Intelligent Environments 2020
C.A. Iglesias et al. (Eds.)

doi:10.3233/AISE200031

Big Data and Pandemics: How to Strike Balance with Data Protection in the Age of GDPR

Aiste Gerybaite[a,1], Paola Aurucci[b1]
[a] *University of Torino; University of Bologna; University of Luxembourg*
[b] *University of Torino*

Abstract. The paper focuses on technological and legal impact of the Covid-19 crisis, drawing the attention to the convergent nature of Big Data in healthcare emergencies. While, Big Data tools have the potential to prevent, predict, manage or treat arising pandemics, at the same time the use of data driven solutions as raise numerous privacy concerns. European General Data Protection Regulation (GDPR) may fall short when it comes to addressing risks of Big Data analytic tools, in particular when it comes to the collective dimension of data protection rights. However, as shown by the recently issued guidelines of the European Data Protection Board (EDPB) is possible to find a "fair-balance" between public authorities and private entities necessity to implement surveillance measures and the respect of data protection fundamental principles.

Keywords. GDPR, Big Data, pandemics

1. Introduction

The risk of epidemics and pandemics is as real as ever. Only in the past decade, the world has dealt with Ebola, Zika, SARS and now, the ongoing 2019 Novel Coronavirus pandemic. Correspondingly, due to the widespread use of technologies, various organisations and countries have started investing into using the vast and various data (otherwise known as Big Data) available to prevent, predict, manage or treat arising pandemics. In order to extract knowledge from such Big Data for epidemiology, machine learning tools are applied. For example, novel digitised syndromic surveillance systems have been rapidly adopted by the World Health Organisation[2] in order to assist with the arising risks of epidemics and pandemics such as the outbreak of SARS in 2002[4]. Roberts observes that the emergence of these syndromic surveillance systems which sought to enhance the surveillance and reporting of pandemic risk in the late 20th century

a[1] Aiste Gerybaite; Law school of the University of Torino, Torino, Italy; Interdepartmental Centre for Research in the History, Philosophy, and Sociology of Law and in Computer Science and Law (CIRSFID) of the University of Bologna, Bologna, Italy; Computer Science Department of the University of Luxembourg, Luxembourg; E-mail: aiste.gerybaite@unio.it
b[1] Paola Aurucci, Department of Management of the University of Turin, Torino, Italy; E-mail: paola.aurucci@unito.it.

[2] Further- WHO

also facilitated a novel broader turn in practices of surveillance towards the development of new digital surveillance technologies, and the implementation of accelerated data-processing capacities to address contingent pandemic risks[14].

In Europe. the introduction of the General Data Protection Regulation[3] has also changed the way scholars, lawyers, governments, consumers, and developers look at data protection in the context of Big Data. The healthcare sector as any other had to adapt and adopt both, the Big Data tools and the GDPR norms. Google Flu Trends and Reporta are just a few Big Data tools that were deployed to manage and track diseases, both of which brought out concerns relating to data protection and unauthorised surveillance. Once the latest pandemic Covid-19 hit Europe, it has also brought on its feet the EU Data Protection Board and the national EU data protection authorities in order to address the emergency state and the request by member states' governments to deploy Big Data tools for the tracking, surveillance and managing of the epidemic. In particular, special attention requires the analysis of the articles of GDPR in the light of ensuring the balance of the protection of personal and sensitive data during such emergencies.

Through addressing the rise of Big Data within epidemiology and in particular within the monitoring, managing and treatment of epidemics globally (such as Covid-19, SARS and so on), the risks to data protection stemming from the notion of Big Data, and the introduction of the GDPR, the paper tackles the issue of balancing the right to data protection in epidemics and considers that GDPR provides the necessary legal ground for the processing of personal and sensitive data in such context.

2. Big Data in epidemiology

The risk of epidemics and pandemics is as real as ever. Only in the past decade, the world has dealt Ebola, Zika, SARS and now, the ongoing Covid-19 pandemic. Correspondingly, due to the widespread of technologies, various organisations and countries have started investing into using the vast and various data (otherwise known as Big Data) available to prevent, predict, manage or treat arising pandemics. In order to extract knowledge from such Big Data for epidemiology, machine learning tools are applied. For example, novel digitised syndromic surveillance systems have been rapidly adopted by the WHO in order to assist with the arising risks of epidemics and pandemics such as the outbreak of SARS in 2002[4]. Roberts observes that the emergence of these syndromic surveillance systems which sought to enhance the surveillance and reporting of pandemic risk in the late 20th century also facilitated a novel broader turn in practices of surveillance towards the development of new digital surveillance technologies, and the implementation of accelerated data-processing capacities to address contingent pandemic risks[14].

