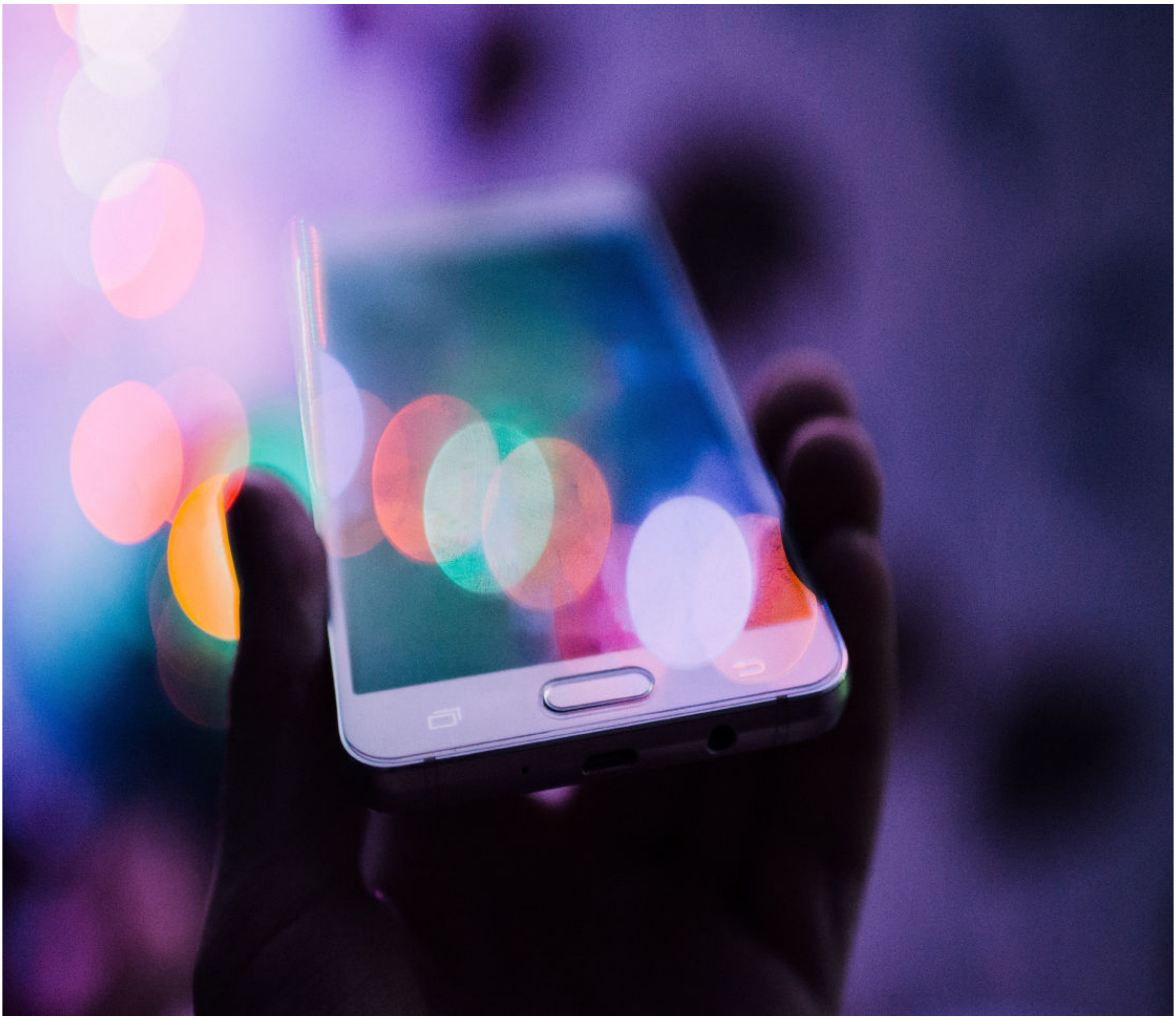


REFLECTION PAPER

DATA DRIVEN HEALTHCARE AND THE DIGITALISATION OF SOCIETY - THE STAKES FOR PUBLIC HEALTH

December 2020

european public health alliance

About EPHA

EPHA is a change agent – Europe's leading NGO alliance advocating for better health. We are a dynamic member-led organisation, made up of public health civil society, patient groups, health professionals, and disease groups working together to improve health and strengthen the voice of public health in Europe.

Co-funded by
the Health Programme
of the European Union

The European Public Health Alliance has received funding under anoperating grant from the European Union's Health Programme (2014-2020). The content of this document represents the views of the authoronly and is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.

Transparency Register Number: 18941013532-08

Contents

Introduction

Digital health technologies encompass a wide range of devices and software.[1] 'These include the use of social media by both members of the general public and healthcare or public health professionals to discuss health and medical issues and disseminate information; remote healthcare consultations and patient self-care using digital technologies (telemedicine and telehealth); the use of virtual reality in medical training; the rapidly expanding number of mobile applications ("apps") devoted to health and medical matters […]; health informatics systems in healthcare delivery; public health surveillance using big data to track disease patterns; wearable self-tracking devices and gaming technologies for monitoring bodily functions and activities using sensors; health promotion employing social media and text messages; 3D printing of medical devices and prosthetics; and community development and activist initiatives involving citizen science/citizen sensor activities to generate environmental information on their local area.' (p. 707)

The outbreak of the COVID-19 virus and digital applications to combat its spread has speeded up the discussion about 'digital health', data protection, and potential infringements of human rights. This discussion focussed especially on public health surveillance using big data to track disease patterns and the use of digital proximity tracking technologies for COVID-19 contact tracing. It triggered a range of academic publications highlighting ethical considerations regarding the technical applications (apps).[2–4] The World Health Organization (WHO) published an interim guidance regarding the use of digital proximity tracking technologies for COVID-19 contact tracing,[5] as did the eHealth Network of the European Commission.[6] These ethical considerations include ensuring public benefit; ensuring scientific validity and accuracy; protecting privacy; preserving autonomy; avoiding discrimination; be aware of repurposing; setting an expiration; and preventing digital inequality.[3] In its interim guidance WHO explicitly states that 'civil society can play a crucial role in holding governments and companies accountable for the deployment and operation of digital proximity tracking technologies.'[5] A case study about the CoronaMelder app in the Netherlands included in this report underpins this role for civil society.

Alongside this upsurge of attention for digital health due to the COVID-19 virus, WHO has published its (draft) global strategy on digital health[7], and the WHO Regional Office for Europe has included a new flagship Initiative, 'Empowerment through Digital Health' in its European Programme of Work 2020-2025.[8] Although the WHO stresses in its (draft) global strategy that 'digital health should be an integral part of health priorities and benefit people in a way that is ethical, safe, secure, reliable, equitable and sustainable', the current network economy is based on the 'winner-takes-all' principle. Civil society will need to play its role regarding flagging these concerns, keeping public values front and centre, and help identifying what 'empowerment' means for 'whom.'

