial-intelligence-european-perspective

Craglia M., Hradec J. and Troussard X. 2020. The Big Data and Artificial Intelligence: Opportunities and Challenges to Modernise the Policy Cycle Chapter 9 in Sucha V., and Sienkiewitz M. (Eds.) 2019 *Science for Policy Handbook*, Elsevier. 2020. https://www.sciencedirect.com/book/9780128225967/science-for-policy-handbook

Criddle, C.,and Kelion, L., Coronavirus contact-tracing: World split between two types of app. *BBC News*, Published 7 May 2020 https://www.bbc.com/news/technology-52355028

Cummins, E. Meditation apps want to calm you down on the same device that stresses you out. *Popular Science*. 2020. https://www.popsci.com/mindfulness-meditation-apps/

Davidson, J. Global Traffic Spikes. No Panic at the Cisco! Retrieved from *CISCO Blogs* 26 March 2020: https://blogs.cisco.com/news/global-traffic-spikes-no-panic-at-the-cisco

DE-CIX. Big upswing in Internet usage due to Covid-19 measures. Retrieved from *DE-CIX* 19 March 2020: https://www.de-cix.net/en/news-events/news/big-upswing-in-internet-usage-due-to-covid-19-measures

Deleuze, G. Postscriptum on the societies of control. *L'autre journal*, N.1, May 1990. English version. https://cidadeinsegurancafiles.wordpress.com/2012/02/deleuze_control.pdf.

De Nigiris S. Craglia M. Nepelski et al. AI Watch sector dive on health 2020. European Commission (forthcoming) 2020.

Dingel J.I. and B. Nieman. *How many jobs can be done at home?* White Paper. Becker Friedman Institute for Economics at UChicago. 2020 https://bfi.uchicago.edu/wp-content/uploads/BFI_White-Paper_Dingel_Neiman_3.2020.pdf

Di Pietro, G., Biagi, F., Costa, P., Karpiński Z., Mazza, J, *The likely impact of COVID-19 on education: Reflections based on the existing literature and international datasets*, EUR 30275 EN, Publications Office of the European Union, Luxembourg , 2020.

Doffman, Z. Coronavirus Police Surveillance Tags Are Now Here: Hong Kong First To Deploy. *Forbes*. 2020. https://www.forbes.com/sites/zakdoffman/2020/03/17/alarming-coronavirus-surveillance-bracelets-now-in-peoples-homes-heres-what-they-do/#54b758474533 .

Dubal, V. The expansion of mass surveillance to stop coronavirus should worry us all. *The Guardian*, 18 April 2020. Retrieved from https://www.theguardian.com/commentisfree/2020/apr/18/mass-surveillance-coronavirus-technology-expansion

ELLIS Society. *ELLIS against Covid-19*. 2020. https://ellis.eu/covid-19/projects

Eurobarometer Special Survey 503. Attitudes towards the impact of digitalization in daily lives. European Commission. 2020. https://data.europa.eu/euodp/en/data/dataset/S2228_92_4_503_ENG

European Commission. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 2016.

European Commission. *Better Regulation Guidelines*. Staff Working Document SWD(2017) 350. 2017.

European Commission. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: *Coordinated Plan on Artificial Intelligence* COM(2018) 795 final, 2018a.

European Commission. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: *Artificial Intelligence for Europe* COM(2018) 237 final, 2018b.

European Commission. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on *enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society*. COM(2018) 233 final, 2018c.

European Commission. *Shaping Europe's Digital Future*. 2020a https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

European Commission. White Paper on Artificial Intelligence: A European approach to excellence and trust. COM (2020)65 Final. 2020b.

European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *A European Strategy for Data*. COM(2020)66 final. 2020c

European Commission. *Scams related to COVID-19*. 2020d. https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/scams-related-covid-19_en .

European Commission. *Coronavirus: EU strengthens action to tackle disinformation*. 2020e. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1006 .

European Commission. *Digital technologies – Innovative solutions during the coronavirus crisis*. 2020f. https://swissmodel.expasy.org/repository/species/2697049 .