Canada is known to be an early adopter of Big Data in healthcare through the creation of the Global Public Health Intelligence Network[4], a cooperative effort between Health Canada and the WHO. GPHIN uses an automated web-based system which scanned newspapers and other communications globally looking for outbreak indications that were analysed by a multilingual team and where a potential risk was assessed

[3] Further- GDPR. 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, OJ L 119/1 of 4.05.2016,

[4] Further- GPHIN

communications were sent out to the appropriate stakeholders to take action[4]. Due to the proliferation of internet, emails and social media, new sources of Big Data were identified, which were also used to analyse and detect signals of early infectious disease outbreaks. With the emergence of new sources of data, new systems for Big Data applications for public health and particular pandemics were introduced too. Crowdsourcing systems which captured voluntarily submitted symptoms from the general public through the web/mobiles were introduced that provided rapid feedback about data in real-time (platforms such as FluTracking, Reporta and Flu Near You) [8].

With the proliferation of sources of the data available for the prevention, detection and management of pandemics, the data analytics field has also expanded. In machine learning, unsupervised learning tools have been used for outbreak detection, and surveillance while supervised learning tools are used for spatiotemporal hot spot detection[12]. Further, in epidemiology particularly, machine learning is integrated into causal inference techniques in order to predict or discover various pandemics[12]. Lastly, machine learning computational tools and verification methods systems allowed to improve the sensitivity and specificity of signals that are detected are being considered[4].

Despite the emergence and the use of the Big Data technologies, the Organisation for Economic Co-operation and Development[5] in its report on health data in the 21st century observed that one of the central dilemma within public healthcare sector when it comes to using Big Data is the so-called "a lot is known, but little is put into practice" issue[16]. However, OECD also notes that integrating and utilising data sources from both health organisational databases and new Big Data sources (for example, wearables, social media) hold the potential to deliver gains in public health. Sadly, only three of the OECD countries (Canada, Estonia, and the Netherlands) use Big Data sources to improve public healthcare[12]. While the potential of the Big Data is clear, the OECD does not forget to mention the requirement for precise and consistent policies to be designed for safeguarding personal and sensitive data within the context of Big Data in public healthcare.

2.1. Big Data risks

The risks associated to the outbreaks of epidemics or pandemics do not only affect global public health or worldwide economy but also due to the proliferation of digitalisation and the data available bring about unforeseen risks associated to the use of the so-called "Big Data" tools within healthcare when trying to prevent, predict, manage or treat arising pandemics. From the vast and various data collected, a value can be retrieved, and that valuable data can be used in various ways. Big Data in healthcare consists not only of electronic health records but also includes various structured and unstructured data such as clinical decisions, physician's prescriptions, medical imagining, laboratory data, data from biomedical sensors, health-app collected health-related data, Fitbit data and even social media data in the case of public health. It is also widely accepted that Big Data in healthcare may include personal and sensitive data[2]. While some of such Big Data may be anonymised or pseudo-anonymised, the reality is that Big Data analytic tools are capable of de-anonymising information and through the use of the various analytic tools re-create a profile of an individual to which the data relates to.

Leading ICT consulting firm, Gartner, defines Big Data as "high volume, high velocity, and/or wide variety information assets that require new forms of processing to

[5] Further- OECD

enable enhanced decision making, insight discovery and process optimisation.[15]" Thus, when talking about Big Data in healthcare, we refer to data sets which are too large or too complex to be managed with traditional software and would include both structured and unstructured, sensitive personal, personal and non-personal data in anonymised, pseudo-anonymised and raw formats. Interestingly, as it stands today, the GDPR scope excludes anonymised data due to the fact that anonymised data cannot be foreseen to be personal data under the scope of article 4 of GDPR. However, from a technological standpoint, there is a possibility of re-identification if an individual through the use of anonymized data in data analytics tools. This poses a question on whether the GDPR falls short in such scenarios and whether the GDPR is one step behind the technological data analytic capabilities.