A new joint The Lancet and Financial Times Commission focusing on the convergence of digital health, artificial intelligence (AI), and universal health coverage (UHC) has been established to run from October 2019 to December 2021. The 'Governing Health Futures 2030: Growing up in a Digital World'[a] Commission will convene a group of independent commissioners from

[a] See https://www.governinghealthfutures2030.org/

diverse sectors and geographical locations to ensure a broad input of voices in moving forward the digital health agenda. 'With the ultimate goal of promoting inclusivity and maximising health equity in resource-poor settings, the Commission will provide a vision for the future that promotes integrated systems to leverage digital health technologies.'[9] Also, in health care and medicine, researchers are flagging their concerns about how disease stereotypes (e.g. heart attack, depression, asthma) are translated to technology and may lack gender and ethnical diversity perspectives.[10] These concerns are addressed in a recent European Parliament resolution.[11]

These developments indicate that digital health might become even bigger a topic of importance for the public health community and this holds a number of opportunities. In particular, the European Public Health Alliance (EPHA) could build on its previous work and use the existing evidence to inform its members and improve their digital literacy, and engage in debates about the digital health processes in the global and European public health levels of WHO. EPHA may also seek to contribute to the 'Governing Health Futures 2030: Growing up in a Digital World' Commission from a European perspective. Moreover, opportunities could be found to engage with the digital data strategy of the European Commission as this strategy supports establishing nine common European data spaces, including a Common European health data space. Europe has exclusive competence over data, but not over health. However, one can impact on health (policies) by regulating data: how it is collected, and how it is used. The Future for Privacy Forum, the Rathenau Instituut and the Technical University, Delft could be interesting partners for collaboration in this regard.

This paper contains reflections based on EPHA's questions about what the stakes are for public health, given the increase in data-driven healthcare and the digitalisation of society. These stakes go well beyond the health sector and invite the public health community to team up with organisations active in the areas of digital rights, gender equality, as well as environmental and economic justice.

Information in this paper is based on a quick-scan of academic and grey publications about these issues, and interviews with experts from the following organisations: Access Now,[b] the Future of Privacy Forum[c] and the Technical University, Delft.

[b] https://www.accessnow.org/

[c] https://fpf.org/

Data-driven solutions in European health systems and advancing its fundamental values

In its report, ‘Directed digitalisation – Working towards a digital transition focused on people and values – The Dutch approach,’ the Rathenau Instituut[12] indicates that government, private sector and civil society organisations need to shape and direct the digital society in such a way that greater focus is placed on people and values. According to the authors, digitalisation has been compromising certain public values such as privacy, digital security, equal treatment and freedom of expression for a long time. Also, the governance system – the collection of actors and institutions responsible for defining social and ethical issues and placing them on the agenda – was insufficiently prepared to protect these public values.[12]

According to the Rathenau Instituut, ‘an integrated approach to innovation is needed, that gives shape and direction to the digital transition and as a result to our society, from the viewpoint of public values.’[12] Hence, we need to ask the question ‘what type of digital society do we want to live in?’ This also means a turnaround in the debate on the deployment and influence of digital technologies: from a focus on technology and the assumption that it will automatically lead to social progress, to a focus on the interaction between digitalisation and values.

Very recently we have seen this happening in (academic) discussions about values underpinning digital public health technologies for pandemic management and more specifically, the development of COVID-19 contact tracing apps. Interdisciplinary research has shown the value of context in managing the societal, legal, and ethical risks of data processing for pandemics that stretch beyond the issue of privacy.[3] In order to avoid so-called solutionist or instrumentalist approaches (where the focus is on the benefit that the technology itself brings to public health management) to digital public health technologies, Gasser et al. instead focus on public health outcomes, as well as the ethical principles guiding these outcomes.

A mapping of ethical and legal challenges reveals that any digital public health technology should

- Ensure public benefit;

- Protect privacy, as all digital public health tools impinge upon individual privacy by requiring some degree of access to information about the health status, behaviour, or location of individuals;

- Preserve autonomy because digital public health technologies have the potential to undermine not only privacy but also personal autonomy;

- Avoid discrimination, because as well as the risk of re-identification and infringement of personal autonomy, digital public health technologies also carry an inherent risk of discrimination;

- Avoid repurposing because there is a risk that digital tools could also be applied to other forms of surveillance in addition to being used for legitimate public health purposes (namely, tracking and monitoring patients with COVID-19);

• Set an expiration, as pandemics are a rare situation where democratic governments can take unchecked executive action decisions for the collective good of their population;

• Prevent digital inequality because digital technology, particularly mobile phone technology, is increasingly widespread globally but unevenly distributed.

Based upon these risks and challenges Gasser et al. propose recommendations that are linked to the different phases of developing a digital public health technology or tool.

Preparation phase: Firstly, this phase involves assembling the right team. The technical, organisational, legal, ethical, public health, and other challenges that need to be managed when using digital tools in response to COVID-19 are complex and require an interdisciplinary and mixed team (e.g., gender, ethnicity, age). Secondly, guidance of ethical principles: make those principles (such as beneficence, justice, non-maleficence, privacy, solidarity, and autonomy) explicit and use them as a reference point.

Planning phase: This phase entails distinguishing tools from their purpose. Defining specific objectives within the containment and mitigation strategy is necessary. Only then can the various digital public health technologies with their different data sources and means to collect, use, and otherwise process them, be considered. Furthermore, this phase also includes avoiding lock-in and path dependency (i.e., revenue models based on closed technology).

Assessment phase: For this phase, validation studies and risk assessments should be undertaken. A robust and systematic risk assessment process should be carried out for each intended purpose, context, instrument, and model, even when pressed for time; well established practices such as human rights impact assessment and privacy risk impact assessment should lead the way, even if they need to be modified.

Development phase: This phase includes embracing privacy in so-called by design and by default approaches.

Deployment and evaluation phase: First, this phase requires proactive and continuous communication. Transparency in the form of provocative communication with the key stakeholders—and where possible, active consultation and participation with the public—is essential and needs to be an integral part of the process from beginning to end.

Benefits and drawbacks

Existing and emerging digital technologies can benefit key public health functions, fundamental rights and equity, but they also have drawbacks. The digitisation of health data, for instance, creates opportunities for more personalised healthcare and prevention.[13] When combined, and taking the diversity of users (in terms of sex, gender, age, ethnicity, technical skills, etc.) for the benefit of people's health into account,[10] different digital services make it possible to access, share and use electronic health data - including outside the healthcare domain. The Rathenau Instituut's report shows that responsible and secure data sharing is best achieved by remaining small in scale and by focusing on what is truly necessary. It gives government, the healthcare sector and policymakers the tools they need to ensure that digital health data services are used for the benefit of a 'socially responsible digital society.'

The Rathenau Instituut concludes that digital sharing can only contribute to social aims such as good quality healthcare, personal health and sickness prevention if the quality of the data is good, data transfer is protected and secure, and there is no pressure to share data. But, currently, there are drawbacks:

1. There is a lack in frameworks governing the use of digital health data services and no coordination of such use, either in the medical domain itself or in its interaction with the non-medical domain.

Potential solutions would be to:

a) Establish ownership of the various responsibilities, including liability in medical interventions, more explicitly in agreements;

b) Establish broad codes of conduct for the development of services, including services that lie outside the medical domain;

c) Maximise learning from best practices in healthcare.

2. There are not enough safeguards in the data chain, i.e., the processes of generating, accessing, sharing and using health data.