European Commission. Towards a European strategy on business-to-government data sharing for the public interest, Report of the B2G expert group. 2020g.

European Commission. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on *Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*, C(2020) 2523 final, 2020h.

European Commission. EU toolbox with the eHealth Network for the use of mobile applications for contact tracing and warning, 15 April 2020k.

European Commission. Recommendation (EU) 2020/518 on a common approach (voluntary) for the use of technology and data to combat and exit from the crisis, 8 April, 2020j.

European Commission. Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics - COM(2020) 64 final – 2020m

European Data Protection Supervisor, Gasser, U., Ienca, M., Scheibner, J., Sleigh, J., Vayena, E. Digital tools against COVID-19: Framing the Ethical challenges and how to address them. *Computers and Society*. 2020. https://arxiv.org/abs/2004.10236

European Union Agency for Fundamental Rights. *Coronavirus pandemic in the EU - Fundamental rights implications: with a focus on contact-tracing apps. 2020*. https://fra.europa.eu/en/publication/2020/covid19-rights-impact-may-1

European Union Labour Force Survey. *Eurostat*. 2019. Version 2 https://doi.org/10.2907/LFS1983-2018V.2

Europol. Corona crimes: *Suspect behind €6 million face masks and hand sanitisers scam arrested thanks to international police cooperation*. 6 April 2020. https://www.europol.europa.eu/newsroom/news/corona-crimes-suspect-behind-6Û-million-face-masks-and-hand-sanitisers-scam-arrested-thanks-to-international-police-cooperation.

Europol. Pandemic profiteering: how criminals exploit the COVID-19 crisis. 2020.

Fast, E., & Chen, B. *Potential T-cell and B-cell Epitopes of 2019-nCoV*. BioRxiv. 2020. https://www.biorxiv.org/content/10.1101/2020.02.19.955484v1 .

FBI Boston. FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic. Retrieved from *FBI* 30 March 2020: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

Finlayson, S. G., H., W. Chung, I.S. Kohane, and A. L. Beam. *Adversarial Attacks Against Medical Deep Learning Systems*. arxiv. 2019. https://arxiv.org/pdf/1804.05296.pdf

Floridi, L. Mind the app. Considerations on the ethical risks of COVID-19 apps. Blog post. *Onlife*. Published 18 April 2020. https://thephilosophyofinformation.blogspot.com/2020/04/mind-app-considerations-on-ethical.html

Flynn, S., Geiger, C., and Quintais, J.P., *Implementing user rights for research in the field of artificial intelligence: a call for action at the international level*, published 20 April, 2020, http://infojustice.org/archives/42260

Fuchs, C. *Communication and capitalism. A critical theory*. University of Westminster Press. 2020.

Galindo, G. XR *Belgium posts deepfake of Belgian premier linking Covid-19 with climate crisis*. April 14. 2020. https://www.brusselstimes.com/all-news/belgium-all-news/politics/106320/xr-belgium-posts-deepfake-of-belgian-premier-linking-covid-19-with-climate-crisis/

Gargiulo, F., Ternes, S., Huet, S., & Deffuant, G. An iterative approach for generating statistically realistic populations of households. *PloS one*, *5*(1), e8828. 2010. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0008828

Ghebreyesus, T. A. *Urgent health challenges for the next decade [WHO Declaration, 13/1/2020]. World Health Organization*. 2020. https://www.who.int/news-room/photo-story/photo-story-detail/urgent-health-challenges-for-the-next-decade .

Giret, L. Microsoft ask developers to not break the Internet with Xbox game updates. Retrieved from *OnMSFT* 26 March 2020: https://www.onmsft.com/news/microsoft-ask-developers-to-not-break-the-internet-with-xbox-game-updates

Glover A., Heathcote J., Krueger D. and Ríos-Rull J.V. *Health versus wealth: on the distributional effects of controlling a pandemic*. NBER working paper 27046, April 2020.