In practice, the terms Big Data and Big Data in healthcare are sometimes used interchangeably because both Big Data and Big Data in healthcare would comprise of at least the 3Vs that are used to identify Big Data: volume, velocity and variety. However, when compared, Big Data and Big Data in healthcare have one significant difference- value (through knowledge). Value extractable from Big Data in healthcare is what separates generic Big Data sets and Big Data sets in healthcare.

Due to the diverse sources and types of Big Data used in epidemiology, the privacy risks associated to the use of such Big Data transpire from the notion of Big Data itself and the features attributable to Big Data, the 3Vs: volume, velocity and variety. Historically the trend for data within the public healthcare sector and particularly within epidemiology referred to the lack or incompleteness of the data available, today, as observed by Roberts, due to the analysis of the mass-data sets via automation and algorithmic processing by Google Flu Trends during the outbreak of H1N1, a new shift arose moving from the problematisation of data incompleteness towards the problematisation of data excess[15]. One can conclude that due to data excess personal privacy is affected as algorithmic tools through the use of the Big Data available are now capable more than never to refer to a particular individual.

Furthermore, due to increased dimensionality of data (variety) makes it challenging to determine whether the data is sufficiently anonymised to prevent deductive disclosure of information capable of identifying a person, as noted by Mooney[12]. Increasing amounts of data may create fingerprints that would allow subjects to be re-identified through deductive disclosure[12]. Lastly, the velocity of the Big Data flooding, for example, research network, may lead to cyberattacks as sinister payloads (such as malware) may be hidden in that flow and pass through the network firewall. From the analysis of principle features attributable to Big Data, one may observe a nexus between the legal protection of the personal or sensitive data and the technological security of data in Big Data. One cannot analyse data protection norms without addressing the technological aspect of data security.

In 2017, the EU Parliament noted that in the case of using Big Data, the risk of extracting predictive knowledge from large sets of data for making decisions concerning individuals or/and groups may lead to risks such as manipulation, discrimination or oppression of individuals and/or groups of individuals due to the mishandling of such data[17]. Similarly, the OECD in its report specified that the use of Big Data within the public healthcare sector, in a cross-border scenario encounters four main challenges: 1. data localisation laws and policies; 2. data security threats that discourage data sharing; 3. lack of global standards for data content and interoperability; and 4. commodification and sale of health data on a world market[18]. In fact, since there are no consistent global standards for content or exchange of such Big Data, private sectors actors are doing business out of it by monetising data. A few years later, in 2019, the Council of Europe issued guidelines concerning the processing of health-related data for GDPR purposes, whereas it outlined the principles such processing should follow. The Council of Europe in its guidelines defined 'health-related data' as "all personal data concerning the physical or mental health of an individual, including the provision of healthcare services, which reveals information about this individual's past, current and future health.[1]" The further elaboration by the Council of Europe on the definition of 'data related to health' and 'health-related data' seems to suggest that the protection of Big Data in healthcare does not only include personal healthcare records but expands to all types of data that can indicate an individual's health status and thus also requires special protection.

Consequently, the Big Data risks from the data protection perspective may be categorized into two dimensions: the individual privacy and the collective dimension of data protection rights when applying Big Data[3][10]. Whilst the risks associated to the individual privacy have been discussed above, a look at the collective dimension of data protection rights and risks related to groups of individuals needs to be analysed as well. Groups of individuals or societies may be manipulated, discriminated or oppressed through the mishandling of Big Data. The collective dimension of data protection rights does not only bring about the legal challenges but also incuse social and ethical issues, particularly with respect to non-discrimination and the right to equal treatment that ought to be addressed by the legislator.

3. A balance between data protection and digital epidemiology

Enhancing the use of digital technology through the creation of a Digital Single Market, is one of the European Commission's main priorities[5].

To achieve it, the EU settled a Digital Single Market strategy[5] in which health is considered a sector where digital transformation could bring benefits for both citizens and enterprises. Digital solutions for health and care have, in fact, the potential to improve access to care, to increase the overall efficiency, quality of care and economic sustainability of the health services. Data is a key enabler for digital transformation and as seen in Paragraph § 2.1 Big Data can be analysed to prevent, predict, manage or treat arising pandemics. The European Commission, in close coordination with Member States took actions to stimulate i) citizens and companies to develop their activities online, ii) innovation and iii) economic growth. At the same time, EU has enacted legislation on data protection, as well as on medical devices, electronic identification and security of network and information systems to facilitate the responsible use of digital technologies in health and care. In few words the aim of the EU is to develop a Single Market where free competition is guaranteed as well as the higher standard of data protection.