Potential solutions would be to:

a) Build on the concept of patient confidentiality and supplement it with technological citizenship;

b) Define precisely what shared decision-making entails;

c) Make safeguards ensuring the quality and reliability of data and data sharing transparent and put appropriate oversight mechanisms into place.

3. There are limits to personal health management; equal access to healthcare and health are not sufficiently guaranteed.

Potential solutions would be to:

a) Establish a governance system that will strike the right balance between the individual and the collective interest;

b) Never lose sight of the right to not be measured, analysed or coached and the right to meaningful human contact.

In order to counteract the lack of frameworks governing the use of digital health data services, the public health community could learn from and potentially contribute to a recent initiative of The Lancet & Financial Times. Their 'Growing up in a digital world: Governing health futures 2030' Commission is exploring the convergence of digital health, artificial intelligence (AI) and other frontier technologies, with universal health coverage (UHC), fundamental rights and equity being central, which is very much in line with EPHA's end-user centric approach established over the past years (see **https://epha.org/digital-health/**)

Adapting to digitalisation: lessons for the healthcare sector

In his speech at the World Health Organization in Dakar, Professor Van den Hoven stated: 'The picture is clear by now. Incumbents in finance and banking, transport, industrial production and retail have all experienced it: you go digital or you disappear.'[14] Inside the healthcare sector 'it is also obvious that data and Artificial Intelligence can reduce costs in healthcare, improve patient safety, empower patients and improve the quality of diagnosis, therapy, patient journeys, billing and logistics. Smartphones and watches with health apps and wearables are part of an Internet of Things revolution that is well underway. In healthcare wearable devices can be used to detect arrhythmia, predict Parkinson via the accelerometer in the phone, and measure a range of biomarkers such as blood sugar, blood pressure, fat percentage, oxygen and stress. They can diagnose skin cancer retina damage and assist in management of eating disorders, phobias, depression, chronic pain and PTSD.'[14]

A study drawn up for the European Economic and Social Committee explored the impact of digitalisation on employment, enterprises and labour relations in terms of the creation, transformation and destruction of jobs, employees' and employers' altered roles, and changes in the organisation of work.[15] It showed that in traditional businesses and industries digitalisation affects existing organisational and management structures, which is most visible due to the higher flexibility and fragmentation of work, changing work monitoring methods, recruitment strategies, and skill and training needs. More generally, the real challenge for industrial operators is whether they, as established firms, can engage their own digital transformation before disruptive competition forces them out of business.

According to the researchers, key factors for successfully adapting enterprises to the changes brought about by digitalisation are the ability to collect and exploit data, the interconnection of value chains, the creation of digital customer interfaces, and the mitigation of cyber threats. These are potential lessons that can be drawn for the healthcare sector.

However, these traditional businesses do not need to uphold public health values and are based on competition rather than on cooperation. As Professor Van den Hoven highlights in his speech: 'can we trust big tech and their acolytes and subsidiaries with our health data? Can we ever be sure that their services will not be solicited by foreign failing states, guarantee that they and our data will not merge with companies and databases in the hands of oligarchs who do not feel constrained by the rule of law or principles of ethics? It is against this background we need to situate the discussion about sharing and using identity relevant data in the health domain.'[14]

This is why Professor Ilona Kickbusch, as co-chair of The Lancet & Financial Times Commission 'Growing up in a digital world: Governing health futures 2030', is exploring the convergence of digital health, AI and other frontier technologies with universal health coverage (UHC).[16] 'We want to contribute to integrated digital development that improves the health and well-being of children and young people. In connection with this, we are examining existing policies for digital health, AI and UHC to identify those with the greatest potential to improve health and well-being, maximise health equity in resource-poor settings and ensure human rights. We want to deliver a clear set of recommendations on the governance of digital health, AI and UHC, taking into account geopolitical, economic and social factors.'

As an example of a good practice for digital health strategies that contribute to improving people's health and well-being, Kickbusch refers to the Montréal Declaration for a Responsible Development of Artificial Intelligence from 2018. 'Just like the WHO Ottawa Charter for Health Promotion that was approved in 1986 and is based on the premise that health is a political choice, the Montreal Declaration is grounded in the idea that matters related to ethics or abuse of technology ultimately become political and therefore belong in the sphere of collective decisions. It includes, for example, the well-being principle, which postulates that artificial-intelligence systems must first and foremost permit the growth of the well-being of "all sentient beings." The respect for autonomy principle makes strong reference to the empowerment of citizens and the fostering of literacy and critical thinking. The solidarity principle states that "the development of artificial-intelligence systems must be compatible with maintaining the bonds of solidarity among people and generations" and includes special reference to health systems. Policies such as these can set the agenda for how digitalisation of the health sector can be designed to benefit all groups of the population, and specifically children and young adults.'[16]

Protection of personal health data in an increasingly transnational data ecosystem

According to Access Now, accessing personal health data is always a threat. This implies that from the beginning of developing a particular technology, privacy protection measures need to be put in place. However, this is not always the case, as is evident from the following two examples from The Netherlands.

In October 2020, journalists from RTL Nieuws revealed, in an investigation into data protection, that due to an error at Jeugdriagg (youth psychiatric help), the files of children with serious psychological problems had been breached.[17] The breached files of Kenter Jeugdhulp, the new name of Jeugdriagg, contained full names of young children with very sensitive details about their private lives, such as mental illness, the unstable home situation, drug use and all kinds of problems at school. Kenter Jeugdhulp, which treats thousands of families, had not closed its old website (Jeugdriagg.nl) securely; anyone could take over the website and the associated e-mail addresses.

The second example concerns another investigation by RTL Nieuws; this time about trade in data from two corona systems of the GGD (Municipal Public

Health Service): CoronIT, which contains the private data of Dutch people who have taken a corona test, and HPzone Light, the system for source and contact research of the GGD.[18] The details of millions of patients were offered for sale, including address details, telephone, and BSN identifiers (Dutch social security number) on chat services such as Telegram, Snapchat and Wickr. Two people who worked in the GGD call centre were arrested. The data/ information can be misused for, among other things, identity fraud, phishing, stalking (and forms of cyber-violence against women).[19] The Dutch health ministry data leak serves as a reminder of the threats posed by malicious insiders.

In its 2019 annual report, the Dutch Data Protection Authority reported that the largest number of data breach reports about the healthcare sector came from hospitals (25%), pharmacies (20%) and foundations that conduct population screening (9%). In more than half of the cases (67%), the data breach involved sending or handing over personal data to the wrong recipient. In other cases it involves hacking, malware and / or phishing incidents (13%).[20]

The network economy has its own threats. In an interview with 'Healthy Europe', Professor Kickbusch argues that the dark side of digital health has long been overlooked. IT giants such as Amazon, Google, Facebook and Alibaba, for example, have access to huge volumes of personal data and use this solely for their own commercial aims.[16] In this context, the health sector is a very large and promising business segment. Also, digitalisation offers countries new possibilities for surveillance and authoritarian governance. 'The risk of technology and data-driven control systems developing in sectors that are considered benign – such as health, education, and social welfare – is possibly even greater than elsewhere. We cannot ignore the huge risks of digitalisation any longer. We cannot develop digital health as a human rights-free zone and destroy our children's future in the process.'[16]