Glyer, C., D. Perez, and S.: Miller, S. Jones. *This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits*. March 25. 2020. https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

Gómez-González, E., & Gómez, E. *Artificial Intelligence in Medicine and Healthcare: applications, availability and societal impact*. EUR 30197 EN, Publications Office of the European Union, Luxembourg, 2020. https://doi.org/10.2760/047666

Goodwin, B. *Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack*. March 22. 2020. https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus

Goud, N. *British Supercomputer ARCHER hit by a Cyber Attack*. 2020. https://www.cybersecurity-insiders.com/british-supercomputer-archer-hit-by-a-cyber-attack/.

Graham-Cumming, J. Internet performance during the COVID-19 emergency. Retrieved from *The Cloudflare Blog* 23 April 2020: https://blog.cloudflare.com/recent-trends-in-internet-traffic/

Graur, F., Radu, E., Al Hajjar, N., Vaida, C., & Pisla, D. 'Surgical Robotics—Past, Present and Future'. In *New Trends in Medical and Service Robots: Design, Analysis and Control* (pp. 159–171). Springer. 2018. https://doi.org/10.1007/978-3-319-59972-4_12

Guillou, I. Covid-19: How unprecedented data sharing has led to faster-than-ever outbreak research. *Horizon: The EU Research & Innovation Magazine*. Published on 23 March 2020, https://horizon-magazine.eu/article/covid-19-how-unprecedented-data-sharing-has-led-faster-ever-outbreak-research.html

Hao, K. Doctors are using AI to triage covid-19 patients. The tools may be here to stay. *MIT Technology Review.* 2020a. https://www.technologyreview.com/2020/04/23/1000410/ai-triage-covid-19-patients-health-care/

Hao, K. Nearly half of Twitter accounts pushing to reopen America may be bots. *MIT Technology Review*. 2020b. https://www.technologyreview.com/2020/05/21/1002105/covid-bot-twitter-accounts-push-to-reopen-america/

Harrari, J. N. The world after coronavirus. *Financial Times*, 20 March 2020. https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Hawkins, A. Alphabet's Sidewalk Labs shuts down Toronto smart city project. *The Verge*, 7 May 2020. https://www.theverge.com/2020/5/7/21250594/alphabet-sidewalk-labs-toronto-quayside-shutting-down

Health Data Hub. *Mission de préfiguration*. 2018. https://solidarites-sante.gouv.fr/IMG/pdf/181012_-_rapport_health_data_hub.pdf

Health Europa. *AI precision medicine mining finds 13 human COVID-19 risk genes*. 2020. https://www.healtheuropa.eu/ai-precision-medicine-mining-finds-13-human-covid-19-risk-genes/99851/

Heaven, W. D. Our weird behavior during the pandemic is messing with AI models. *MIT Technology Review*. 2020. https://www.technologyreview.com/2020/05/11/1001563/covid-pandemic-broken-ai-machine-learning-amazon-retail-fraud-humans-in-the-loop/

Hern. A. and Sabbagh D. Critical mass of Android users crucial for NHS contact-tracing app. The Guardian, 6th May 2020. Retrieved 15th July 2020. https://www.theguardian.com/world/2020/may/06/critical-mass-of-android-users-needed-for-success-of-nhs-coronavirus-contact-tracing-app

Horowitz, J. In Italy, Going Back to Work May Depend on Having the Right Antibodies. *The New York Times*. 2020. https://www.nytimes.com/2020/04/04/world/europe/italy-coronavirus-antibodies.html

Howell O'Neill, P., Ryan-Mosley, T., & Johnson, B., A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*. 2020. https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

Interpol. *Cybercriminals targeting critical healthcare institutions with ransomware*. April 4. 2020. https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

IPSOS for the European Commission. *European enterprise survey on the use of technologies based on artificial intelligence.* Luxembourg: Publications Office of the European Union, 2020.