For this reason, GDPR tries guarantee the protection of patients' data while ensuring the free movement of these data, which include sharing patient data when is necessary for healthcare and research purposes. However, some doubts on its success remain since as pointed out by Annabelle Gawer the enforcement of the regulation is local while the actors involved in the processing of personal data act at a global and interconnected level[6].

In emergency exceptional situations, like the global outbreak of the COVID-19, the sheer urgency of containing an exponentially spreading virus has thrown it into sharp relief the always present conflict between data protection and right to life, the actual ability of the GDPR to strike a balance between conflicting interests and, eventually, protection of personal data has become a controversial issue. This last aspect is due to two main related factors. First, the increasing demand from public authorities and private entities for tighter measures that involve the massive processing of different types of personal data to contain and mitigate the effects of the virus. Second, the "wrong" belief that increased surveillance and unlimited limitations to the right of protection of personal data is "a necessary evil" to preserve lives[11].

In this context, the GDPR has been criticized as considered to be an obstacle to the adoption of measures that could reduce the spread of the virus.

However, as specified in Recital 1 and 4 of the GDPR, even if the right to the protection of personal data protection has been recognized as a fundamental right by the Charter of Fundamental Rights of the European Union[6] and by the Treaty on the Functioning of the European Union[7] it is not "absolute", and it must be considered in relation to its function in society and be balanced against other fundamental rights. In the strike of a fair balance between these fundamental rights and other tasks carried out in the public interest, the EU and Member States should respect the principle of proportionality. According to this principle any limitations to this right of data protection must be, as provided by law, necessary and must genuinely meet the general interest as encamped in article 52(1) of the Charter.

This said, on 16th March 2020, the Chair of the European Data Protection Board[8], Andrea Jelinek, published a statement in which, besides specifying that the GDPR rules, as seen, do not hinder measures taken in the fight against the coronavirus pandemic, it reiterates the importance of protecting personal data even in an emergency context. The same content was highlighted in the statement of 19th March[7] in which the EDPB specified the requirements of a lawful processing of personal data in the current emergency context. In particular, Andrea Jelinek, Chair of the EDPB, stressed that "Data protection rules (such as GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. However, I would like to underline that, even in these exceptional times, the data controller must ensure the protection of the personal data of the data subjects. Therefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data."[7] Thus, the EDPB statement recalls the provisions of the GDPR that should be considered for processing personal data in a context such as the one relating to COVID-19.

In particular, EDPB stressed that Article 6 of the GDPR allows the processing of personal data - without the consent of the data subject - when it is "necessary" for compliance with a legal obligation to which the controller is subject, to protect the vital interests of the data subject or of another natural person, or when it is "necessary" for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Recital 46 specifically recognizes that certain provisions in Article 6 may be relevant for purposes of public health crises such as "monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters". Data concerning health, that are relevant in this specific circumstance, are considered as "special categories of data". The processing of these data is generally prohibited, unless there are specific exemptions in the GDPR or national laws. Article 9 foresees derogations to the prohibition of processing of certain special categories of personal data, such as health information,

[6] Further- the Charter

[7] Further- TFEU

[8] Further- EDPB

where it is necessary for reasons of substantial public interest in the area of public health "such as protecting against serious cross-border threats to health" on the basis of Union or national law "which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject", such as professional secrecy article (2)(i) or where there is the need to protect the vital interests of the data subject under article 9(2)(c) of GDPR. Recital 54 of the GDPR clarifies that in these circumstances - in which processing is necessary for public health reasons - processing special categories of personal data can be done without consent, but it makes clear such processing should not result in the data being processed for other purposes by third parties, such as employers or insurance companies.

Furthermore, with regard to the processing of electronic communication data, such as location data, EDPB mentions the Directive 2002/58/EC[9], which allows the use of an individual's location data only if made anonymous or with the consent of the data subject. The EDPB stressed that under Article 15 of that Directive, Member States may adopt legislative provisions restricting the rights and obligations contained in the directive if such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society. EDPB adds that "these measures must be in accordance with the Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms» and should also be «strictly limited to the duration of the emergency"[7].