GDPR, ePrivacy, cybersecurity

The Future of Privacy Forum is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. According to the Forum, 'the EU took advantage of its mature data protection legal framework and acted rapidly to outline the possibility of a pan-European approach to support the fight against the [COVID-19] pandemic with data, be it under the guise of mobility data for heat maps and modelling, health data for research purposes or proximity data for contact tracing, while ensuring fundamental rights and freedoms remain protected.'[21] Also, 'developments at national level, at least in the Member States of the EU, will be ultimately influenced by EU policy' and 'personal data for modelling or research in the context of the COVID-19 pandemic, [...] will all need to follow data protection rules and principles, as provided by EU law.'[21]

According to the Future of Privacy Forum, the Guidelines of the European Data Protection Board (EDPB) are very important because they represent the agreed position of all national Data Protection Authorities (DPAs). DPAs are the only administrative entities that have competence to enforce the General Data Protection Regulation (GDPR) and the Law Enforcement Directive at national level, both against government bodies and private organizations. Also, they are capable of ensuring a harmonized approach across the EU, at a time when national governments prefer to act by themselves, contributing thus decisively to a pan-European approach to the data-based response to the COVID-19 pandemic.

The Future of Privacy Forum strongly suggests becoming familiar with the actors involved in EU policymaking regarding data protection and the digital agenda.

The data strategy of DG Connect is of particular importance: it supports establishing nine common European data spaces, including a Common European Health Data Space.[22] The EU has exclusive competence over data, but not over health. However, one can impact on health (policies) by regulating data: how it is collected, and how it is used.

Digital inclusion for all, in times of data-driven commercialisation

It is not always apparent where vested interests lie in the provision of medical information in apps either for the general public or members of the medical professions.[23,24] Shoshana Zuboff, author of 'The Age of Surveillance Capital'[25] puts it more bluntly: 'Nearly every product or service that begins with the word "smart" or "personalised," every internet-enabled device, every "digital assistant," is simply a supply-chain interface for the unobstructed flow of behavioural data on its way to predicting our futures in a surveillance economy.'

Zuboff poses three crucial questions that could guide stakeholders such as policymakers and civil society to be alert:

1. Who has the knowledge?

2. Who decides who has the knowledge?

3. Who decides who can decide who has the knowledge?

Developing digital healthcare applications in cooperation with their end users, healthcare practitioners and researchers can help challenging tech arguments in favour of promoting prevention, health promotion and digital inclusion for all. MIDATA is an example of a scientist-initiated health cohort in which individuals control data access. It uses open source code, has a transparent governance structure, secures data through encryption, and has a regional focus.[26]

In its research on digital health in the Netherlands, the Rathenau Insituut[13], encouraged the Dutch government to implement best practice examples of digital health based upon cooperation between users, healthcare practitioners and researchers. That could ensure that the quality of the data, healthcare that respects human dignity, and health itself, are at the centre, with people being protected against the unwanted use of their data. TU Delft uses the wording of 'value sensitive design': all stakeholders should be involved in the design of a digital health technology and it should be based on values such as privacy by design linked with health system goals. These values need to be translated into requirements and in the evaluation this should be assessed.

Another way to challenge tech arguments is provided by the Future of Privacy Forum. In its testimony about 'Enlisting Big Data in the Fight Against Coronavirus,' the Future of Privacy Forum recommended that data should follow the lead of public health experts. 'Rather than leading the way with data that is already available, technology companies should play a supporting role to epidemiologists, established research partners, and public health experts and rely on their expertise in determining what data is useful to achieving specific, clear public health goals.'[27]

Digitalisation and health

Digitalisation has impact on every dimension of health, Access Now explains:

• Physically: sitting behind the computer all day is not healthy.

• Mentally: radicalisation of thought may occur, which is visible on social media. Also, people may experience constant pressure of processing information digitally.

• Environmentally: the energy used for data processing and storage is increasing tremendously.

• However, in times of COVID-19 it is also technology which helps us to continue working (online) and meeting friends (online).

Digital health devices such as wearable self-tracking devices, social media platforms, apps and patient support websites could work as 'disciplinary tools', according to Lupton.[1] They invite users to conform to the ideals of healthism (privileging good health above other priorities) and the responsible self-management and self-monitoring of one's health and body, including avoiding exposure to risk.

Digitalisation and the Right to Health

Digital health initiatives can amplify socioeconomic inequalities and contribute to healthcare disparities. Even within high-income countries, susceptible groups, such as those in low-income neighbourhoods or remote regions, might not have access to broadband signals, smartphones, or wearable technology such as smartwatches.[28] This could threaten the right to health and can only be solved if investments are made in technology and infrastructure from the perspective of digital inclusion for all instead of commercial gains.

Technology is not necessarily a solution and it is not necessarily a risk - it is on the grey-scale and provides both benefits and risks, according to Access Now. In 2019 the European Journal of Public Health published a special issue about the potential and pitfalls of digitalisation from a public health perspective.[29] McKee et al. highlight benefits associated with digitalisation including the power of information sharing amongst disparate communities as well as improved surveillance and diagnostics.[30] However, the impact of other aspects of digital technology such as wearable devices on human health may have been largely oversold. Five factors that we may call 'lowlights' of digitalisation are: discrimination; breaches of privacy; iatrogenesis; disinformation and misinformation or 'fake news;' and cyber-attacks.

These harmful impacts of digitalisation can be avoided if we have effective and appropriate governance mechanisms that are able to align digital innovation with public health system goals. European countries typically pursue health systems goals that include high quality, efficiency, equity, affordability and accessibility of health care. Ricciardi et al. emphasise the onus on governments to create the policy environment and incentives that steer the industry towards the development, adoption and use of technologies that contribute to health system goals going beyond the confines of health technology assessment in evaluating specific technologies to see whether they should be funded.[31]

The Rathenau Instituut has proposed five actions that will help policy makers, businesses and civil society organisations to reinforce the governance system:[12]

• Invest in a value-driven approach to innovation;

- Arrive at a proactive, overarching agenda and action plan for the societal and ethical aspects of digitalisation;
- Invest in a strong position for supervisory bodies;
- The private sector: engage in socially responsible digitalisation;
- Encourage technological citizenship.

Digitalisation and empowerment

One of the many benefits of digitalisation is that patients with chronic conditions can become much better informed about their disease, including ways of adapting to its impact.[30] Studies of patients' experiences of using digital technologies for at-home self-care, for example, have demonstrated the complexity, ambivalence and strong emotion involved. Lupton found that patients may find using these devices empowering, allowing them to reduce travel to see their healthcare provider or to live independently at home.[1] However, Lupton added, many patients resent the invasion into their homes of medical devices that constantly remind them that they are old and infirm or are dealing with a serious chronic illness, or make them feel that they are under constant surveillance. Furthermore, while the devices promise certainty and simplicity, they are often difficult to use and ambiguous in the information they convey.