Jacobs, A. App Shows Promise in Tracking New Coronavirus Cases, Study Finds. *The New York Times*. 2020. https://www.nytimes.com/2020/05/11/health/coronavirus-symptoms-app.html

Jaidka, K., Giorgi, S., Schwartz, H. A., Kern, M. L., Ungar, L. H., & Eichstaedt, J. C. Estimating geographic subjective well-being from Twitter: A comparison of dictionary and data-driven language methods. *Proceedings of the National Academy of Sciences*, 117(19), 10165–10171. 2020. https://doi.org/10.1073/pnas.1906364117

Johnson, B. Nearly 40% of Icelanders are using a covid app—and it hasn't helped much. *MIT Technology Review*, 11 May 2020. https://www.technologyreview.com/2020/05/11/1001541/iceland-rakning-c19-covid-contact-tracing/

Joint Statement on Contact Tracing: 19th April 2020. https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view

Kahn, J., & Hopkins, J. (Eds.). *Digital Contact Tracing for Pandemic Response*. Johns Hopkins University Press. 2020. https://doi.org/10.1353/book.75831

Kan, M. *Google: We're Blocking 18 Million COVID-19 Phishing Emails a Day*. April 17. 2020. https://www.pcmag.com/news/google-were-blocking-18-million-covid-19-phishing-emails-a-day

Keßler, C., & McKenzie, G. A geoprivacy manifesto. *Transactions in GIS*, 22(1), 3-19. 2018.

Kietzmann, J., L. W. Lee, I.P. MacCarthy, and T. Kietzmann. Deepfakes: Trick or Treat? *Business Horizons*. 2019.

Kim, M. S. South Korea is watching quarantined citizens with a smartphone app. *MIT Technology Review*. 2020. https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/

Klein, N. How big tech plans to profit from the pandemic. *Guardian*, 13 May 2020 https://www.theguardian.com/news/2020/may/13/naomi-klein-how-big-tech-plans-to-profit-from-coronavirus-pandemic

Klenk, Michael and Duijf, Hein and Engels, Christian, *Ethics of Digital Contact Tracing and COVID-19: Who Is (Not) Free to Go?* 2020. http://dx.doi.org/10.2139/ssrn.3595539

Lauwaert, L., Simonis, M. & Smuha, N. *Opinion – More debate on Coronavirus App is Needed*. 5 May 2020. https://www.e-ir.info/2020/05/05/opinion-more-debate-on-the-coronavirus-app-is-needed/

Lenormand, M., & Deffuant, G. Generating a synthetic population of individuals in households: Sample-free vs sample-based methods. *arXiv preprint arXiv:1208.6403*. 2012. http://jasss.soc.surrey.ac.uk/16/4/12.html

Li, C., & Lalani, F. The COVID-19 pandemic has changed education forever. This is how. *World Economic Forum* 29 April 2020: https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning /

Lin, L., & Martin, T. W. How Coronavirus is Eroding Privacy. *The Wall Street Journal*. 2020. https://www.wsj.com/articles/coronavirus-paves-way-for-new-age-of-digital-surveillance-11586963028

Lomas, N. Netflix and other streaming platforms urged to switch to SD during COVID-19 crisis. *TechCrunch* 19 March 2020: https://techcrunch.com/2020/03/19/keep-calm-and-switch-to-sd/

Lomas, N. YouTube goes SD streaming by default in Europe due to COVID-19. *TechCrunch* 3 march 2020: https://techcrunch.com/2020/03/20/youtube-goes-sd-streaming-by-default-in-europe-due-to-covid-19/

Long, C. Privacy and Pandemics. In Pistor, K. (ed.). *Law in Times of COVID*, pp. 89-98. Columbia Law School 2020. https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1239&context=books

Lubell, M., Heller, J., & MacSwan, A. Israeli defense ministry launches COVID-19 voice-test study. *Reuters*. 2020. https://www.reuters.com/article/us-health-coronavirus-israel-study/israeli-defense-ministry-launches-covid-19-voice-test-study-idUSKBN21B2YV

Lupton, D. Health promotion in the digital era: A critical commentary. *Health Promotion International, 30(1): 174-183*. 2015.