In conclusion, EDPB specifies that GDPR does not represent an obstacle to the efficiency of prevention and contrast of the epidemic but, at the same time, does not allow the unlimited limitation of a fundamental right. Therefore, to stop the spreading of the epidemic, technological solutions that use anonymous data should be a preferred way forward. The use of personal data will be admissible in emergency situations, however, appropriate safeguard to the right of data protection should be implemented and limited to the duration of the emergency.

After this statement, several Member States have started the process for adopting, "emergency legislation" to fight COVID 19 [13], and decided to make use of their discretionary powers to allow mobile device tracking as a measure to limit the spread of the disease. As a consequence, EU Member States have launched—or are in the process of launching— contact tracing apps to fight the spread of the virus. These initiatives are receiving great attention by general public and, in response, some EU Supervisory Authorities have issued statements in relation to such apps (*e.g.* Italy, Belgium, Germany, Spain and Slovenia). The lack of alignment of these Supervisory Authorities on the requirements and measures that public authorities and private sector bodies that want to use personal data (health data and location data) to track the spreading of COVID-19 should adopt to be comply with EU data protection principles have led EDPB to issue two new guidelines: on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak and the guideline on the use of location data and contact tracing tools in the context of the COVID-19 outbreak [8]. This last guideline underlines the difference between location data that can be used for modelling the spread of the virus and monitoring the overall effectiveness of confinement measure and contact tracing that - in order to break the contamination chains - can be used to notify individuals of the fact that they have been in close proximity of

[9] Further e-Privacy Directive. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), L 201/37 of 12.07.2002

someone who is eventually confirmed to be a carrier of the virus. Further, it clarifies the data protection conditions and principles that governments and private actors should follow when they want to use these data driven solutions as part of the response to the COVID-19 pandemic. In regard of the first scenario, the EDPB recalls that for location data collected from electronic communication providers shall only be processed in compliance with the Article 6 and Article 9 of the ePrivacy Directive. According to these articles, location data shall only be transmitted to authorities or other third parties if the user has given its consent[10], or such data has been anonymized. The EDPB mention (again) that - as stipulated under Article 15 of the ePrivacy Directive – there is the possibility for Member States to restrict such provisions through emergency legislation that must be necessary, appropriate and proportionate measures within a democratic society. The Board then acknowledges that rendering data anonymous is highly complex, but suggests that options for effective anonymization of mobile phone datasets do exist. In few words, in the context of pandemic, whenever possible, the processing of anonymized location data should be preferred over the processing of identifiable data. Regarding contact tracing app EDPB doesn't seem to raise objections to the use of contact tracing apps – however – they should be subject to several measures and requirements. The EDPB underlines that such applications must s be voluntary [11] , should respect minimization, purpose and storage limitation principles, should not trace individual movements but rather rely on proximity information. Moreover, these apps should be subjected to a data protection impact assessment (DPIA) prior to their implementation (the EDPB also recommends the publication of the DPIA), app-related algorithms must be auditable and it is also recommended the availability of the app's source code. The EDPB states that these applications can be based on a centralized or a decentralized approach (preferred solution)[12], yet, they must be based on an architecture relying as much as possible on users' devices and the patient's contact history (or its identifiers) should be transmitted to servers after the confirmation of the COVID-19 diagnosis. Furthermore, the EDPB also recommends that these apps can function without direct identification of individuals and some specific technical requirements should be put in place such as state-of-the-art cryptographic processes, or pseudonymous identifiers exchanging technology between users' mobile.

[10] This is valid only for data indicating the geographic position of the terminal equipment of a user which do not constitute traffic data (where separate rules apply)

[11] The Board stresses that the fact that an app is used on a voluntary basis does not necessarily mean that the relevant processing of personal data will be based on consent. Other legal bases may be relevant; in particular Article 6(1)(e) (*e.g.*, processing for the performance of a task in the public interest) may apply. To rely on these legal basis, Member States should adopt a specific legislative measure defining the purpose of the processing and appropriate safeguards. Furthermore, for the processing of special categories of data, the legal basis identified under Article 6 shall be applied only if Article 9 GDPR provides for a specific derogation from the general prohibition to process special categories of data. The EDPB considers that the appropriate Article 9 conditions for processing sensitive data in this scenario could either be that the processing is necessary for reasons of public interest in the area of public health (conditions of art. 9(2)(i) GDPR) or for health care purposes (condition under Art.9(2)(h) GDPR).