Digitalisation and empowerment of patients regarding their digital data means something different. Healthcare professionals who use online portals, for example, empower patients to take their own decisions by reassuring them that they can manage their data through the portal. If patients can decide if and what information they provide in an online module, this may provide them with greater control over data sharing, but it might not add to 'feeling empowered'.[13] The Rathenau Instituut questions the underlying principle of putting people in control. 'Patients become more resilient, but also more critical of practitioners and the healthcare process. They may also become more vulnerable, in fact, because they share data with third parties without gaining any direct benefits and without always being able to control this aspect.'[13]

An increasingly important question for health advocates is what empowerment of individuals and communities in relation to their health actually means. Both the WHO European Region's Programme of Work[8] and the European Commission's 'Shaping Europe's Digital Future'[32] have put empowerment at the centre. The public health community should be aware that digitalisation in healthcare may affect certain goals or certain groups positively, while at the same time negatively affecting others.[33] In 'Ethical aspects of digital health from a justice point of view' Brall et al. provide three key points[34] for the public health community to consider:

- Fair and equitable access to digital health technologies and interventions offers chances to healthcare coverage, spread of health information and literacy, and potentially efficiency of care;
- The diversity and range of stakeholders in digital health calls for a clear demarcation of each stakeholder's specific responsibilities in assuring an ethical and fair digital health;
- Regulations and policies focusing on ethical guidance are needed to foster fair, equitable and trustworthy digital health aiming to empower users.

‘In order to make people capable to actually use the opportunities offered to them if they wish, truthful information about the benefits and risks of engaging in digital health methods has to be provided to the individual users. Hence, users should be motivated and empowered (in an informational as well as technical sense) to engage in digital health technology. For this, open communication, technical training and education should be offered.’[34] (p.19)

Possible ways forward

Stakes for public health are high regarding data-driven healthcare and the digitalisation of society. The question is, how to move forward? Marleen Stikker shows a possible way. According to the author of ‘The Internet is Broken’[35] (Dutch: Het internet is stuk) we are continuously being ‘nudged, trolled and gamified’ when we browse the internet. Stikker is also one of the founders of De Digitale Stad [The Digital City], a virtual public space based on democratic principles. Nowadays tech giants dominate the web and earn a lot of money with our metadata. How can the internet be fixed again and become a truly democratic, public infrastructure? The way to create a different internet, Stikker says, is by realising that that technology is never neutral, and that there is always an intention in design. This is also applicable to digital health technologies.

A second route to fixing the internet that Stikker explores is explained in the book ‘Doughnut Economics’ by Kate Raworth.[36] Raworth places ‘the safe and just space for humanity to thrive’ between two concentric circles. The outer circle is the environmental ceiling, and the inner circle is the social foundation. The basic principle is that economic activity should be ‘regenerative’ and not ‘extractive.’ This means that the capacity for recovery must be central, and profits should not be made at the expense of exhausting the system, as this is unsustainable. This is also the case if tasks of handling identity-relevant data in the health domain are outsourced (e.g., to call centres). It runs the risk that they are performed by individuals whose working conditions are compromised and whose tasks are not fairly remunerated.[37] If we view the internet and ‘digital health’ from the perspective of this model, different choices would need to be made.

Guiding questions[35] for those choices could be:

- What values do we prefer? Public values, such as human rights or doughnut economics lead us to governance questions like, how is control organised? How does decision-making take place? Who is participating? Who designs? Who decides? What are the procedures?

- How can we guarantee privacy?

- How can we make digital health technologies accessible for all?

- How can we improve their public character and protect it? How can we facilitate social support for that and political will?

- What could economic models look like that are not based on competition but on cooperation, that optimise public values, are regenerative and respect both human beings and our ecosystem? For instance, what natural resources are used and do they contain conflict minerals? What is the ecological footprint of this application? What are the working conditions?

To unlock the full potential of new tools, technologies and digital solutions for a healthy society, Oertelt-Prigione highlights that access to and use of digital solutions might differ by gender.[38] The way forward should guarantee equal access for all and therefore include a gender and intersectional perspective. It should also guarantee safety for all end users, regardless of their gender and/or ethnicity. The European Parliament resolution of 21 January 2021 on the gender perspective in the COVID-19 crisis and post-crisis period (2020/2121(INI)) could provide further guidance on this issue.[11]

To guarantee digital inclusion for all and further explore the answers to the guiding questions of this paper, the public health community could extend its collaboration with (civil society) organisations that are concerned with digital rights, value-driven or sensitive approaches to innovation, gender & social justice, environment, and economic justice. Organisations such as Access Now, the Future of Privacy Forum, and research institutes that investigate the impact of data-driven solutions in national and European health systems such as the Rathenau Instituut or the Technical University, Delft (value-sensitive design) could provide a good starting-point.

Case study:

The CoronaMelder App in the Netherlands

The Netherlands' approach to the COVID-19 pandemic has been to keep the virus under control as much as possible in order to protect vulnerable groups and make sure the healthcare system can cope.[d] A digital tool, the CoronaMelder app, has been designed to support the contact tracing work being done by the GGD (Municipal Public Health Service). The process, from announcing the Dutch cabinet's intention to use special 'corona apps' to the actual implementation of the 'Coronamelder app,' provides some key insights regarding the democratic processes influencing the final product. Also, it shows how the application is embedded in policy, legislation and public health measures.

Dutch approach to COVID-19

In The Netherlands, the COVID-19 pandemic has been approached with an 'intelligent lockdown' when worries about a lack of ICU capacity increased, fearing an 'Italian situation' and the need to triage patients. In April 2020 people were confused about what the strategy to combat the COVID-19 virus would look like. The Dutch government introduced the 'one-and-a-half-metre society' concept. Also, on April 7 2020, public health Minister Hugo de Jonge announced the cabinet's intention to use special 'corona apps' in an attempt to prevent the further spread of the coronavirus.[e]

First attempt to develop an app

On April 11 2020, the Dutch Ministry of Health, Welfare and Sport extended an invitation to commercial companies of all kinds to join the effort of developing and deploying specialised anti-corona apps. More than 750 proposals were submitted.[f]

On April 13 2020, sixty scientists, in a letter to the Dutch Cabinet, pointed out the importance of critically assessing 'usefulness, necessity and effectiveness of the now proposed apps, while also taking into account the impact they may have on the overall social institutions, including the fundamental rights and

[d] See https://www.government.nl/topics/coronavirus-covid-19/tackling-new-coronavirus-in-the-netherlands, accessed 28 January 2021.

[e] Parliamentary Papers II 2019–2020, 25 295, nr. 219; see also https://www.rijksoverheid.nl/actueel/nieuws/2020/04/11/oproep-om-mee-te-denken-over-apps, accessed 28 January 2021.

[f] See https://www.government.nl/latest/news/2020/04/15/health-ministry-to-hold-digital-event-to-test-coronavirus-apps, accessed 28 January 2021.

freedoms of individual persons.'[g]

Their main points are summarised below:

- The use of these apps is very far-reaching. It is therefore important to take a critical look at their actual usefulness, necessity and effectiveness, as well as the social and legal impact, before deciding to use them.

- Technology is rarely the solution to a particular problem. Beware of techno-solutionism. The option must remain to decide not to use such apps. Less invasive solutions should be preferred.

- Effectiveness and reliability is of enormous importance, because ineffectiveness and unreliability can actually lead to a greater risk of infection by creating a 'false sense of security'.

- These apps have an impact on more than just (data) privacy. They also affect the freedom of association, the right to security, the right to health and the right to non-discrimination.

- Fundamental rights and freedoms cannot simply be put aside. There must be a legitimate interest for this action, it must be strictly necessary, proportionate and, above all, limited in time.