Ma L. and Srinivasan S. Synthetic population generation with multilevel controls: A fitness-based synthesis approach and validations. Computer-aided civil and infrastructure engineering. 30(2) 135-150. 2015. https://onlinelibrary.wiley.com/doi/abs/10.1111/mice.12085

Magalhaes, J.C. & Couldry, N. *Tech Giants Are Using This Crisis to Colonize the Welfare System*. 2020. https://www.jacobinmag.com/2020/04/tech-giants-coronavirus-pandemic-welfare-surveillance

Mann A. Starlink: Space-X's satellite internet project, 7th January 2020. *Space.com*. https://www.space.com/spacex-starlink-satellites.html

Marczak, B. a.-R. Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings. Retrieved from *The CitizenLab of Munk School of the University of Toronto* 20 March 2020: https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

Marr B. How the COVID-19 pandemic is fast-tracking digital transformation in companies. *Forbes*. 17th March 2020. https://www.forbes.com/sites/bernardmarr/2020/03/17/how-the-covid-19-pandemic-is-fast-tracking-digital-transformation-in-companies/#73be6999a8ee

McKeay, M. The building wave of internet traffic. *Akamai Security Intelligence & Threat Research 2020*: https://blogs.akamai.com/sitr/2020/04/the-building-wave-of-internet-traffic.html

McKinsey & Company. *Transforming healthcare with AI. The impact on the workforce and organisations*. 2020. https://eithealth.eu/wp-content/uploads/2020/03/EIT-Health-and-McKinsey_Transforming-Healthcare-with-AI.pdf

Mello, M. & Wang, C. Ethics and governance for digital disease surveillance. *Science*. 2020. https://science.sciencemag.org/content/368/6494/951.full

Memes That Kill: The Future Of Information Warfare. CB Insights. 2018. https://www.cbinsights.com/research/future-of-information-warfare/

Menni, C., Valdes, A. M., Freidin, M. B., Sudre, C. H., Nguyen, L. H., Drew, D. A., Ganesh, S., Varsavsky, T., Cardoso, M. J., El-Sayed Moustafa, J. S., Visconti, A., Hysi, P., Bowyer, R. C. E., Mangino, M., Falchi, M., Wolf, J., Ourselin, S., Chan, A. T., Steves, C. J., & Spector, T. D. Real-time tracking of self-reported symptoms to predict potential COVID-19. *Nature Medicine*. 2020. http://www.nature.com/articles/s41591-020-0916-2

Mickle, T., Copeland, R., & Schechner, S. Apple, Google to Turn Smartphones Into Coronavirus Tracking Devices. *The Wall Street Journal*. 2020. https://www.wsj.com/articles/apple-google-partner-on-coronavirus-contact-tracing-technology-11586540203

Milsom, L., Abeler, J., Altmann, S., Toussaert, S., Zillessen, H., & Blasone, R. *Survey of acceptability of app-based contact tracing in the UK, US, France, Germany and Italy*. 2020. https://osf.io/7vqq9/

Milusheva S. *Using Mobile Phone Data to Reduce Spread of Disease*, World Bank Policy Research Working Paper 9198, March 2020.

Misuraca, G., and van Noordt, C., *Overview of the use and impact of AI in public services in the EU*, Publications Office of the European Union, Luxembourg, 2020. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120399/jrc120399_misuraca-ai-watch_public-services_30062020_def.pdf

Mooney, P., & Juhász, L. Mapping COVID-19: How web-based maps contribute to the infodemic. *Dialogues in Human Geography*, 10(2). 2020. https://doi.org/10.1177/2043820620934926.

Montacute, R. *Social Mobility and COVID-19*, Sutton Trust Report, 2020.