[12] The applications should not store any information which may identify COVID-19 positive individuals and possibly infected ones - due to epidemiologically relevant contact - in their centralized servers.

4. Conclusions

In this article we have discussed the convergent nature of Big Data in healthcare emergencies, such as the Covid-19 pandemics, and the interrelationship of Big Data In the light of GDPR. The authors also analysed the recent guidance issued by the EU authorities with respect to the processing of personal data for Covid-19 related tools and the strike of balance between the fundamental rights to privacy and health.

The authors of the article argued that, on the one hand, Big Data tools are extremely important when fighting various pandemics, while on the other hand, GDPR may fall short when it comes to addressing risks of Big Data analytic tools, in particular when it comes to the collective dimension of data protection rights. In this respect the authors underlined that the legislator should not only take into account the legal challenges but also address the social and ethical issues, particularly with respect to non-discrimination and the right to equal treatment.

Lastly, through the analysis of the recently issued guidelines, the authors reiterated the constant battle for the need to balance of the fundamental rights, as also noted by the EDPB. The Board underlines that EU data protection law is flexible enough to allow an efficient response to the pandemic without the erosion of individual fundamental rights. However, it notes that governments and private actors should be mindful of a number of considerations when they use data-driven solutions in response to the COVID-19 outbreak.

5. Acknowledgement

This project has been partially funded by the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie ITN EJD grant agreement No. 81417.

References

[1] Council of Europe (2019) Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data

[2] Council of Europe , European Court of Human Rights , European Data Protection Supervisor EUA for FR (EU body or agency) (2018) Handbook on European data protection law - Publications Office of the EU

[3] Council of Europe CC of C 108 (2017) Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. Strasbourg

[4] Dion M, AbdelMalik P, Mawudeku A (2015) Big Data and the Global Public Health Intelligence Network (GPHIN). Canada Commun Dis Rep 41:209–214. doi: 10.14745/ccdr.v41i09a02

[5] European Commission SWD(2015) 100 final, A Digital Single Market Strategy for Europe,

[6] European Commission (2016) Digital4EU 2016 Stakeholder Forum Report.

[7] European Data Protection Board (2020) Statement by the EDPB on the processing of personal data in the context of the COVID-19 outbreak, Brussels,

[8] European Data Protection Board, Guidelines04/2020onthe use of location data and contact tracing

tools in the context of the COVID-19 outbreak

[9] Gartner Big Data. https://www.gartner.com/en/information-technology/glossary/big-data. Accessed 29 Oct 2019

[10] Mantelero A (2016) Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. Comput Law Secur Rev 32:238–255. doi: 10.1016/j.clsr.2016.01.014

[11] Micozzi FP (2020) Le tecnologie, la protezione dei dati e l'emergenza Coronavirus: rapporto tra il possibile e il legalmente consentito. BioLaw Journal 2:1-8. Available at: https://www.biodiritto.org/content/download/3780/45269/version/1/file/13+Micozzi.pdf

[12] Mooney SJ, Pejaver V (2018) Big Data in Public Health: Terminology, Machine Learning, and Privacy. Annu Rev Public Health 39:95–112. doi: 10.1146/annurev-publhealth-040617-014208

[13] Pagallo U (2020) Sovereigns, Viruses, and the Law: The Normative Challenges of Pandemic in Today's Information Societies. Available at SSRN: https://ssrn.com/abstract=

[14] Roberts SL (2019) Big data, algorithmic governmentality and the regulation of pandemic risk. Eur J Risk Regul 10:94–115. doi: 10.1017/err.2019.6

[15] Roberts SL (2019) Big data, algorithmic governmentality and the regulation of pandemic risk. Eur. J. Risk Regul. 10:94–115

[16] Health in the 21st Century - Putting Data to Work for Stronger Health Systems - en - OECD. https://www.oecd.org/health/health-in-the-21st-century-e3b23f8e-en.htm. Accessed 14 Jan 2020

[17] (2017) Resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI))

[12] (2019) Health in the 21st Century. OECD