- Their use must be waived if: (i) 'contact tracking' or health monitoring is not (any longer) effective, effective or reliable; (ii) less invasive solutions are possible; (iii) the social implications outweigh the benefits; (iv) it is not possible to make a widely-held, responsible balance between conflicting (fundamental) rights and freedoms.

- Any form of obligation or coercion may not accomplish the apps' objectives.

- A broad team of experts from various disciplines must be involved in decision-making and the possible development and use of apps, including computer scientists, data scientists, epidemiologists, intensivists and pulmonologists, legal scientists (privacy and data protection, human rights and administrative law,) behavioural scientists, communication scientists, and ethicists.

- Their possible use must not only be temporary (and therefore reversible), but also strictly necessary and proportionally verifiable, transparent and verifiable.

- Just rolling them out, without looking at the influence on the (social) systems and behavioural patterns, and without the underlying infrastructure (GGDs, test labs, etc.) being set up, is insufficient.

'Appathon'

The Ministry of Health, Welfare and Sports organised an 'appathon' shortly thereafter. This was a public online event. After the event, the Dutch Data Protection Authority and the State Attorney announced that none of the apps met the government's requirements. Critics and experts expressed concern that the app was pushed through far too quickly.

Those processes and critiques motivated the Standing Committee for Health, Welfare and Sports to organise a round table discussion on 22 April 2020. The Standing Committee invited several of the scientists that signed the letter to the Dutch government to provide more in-depth input. Organisation such as Privacy First, Bits of Freedom and Waag represented civil society. The private sector was

[g] See https://allai.nl/wp-content/uploads/2020/04/Online-versie-Brief-Minister-President-Rutte-Ministers-De-Jonge-Van-Rijn-Grapperhaus-de-heer-Sijbesma-inzake-COVID-19-tracking-en-tracing-en-gezondheidsapps.pdf, accessed 28 January 2021.

also represented.

Based on this input the Dutch Minister of Health concluded that none of the presented apps met the requirements that were set and that ‘all [future] solutions must be open source’.

Second attempt to develop an app

The Ministry of Health, Welfare and Sports published its ‘Programme of Requirements for a digital solution to supplement source and contact research’ on 19 May 2020.[h] Before then the Ministry requested external experts to participate in the development team of specialists in the field of app design, development, architecture and involving the open source community.[i] This team included persons who voiced their criticisms regarding the first attempt of developing an app.

In his letter to the Dutch Parliament (28 August 2020), public health minister De Jonge wrote that from the start of building the app, as much transparency as possible has been key. Intermediate products in the development of the app have therefore been continuously published by the development team on GitHub,[j] an online platform where software can be placed by developers to invite others to watch and participate. The same also applies to the designs of the user interface. Because of this open way of working, the so-called ‘communities’ already shared their ideas during construction and cooperated in the continuous improvement of the app’s intermediates.

Supervisory committees and taskforces

During the development of the CoronaMelder app, the independent Supervisory Committee Digital Support Combat Covid-19, the Task Force Digital Support to combat COVID-19 and the Task Force Behavioural Sciences critically reviewed the process and provided their advice.

The Supervisory Committee Digital Support Combat Covid-19 advises the Ministry of Health, Welfare and Sport on digital support for combating the coronavirus. This supervisory committee consists of about 15 participants with knowledge of i.e., epidemiology, virology, technology, privacy and security. Their advice is partly based on proposals from the Taskforce Digital Support against COVID-19 and the Taskforce Behavioural Sciences. In doing so, the Supervisory Committee examines to what extent a proposal for digital support contributes to combating COVID-19, and to what extent the proposal meets the set preconditions.

The Taskforce digital support to combat COVID-19 has been set up to look at the possibilities of digital support in combating the coronavirus from science and practice. The Taskforce therefore includes university scientists from various disciplines, scientists and practice professionals from the National Institute for Public Health and the Environment and scientists and practice professionals from the Municipal Public Health Services (GGD).

The Behavioural Sciences Task Force uses behavioural science expertise to look at the contribution that digital support can make to the control and follow-up of infections with the coron virus. The Taskforce looks at proposals from the developers, but can also issue advice independently. The aim of the recommen-

[h] See https://www.rijksoverheid.nl/onderwerpen/coronavirus-app/documenten/publicaties/2020/05/19/programma-van-eisen, accessed 28 January 2021.

[i] See https://www.rijksoverheid.nl/documenten/publicaties/2020/05/29/digitale-ondersteuning-bestrijding-covid-19---uitbreiding-bouwteam, accessed 28 January 2021.

[j] See https://github.com/minvws/nl-covid19-notification-app-design , accessed 28 January 2021.

dations is to increase the acceptance of the digital tools, to reduce unwanted effects and to increase desirable behaviour.

In addition to bringing in experts from within and outside the government to develop the app, the minister also set up a careful process of tests and checks to test the app. This includes a Data Privacy Impact Assessment (DPIA), advice from the perspective of information security, analysis of national security risks, technical tests, evidence of software integrity, accessibility, lab testing, and field-testing of the application in specific regions in The Netherlands.

Purpose of the CoronaMelder app

The CoronaMelder app is developed as an addition to the regular source and contact tracing of the Municipal Public Services to help curb the spread of the virus as much and as quickly as possible. The aim of CoronaMelder is to contribute to informing citizens as quickly as possible about their risk of infection from h the virus, and thus to controlling the spread of the virus.[k]

Check and balances

According to the Minister of Health, Welfare and Sport, the CoronaMelder app has been developed in such a way that the risk of identifying users is virtually impossible. However, with a view to taking maximum care, it is assumed that personal data is always involved, which means that the requirements of the GDPR must be met. In developing CoronaMelder, the Minister of Health, Welfare and Sport therefore followed the guidelines of the European Data Protection Supervisor (EDPB) regarding the use of location data and contact tracking tools in the context of the COVID-19 outbreak. This app applies the GDPR principles of data minimisation, privacy by design and privacy by default.

An expert panel chaired by Twente University conducted an ethical analysis of this app based on the following values: 1) Voluntariness, 2) Effectiveness, 3) Privacy, 4) Fairness, 5) Inclusion, 6) Procedural fairness, 7) Responsibility, 8) Preventing improper use, 9) Safeguarding civil liberties, and 10) Necessity and proportionality. Based on the analysis the expert panel provided the following recommendations:

- There must be adequate legal regulation for the app, which ensures adequate purpose description and purpose limitation, in particular with regard to use by the government, but also by private parties;

- The use of the app should be completely voluntary, but the government should be able to make a moral appeal to citizens to use the app as part of their collective responsibility for fighting the pandemic;;

- It must be investigated whether the app is accessible to everyone and whether the risks and burdens of the app do not reach certain population groups disproportionately.

- The government should carefully monitor the social impact of the app on the basis of the principles presented in this assessment;

- To prevent the app from heralding a culture change in which people become less reluctant to surveillance, the app should be used and positioned as a means of digital solidarity;

- The app should only become generally available if the tests and DPIA are positive, and not only the app itself, but also the surrounding infrastructure is ready,

[k] For information about how the CoronaMelder app works, see https://www.coronamelder.nl/en/faq/6-hoe-werkt-de-app/, accessed 28 January 2021.

including information provision, complaint options and supporting and pre-conditional legislation and regulations.