Muncaster, D. *COVID19 Drives Phishing Emails Up 667% in Under a Month*. March 26. 2020. https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/

Naughton, J. Contact apps won't end lockdown. But they might kill off democracy. *The Guardian*, 25 April 2020 https://www.theguardian.com/commentisfree/2020/apr/25/contact-apps-wont-end-lockdown-but-they-might-kill-off-democracy

NCCGroup. *Deepfake attack threat during Covid19*. March 27. 2020. http://www.mynewsdesk.com/nccgroup/news/deepfake-attack-threat-during-covid-19-398391

Nicolls D. How Covid-19 is shaping digital transformation: A small silver lining in the midst of the pandemic. *Techradar* 7th April 2020. https://www.techradar.com/news/how-covid-19-is-shaping-digital-transformation

OECD. *Beyond GDP: Measuring what counts for economic and social performance*. 2018. https://www.oecd-ilibrary.org/sites/9789264307292-3-en/index.html?itemId=/content/component/9789264307292-3-en

OECD, *Economic Outlook, June 2020*. http://www.oecd.org/economic-outlook/june-2020/

Okta. Businesses @ Work. Retrieved from Okta 2020: https://www.okta.com/businesses-at-work/2020/

Pignatelli, F., Boguslawski, R., Bargiotti, L., Gielis, I., Verdegem, B., Smits, P. and Keogh, D., *Guidelines for public administrations on location privacy*, EUR 30070 EN, Publications Office of the European Union, Luxembourg, 2020. https://publications.jrc.ec.europa.eu/repository/handle/JRC119398

Polton, D. Les données de santé. *médecine/sciences*, *34*(5), 449-455. 2018.

Portes, J. The lasting scars of the Covid-19 crisis: Channels and impacts, *VoxEU.org*, 1 June 2020.

Preciado, P. The Biopolitics of COVID-19. Learning from the virus. *Biopolitical Philosophy*, 4 April 2020. https://biopoliticalphilosophy.com/2020/05/04/the-biopolitics-of-covid-19/

Privacy Cannot Be a Casualty of the Coronavirus. *The New York Times*. 2020. https://www.nytimes.com/2020/04/07/opinion/digital-privacy-coronavirus.html .

Priyardashini M. *Open-Source Deepfake Tool Turns You into Elon Musk In Zoom, Skype Calls*. April 20. 2020. https://fossbytes.com/open-source-deepfake-tool-turns-elon-musk-zoom-skype-calls/

Redmiles, E., Kaptchuk, G. & Hargittai, E., The Success of Contact Tracing Doesn't Just Depend on Privacy. *Wired*. May 23, 2020.

Research and Markets. Online Education Market Study 2019 | World Market Projected to Reach $350 Billion by 2025, Dominated by the United States and China. Retrieved from *Research and Markets* 9 December 2019: https://www.globenewswire.com/news-release/2019/12/17/1961785/0/en/Online-Education-Market-Study-2019-World-Market-Projected-to-Reach-350-Billion-by-2025-Dominated-by-the-United-States-and-China.html

Reuters. Norway to halt COVID-19 track and trace app on data protection concern. *Reuters*, 2020. https://www.reuters.com/article/us-health-coronavirus-norway-apps/norway-to-halt-covid-19-track-and-trace-app-on-data-protection-concerns-idUSKBN23M18T

Richtel, M. W.H.O. Fights a Pandemic Besides Coronavirus: An 'Infodemic.' *The New York Times*. 2020. https://www.nytimes.com/2020/02/06/health/coronavirus-misinformation-social-media.html .

Rossi, C. App Immuni, un terzo degli italiani teme per la privacy. Report Swg. *Policymakermag*. 2020. https://www.policymakermag.it/fact-checking/app-immuni-un-terzo-degli-italiani-teme-per-la-privacy-report-swg/

Rossignol, C., & Lenoir, F. Belgian rail tests sensors to keep workers apart during COVID-19. *Reuters*. 2020. https://www.reuters.com/article/us-health-coronavirus-belgium-railways/belgian-rail-tests-sensors-to-keep-workers-apart-during-covid-19-idUSKBN2311SQ

Samoili, S., López Cobo, M., Gómez, E., De Prato, G., Martínez-Plumed, F., and Delipetrev, B., *AI Watch. Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence*, Publications Office of the European Union, Luxembourg, 2020. https://ec.europa.eu/knowledge4policy/ai-watch/defining-artificial-intelligence_en

Sarasin, P. Understanding the Corona pandemic with Foucault. *Foucault blog*, 31 March 2020. https://www.fsw.uzh.ch/foucaultblog/essays/254/understanding-corona-with-foucault?fbclid=IwAR0a21aWdBhjqJAmGxMyIn32XP9AMhs71PVkGDbid_jV-KDsCxiIWq3lMY4

Savevski V. Quando la lastra e un deepfake. *Wired* May 12. 2020. https://www.wired.it/scienza/medicina/2020/05/13/sanita-digitale-hacker-lastre-fotoritocco/

Scams are thriving during COVID-19. Here's what to watch out for. *Popular Science*. 2020. https://www.popsci.com/story/technology/coronavirus-online-email-text-scams/

Schectman, J., Bing, C., & Stubbs, J. Special Report: Cyber-intel firms pitch governments on spy tools to trace coronavirus. *Reuters*. 2020. https://www.reuters.com/article/us-health-coronavirus-spy-specialreport/special-report-cyber-intel-firms-pitch-governments-on-spy-tools-to-trace-coronavirus-idUSKCN22A2G1

Scott, M., Cerulus, L., & Delcker, J. Coronavirus is forcing people to work from home. Will it break the internet? *POLITICO* 18 March 2020: https://www.politico.eu/article/coronavirus-covid19-internet-data-work-home-mobile-internet/

Scudellari, M. Hospitals Deploy AI Tools to Detect COVID-19 on Chest Scans. *IEEE Spectrum*. 2020. https://spectrum.ieee.org/the-human-os/biomedical/imaging/hospitals-deploy-ai-tools-detect-covid19-chest-scans

Severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2). *Biozentrum*. 2020. https://swissmodel.expasy.org/repository/species/2697049

Shishehgar, M., Kerr, D., & Blake, J. A systematic review of research into how robotic technology can help older people. *Smart Health*, 7–8(March), 1–18. 2018. https://doi.org/10.1016/j.smhl.2018.03.002

Siatitsa, I. and Kouvakas, I. Indiscriminate COVID-19 location tracking (Part II): Can pandemic-related derogations be an opportunity to circumvent Strasbourg's scrutiny. *Strasbourg Observers*.

https://strasbourgobservers.com/2020/05/05/indiscriminate-covid-19-location-tracking-part-ii-can-pandemic-related-derogations-be-an-opportunity-to-circumvent-strasbourgs-scrutiny/ 2020

Spataro, J. Learning from our customers in Italy. *Microsoft* 8 April 2020: https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/08/learning-from-customers-italy/

Spring, M. Coronavirus: The human cost of virus misinformation. *BBC News*. 2020. https://www.bbc.com/news/stories-52731624

Stubb, C. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. August 30. 2019. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

Stubbs, J., and C. Bing. Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead - sources. *Reuters*. May 8. 2020. https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex/exclusive-iran-linked-hackers-recently-targeted-coronavirus-drugmaker-gilead-sources-idUSKBN22K2EV

Su, E. Roaming "robodog" politely tells Singapore park goers to keep apart. *Reuters*. 2020. https://www.reuters.com/article/us-health-coronavirus-singapore-robot/roaming-robodog-politely-tells-singapore-park-goers-to-keep-apart-idUSKBN22K1S6

Thomas, Z. Coronavirus: Will Covid-19 speed up the use of robots to replace human workers? *BBC News*. 2020. https://www.bbc.com/news/technology-52340651

Tidy, Joe. Coronavirus: How hackers are preying on fears of Covid-19. *BBC News*. March 13. 2020. https://www.bbc.com/news/technology-51838468

Timberg, C., & Harwell, D. Most Americans are not willing or able to use an app tracking coronavirus infections. That's a problem for Big Tech's plan to slow the pandemic. *The Washington Post*. 2020. https://www.washingtonpost.com/technology/2020/04/29/most-americans-are-not-willing-or-able-use-an-app-tracking-coronavirus-infections-thats-problem-big-techs-plan-slow-pandemic/

Troncoso C. Payer M. Hubaux J-P. et al. Decentralzed Privacy-Preserving Proximity Tracing. Version 25th May 2020. https://raw.githubusercontent.com/DP-3T/documents/master/DP3T%20White%20Paper.pdf

UNESCO. During this coronavirus pandemic, 'fake news' is putting lives at risk. *UN News*. 2020. https://news.un.org/en/story/2020/04/1061592 .