Upon the request of the Minister of Health Welfare and Sport, a senior expert specialised in IT security and privacy has reviewed all measures taken regarding information security and privacy protection. The senior expert provided the urgent advice to continue to intensively monitor all existing risks and identify potential new risks after its launch.

The government submitted its revised proposal for the Coronavirus Act to Parliament, to provide a legal basis for measures taken against the spread of the coronavirus, in June 2020. This law was meant to take effect on July 1, but it was revised by the government following much criticism.

In the amended proposal, the coronavirus notification app was removed from the proposed legislation. A proposed new law, specifically for the app was presented which included an anti-abuse provision to prevent the app from being used for the wrong purposes.

Since August 2020 the ‘CoronaMelder app’ was trialed in several regions in The Netherlands. After the necessary revisions, the Dutch Parliament approved the CoronaMelder app in early September 2020. On 6 October 2020 the Senate also approved the CoronaMelder App. The Minister of Health, Welfare and Sport officially launched the CoronaMelder App on 10 October 2020.

Concluding observations

It is problematic for politicians or policymakers to portray contact-tracing apps as an easy solution to ease our way out of lockdown and mitigate new waves of infection.[39] However, the discussion regarding the usefulness of CoronaMelder app has died down and the potential of the COVID-19 vaccines have currently overtaken this ‘solution’. The trajectory of the CoronaMelder app shows that a democratic process and ethical considerations are necessary for having ‘checks and balances’ in place. However, the tendency towards techno-solutionism is seemingly difficult to resist.

References

1. Lupton D. Beyond Techno-Utopia: Critical Approaches to Digital Health Technologies. Societies. 2014;4(4). doi:10.3390/soc4040706

2. Mello BMM, Wang CJ. Ethics and governance for digital disease surveillance. Science. Published online May 11, 2020:eabb9045. doi:10.1126/science.abb9045

3. Gasser U, Ienca M, Scheibner J, Sleigh J, Vayena E. Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid. The Lancet Digital Health. 2020;2(8):e425-e434. doi:10.1016/S2589-7500(20)30137-0

4. Sweeney Y. Tracking the debate on COVID-19 surveillance tools. Nature Machine Intelligence. 2020;2(6):301-304. doi:10.1038/s42256-020-0194-1

5. World Health Organization. Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing: Interim Guidance, 28 May 2020. World Health Organization; 2020. https://apps.who.int/iris/handle/10665/332200

6. eHealth Network. Common EU Toolbox for Member States.; 2020. Accessed October 8, 2020. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

7. World Health Organization. Draft Global Strategy on Digital Health 2020-2025.; 2020. Accessed October 13, 2020. https://apps.who.int/iris/handle/10665/75211

8. World Health Organization Regional Committee for Europe. European Programme of Work, 2020-2025- "United Action for Better Health in Europe."; 2020. Accessed October 13, 2020. https://apps.who.int/iris/bitstream/handle/10665/333908/70wd11e-rev4-EPW-200673.pdf?sequence=1&isAllowed=y

9. Kickbusch I, Agrawal A, Jack A, Lee N, Horton R. Governing health futures 2030: Growing up in a digital world—a joint The Lancet and Financial Times Commission. The Lancet. 2019;394(10206):1309. doi:10.1016/S0140-6736(19)32181-6

10. Oertelt-Prigione S. Prof. Sabine Oertelt-Prigione - Conference Ethics and Digitalization, 01.10.2020, in coop. with VIU - YouTube. Published October 12, 2020. Accessed October 14, 2020. https://www.youtube.com/watch?v=AEczB-De41o8

11. European Union: European Parliament. The Gender Perspective in the COVID-19 Crisis and Post-Crisis Period, 21 January 2021, P9_TA-PROV(2021)0024.; 2021. Accessed January 29, 2021. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0024_EN.pdf

12. Kool L, Dujso E, van Est R. Directed Digitalisation Working towards a Digital Transition Focused on People and Values-The Dutch Approach.; 2018. Accessed October 8, 2020. https://www.rathenau.nl/sites/default/files/2018-11/Directed%20Digitalisation.pdf

13. Niezen M, Edelenbosch R, van Bodegom L, Verhoef P. Health at the Centre – Responsible Data Sharing in the Digital Society.; 2019. Accessed October 8, 2020. https://www.rathenau.nl/sites/default/files/2019-06/HealthAtTheCentre_report.pdf

14. Webredactie TU Delft. Saving the life of medical ethics in the age of AI and

big data. Published March 26, 2018. Accessed February 14, 2021. https://www.tudelft.nl/2018/tbm/saving-the-life-of-medical-ethics-in-the-age-of-ai-and-big-data

15. European Economic and Social Committee. Impact of Digitalisation and the On-Demand Economy on Labour Markets and the Consequences for Employment and Industrial Relations; Final Study.; 2017. Accessed October 8, 2020. https://www.eesc.europa.eu/resources/docs/qe-02-17-763-en-n.pdf

16. Schobel D. Children are living in both worlds – Healthy Europe Magazine. Published online September 8, 2020. Accessed October 8, 2020. https://www.healthyeurope.info/children-are-living-in-both-worlds/

17. Verlaan D. Groot datalek bij Jeugdriagg: medische dossiers kwetsbare kinderen gelekt | RTL Nieuws. Published October 1, 2020. Accessed October 15, 2020. https://www.rtlnieuws.nl/nieuws/nederland/artikel/5187220/jeugdriagg-kenter-jeugdhulp-datalek-dossiers

18. Verlaan D. Illegale handel in privégegevens miljoenen Nederlanders uit coronasystemen GGD | RTL Nieuws. Published January 25, 2021. Accessed January 28, 2021. https://www.rtlnieuws.nl/nieuws/nederland/artikel/5210644/handel-gegevens-nederlanders-ggd-systemen-database-coronit-hpzone

19. Council of Europe. Stop cyberviolence against women and girls - View. Published November 25, 2020. Accessed January 29, 2021. https://www.coe.int/en/web/commissioner/-/stop-cyberviolence-against-women-and-girls

20. Autoriteit Persoonsgegevens. Meldplicht Datalekken: Facts & Figures. Overzicht Feiten En Cijfers 2019.; 2020. Accessed October 15, 2020. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarcijfers_meldplicht_datalekken_2019.pdf

21. Zanfir-Fortuna G. European Union’s Data-Based Policy Against the Pandemic, Explained - Future of Privacy Forum. https://fpf.org/. Published April 30, 2020. Accessed February 14, 2021. https://fpf.org/blog/european-unions-data-based-policy-against-the-pandemic-explained/

22. European Commission. A European Strategy for Data.; 2020.

23. Lupton D. The commodification of patient opinion: the digital patient experience economy in the age of big data. Sociology of Health & Illness. 2014;36(6):856-869. doi:10.1111/1467-9566.12109

24. Lupton D. Apps as Artefacts: Towards a Critical Perspective on Mobile Health and Medical Apps. Societies. 2014;4(4). doi:10.3390/soc4040606

25. Naughton J. “The goal is to automate us”: welcome to the age of surveillance capitalism. The Guardian. Published January 20, 2019. Accessed October 13, 2020. https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

26. Hafen E. Data to the People - A Fair Citizen-Centered Health Data Ecosystem. The Festival of Genomics & Biodata(2020). Accessed October 13, 2020. https://frontlinegenomics.com/wp-content/uploads/2020/04/Ernst-Hafen-ETH-Zurich.pdf

27. Gray S. Enlisting Big Data in the Fight Against Coronavirus; Senate Committee on Commerce, Science, and Transportation. Testimony and Statement for the Record.; 2020. Accessed October 13, 2020. https://www.commerce.senate.gov/services/files/F24D0AF8-D939-4D14-A963-372B9357DD7E

28. Whitelaw S, Mamas MA, Topol E, van Spall HGC. Applications of digital technology in COVID-19 pandemic planning and response. The Lancet Digital Health. 2020;2(8):e435-e440. doi:10.1016/S2589-7500(20)30142-4

29. Azzopardi-Muscat N, Ricciardi W, Odone A, Buttigieg S, Zeegers Paget D. Digitalization: potentials and pitfalls from a public health perspective. European Journal of Public Health. 2019;29(Supplement_3):1-2. doi:10.1093/eurpub/ckz169

30. McKee M, van Schalkwyk MCI, Stuckler D. The second information revolution: digitalization brings opportunities and concerns for public health. European Journal of Public Health. 2019;29(Supplement_3):3-6. doi:10.1093/eurpub/ckz160

31. Ricciardi W, Pita Barros P, Bourek A, Brouwer W, Kelsey T, Lehtonen L. How to govern the digital transformation of health services. European Journal of Public Health. 2019;29(Supplement_3):7-12. doi:10.1093/eurpub/ckz165

32. European Commission. Shaping Europe’s Digital Future.; 2020. doi:10.2759/48191

33. Azzopardi-Muscat N, Sørensen K. Towards an equitable digital public health era: promoting equity through a health literacy perspective. European Journal of Public Health. 2019;29(Supplement_3):13-17. doi:10.1093/eurpub/ckz166

34. Brall C, Schröder-Bäck P, Maeckelberghe E. Ethical aspects of digital health from a justice point of view. European Journal of Public Health. 2019;29(Supplement_3):18-22. doi:10.1093/eurpub/ckz167

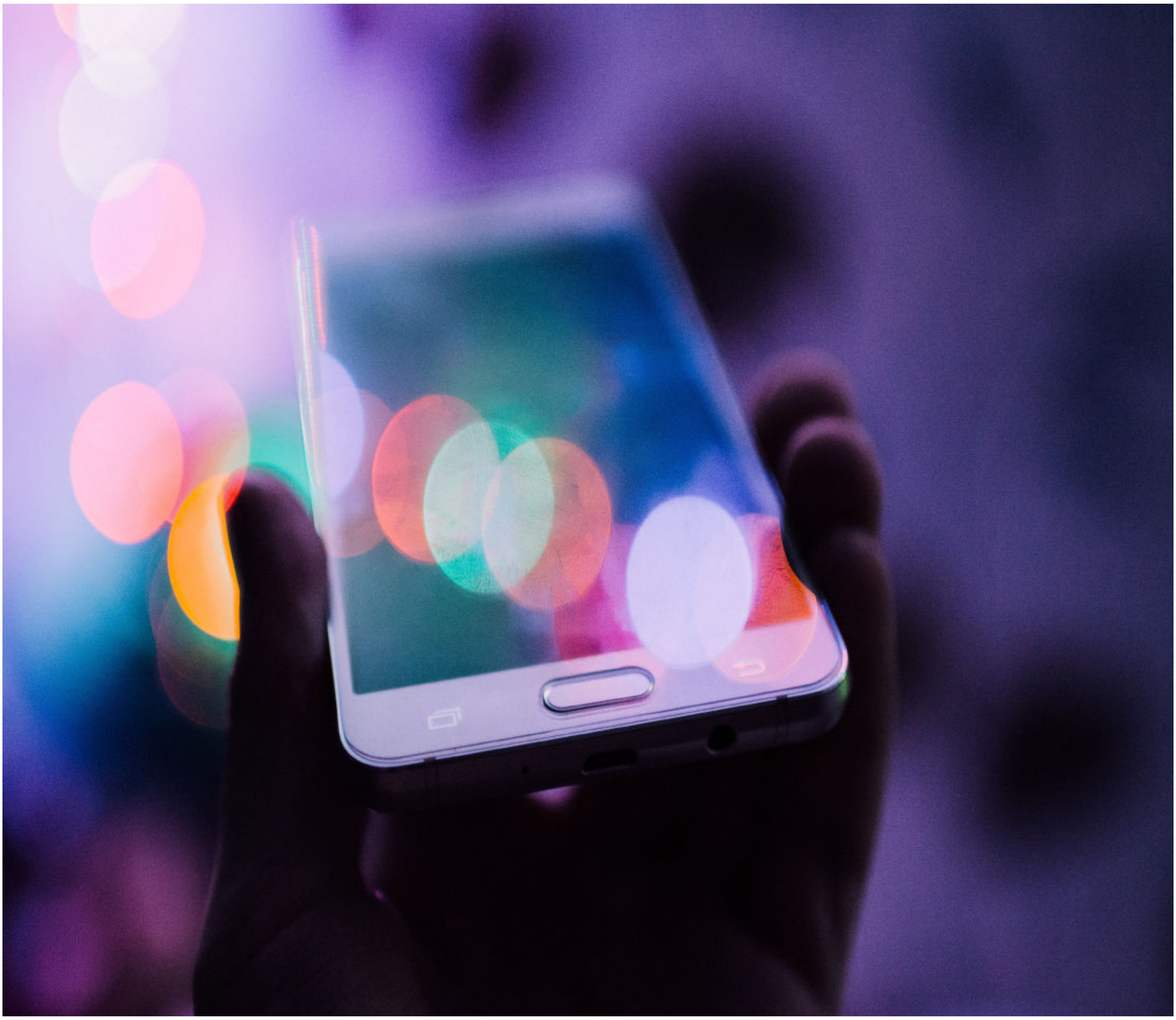
35. Stikker M. Het Internet Is Stuk. Maar We Kunnen Het Repareren. De Geus; 2019.

36. Raworth K. Doughnut Economics: Seven Ways to Think like a 21st-Century Economist. Random House; 2017.

37. Berg J, Furrer M, Harmon E, Rani U, Silberman MS. Digital Labour Platforms and the Future of Work Towards Decent Work in the Online World.; 2018.

38. Oertelt-Prigione S. The Impact of Sex and Gender in the COVID-19 Pandemic, P9_TA-PROV(2021)0024.; 2020. doi:10.2777/17055

39. Lucivero F, Hallowell N, Johnson S, Prainsack B, Samuel G, Sharon T. COVID-19 and Contact Tracing Apps: Ethical Challenges for a Social Experiment on a Global Scale. Journal of Bioethical Inquiry. 2020;17(4):835-839. doi:10.1007/s11673-020-10016-9



EUROPEAN PUBLIC HEALTH ALLIANCE (EPHA)

Rue de Trèves 49-51 • 1040 Brussels (BELGIUM) • +32 (0) 2 230 30 56 • https://epha.org/ • epha@epha.org