United Nations Department of Economic and Social Affairs: *Everyone included: Social impacts of COVID-19* 2020. https://www.un.org/development/desa/dspd/everyone-included-covid-19.html

Upatham, P., and J. Trainen. Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted. *VMware carbon black*. April 15. 2020. https://www.carbonblack.com/2020/04/15/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/.

Van Dijk, J. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance and society*, 12(2): 197-208. 2014.

Van Roy, V. *AI Watch -National strategies on Artificial Intelligence: A European perspective in 2019*, Publications Office of the European Union, Luxembourg, 2020. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC119974/national_strategies_on_artificial_intelligence_final_1.pdf

Verseck, K. (2020). Coronavirus rule of law under attack in SE Europe. *Deutsche Welle*, 25 March 2020. https://www.dw.com/en/coronavirus-rule-of-law-under-attack-in-southeast-europe/a-52905150?maca=en-Facebook-sharing&fbclid=IwAR1UuhV83IDFzrz7I1T-LOEBYX0fwlNbKsYueqIekYDS2IS7CAZnD86UTjk

Vesnic-Alujevic, L., Breitegger, M. & Guimarães Pereira, Â. 'Do-It-Yourself' Healthcare? Quality of Health and Healthcare Through Wearable Sensors. *Sci Eng Ethics* 24, 887–904 (2018). https://doi.org/10.1007/s11948-016-9771-4

Vesnic-Alujevic, L., Nascimento, S., Polvora, A. (2020). Societal and ethical impacts of artificial intelligence: Critical notes on European policy frameworks, *Telecommunications Policy*, https://doi.org/10.1016/j.telpol.2020.101961.

Wakefield, J. Coronavirus: AI steps up in battle against Covid-19. *BBC News*. 2020. https://www.bbc.com/news/technology-52120747.

Waltner-Toews, D., Biggeri, A., De Marchi, B., Funtowicz, S., Giampietro, M., O' Connor, M., Ravetz, J., Saltelli, A, Van Der Sluijs, J. Post-normal pandemics: why covid-19 requires a new approach to science. 2020. https://steps-centre.org/blog/postnormal-pandemics-why-covid-19-requires-a-new-approach-to-science/

Wellcome. *Sharing research data and findings relevant to the novel coronavirus (COVID-19) outbreak*. Published 31 January 2020, https://wellcome.ac.uk/coronavirus-covid-19/open-data.

Wu, F., Zhao, S., Yu, B. et al. A new coronavirus associated with human respiratory disease in China. *Nature* 579, 265–269, 2020. https://doi.org/10.1038/s41586-020-2008-3.

Yee Y. W. Coronavirus: More need to use contact tracing app for it to be effective**.** *The Straits Times*. 1st May 2020. Retrieved 15 July 2020. https://www.straitstimes.com/singapore/more-need-to-use-contact-tracing-app-for-it-to-be-effective

Yuan, E. S. A Message to Our Users. *Zoom Blog* 1 April 2020: https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

Zahuranec, A. and Verhulst, S. Mapping how data can help address COVID-19. 2020. https://medium.com/data-policy/mapping-how-data-can-help-address-covid19-a7be2e631aec

Zoom. 90-Day Security Plan Progress Report. *Zoom Blog* 22 April 2020 https://blog.zoom.us/wordpress/2020/04/22/90-day-security-plan-progress-report-april-22/

Zuboff, S. *The age of surveillance capitalism*. Profile books Ltd. 2019.

List of figures

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00800 6 7 8 9 10 11 (certain operators may charge for these calls),

- at the following standard number: +32 22999696, or

- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

KJ-NA-30306-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub

ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office of the European Union

doi:10.2760/166278

ISBN 978-92-76-20802-0