Privacy protection, big data gathering and public health issues: COVID-19 tracking app use in Italy

by Elena Falletti[1]

Abstract:

The Covid-19 global outbreak showed that big data gathering is an issue of international and national public health. According to comparative experience carried out especially in Taiwan, Hong Kong and South Korea contagion containment action should take place through the coordinated use of tests and tracking of infected contacts. From the end of March 2020, the Italian authorities started to prepare preparations for non-pharmaceutical interventions in order to be able to reactivate economic life and prevent the spread of COVID-19 in the country.

From this perspective, the massive collection of personal data related to COVID-19 could present a possible opportunity for the elaboration of predictive models, especially after an open discussion involving experts and public opinion about the effectiveness of the enforcement of AI models. The main challenge here was to persuade people to download and use the app, showing trust in public policies and strategies planned by the Italian Government against the COVID-19 outbreak.

In order to collect massive personal data according to the relevant constitutional and legal provisions, the Italian Government promoted a Law-decree No. 28/2020 regarding urgent measures for the introduction of a national Covid-19 alert system. It was called "Immuni". This regulation disciplines the collection and management of big data through a black box. Regarding privacy protection, this law establishes some guarantees for users, and for this purpose any person, on a voluntary basis, can download a special software application, respecting the transparency principle and providing the proper information regarding the legal framework of this data collection.

According to the Italian government, privacy protection, individual consent, and local data management were considered preferable to mandatory traceability and centralised management of the same data. However, first empirical analysis underlined that Italian people did not seem confident in the Immuni app since only 10 million people (over 60 million people of Italian population) downloaded it. Some questions about its public dissemination among citizens could emerge.

1. Introduction

1Paper presented at the Conference "Human Sovereignty and Machine Efficiency in the Law" January 14-16, 2021, The Chinese University of Hong Kong.

The Covid-19 global outbreak showed that big data gathering is an issue of international and national public health. According to comparative experience carried out especially in Taiwan, Hong Kong and South Korea contagion containment action should take place through the coordinated use of tests and tracking of infected contacts. From the end of March 2020, the Italian authorities started preparations for non-pharmaceutical interventions in order to be able to reactivate economic life and prevent the spread of COVID-19 in the country.

From this perspective, the massive collection of personal data related to COVID-19 could present a possible opportunity related to the elaboration of predictive models especially after an open discussion involving experts and public opinion about the effectiveness of the enforcement of AI models. The main challenge here was to persuade people to download and use the app, showing trust in public policies and strategies planned by the Italian Government against the COVID-19 outbreak.

In order to collect massive personal data under proper constitutional and legal provisions, the Italian Government promoted a Law-decree No. 28/2020 regarding urgent measures for the introduction of a national Covid-19 alert system. It was called “Immuni”. This regulation disciplines the collection of big data and management through a black box. Regarding privacy protection, this law establishes some guarantees for users, and for this purpose any person, on a voluntary basis, can download a special software application, respecting the transparency principle and providing the proper information regarding the legal framework of this data collection.

According to the Italian government, privacy protection, individual consent, and local data management were considered preferable to mandatory traceability and centralised management of the same data. However, first empirical analysis underlined that Italian people did not seem confident in the Immuni app since only 10 million people (over 60 million people of Italian population) downloaded it. On the one hand some questions about its public dissemination among citizens could emerge, and on the other hand issues regarding the management of contagion tracking have to be solved.

2. COVID-19 emergency and using a people tracking app (“IMMUNI”) in Italy

From the end of March 2020, the Italian authorities started preparations for non-pharmaceutical interventions (E. Gibney, 2020) in order to be able to reactivate economic life and prevent the spread of COVID-19 in the country. According to comparative experience (N. Lu, K. W. Cheng, P. Nafees Qamar, K. C. Huang, J. A. Johnson, 2020) carried out especially in Taiwan (N. Lu, K. W.

Cheng, P. Nafees Qamar, K. C. Huang, J. A. Johnson, 2020, cit.), Hong Kong and South Korea (D. De Falco, M. L. Maddalena, 2020), contagion containment action should take place through the coordinated use of tests and tracking of infected contacts (D. Shu Wei Ting, L. Carin, V. Dzau, T. Y. Wong, 2020). By tracing and containing the potential chain of infections and the isolation of the infected people, the resurgence of the general lockdown could be avoided. From this perspective, the massive collection of personal data related to COVID-19 could present a possible opportunity related to the usability for scientific research purposes (C. V. Cosgriff, D. K. Ebner, L. A. Celi, 2020), and for the elaboration of predictive models (A. Cho, 2020; L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dörner, M. Parker, D. Bonsall, C. Fraser, 2020; 10.1126/science.abb6936; D. S. Wei Ting, L. Carin, V. Dzau, T. Y. Wong, 2020; C. Buckee, 2020), especially after an open discussion involving experts and public opinion about the effectiveness of the enforcement of theoretical models.

At the end of the emergency, (e.g., the so-called "phase II") a new issue emerged. This concerned the development and putting into practice of several new contact-tracing apps that could help to keep economic activities, social life and countries open before a vaccine became available (Edwards, 2020, 301). The main challenge here was to persuade people to download and use the app, showing trust in public policies and strategies planned by the Italian Government against the COVID-19 outbreak.

The policy choice made by national governments, including the Italian one, was between two different approaches. On one hand, there is the centralised model, in which the anonymised data gathered is uploaded to a single national remote server where data matches are made with other contacts, in the case where a person starts to develop Covid-19 symptoms. This choice allows outbreak control and data collection, storage and treatment to be maintained at national level, placing the protection of privacy in the background, even if personal data are anonymised. On the other hand, the decentralised model keeps personal information on the users' device. In this case, data matches are made with people who may be contaminated (Trucco, 2020, 3; Frosini, 2020). From a technical perspective, this approach uses technological infrastructures provided by Google and Apple. Apparently, it seems to be more privacy focused, but it grants both American tech giants significant "soft power" (Trucco, 2020).

In order to collect personal (big) data under constitutional and legal provisions, the Italian Government promoted a Law-decree No. 28/2020 regarding, at Article No. 6, urgent measures for the introduction of a national Covid-19 alert system.

However, from my investigative point of view, big data collected in such a manner concerns health and personal feelings, and both belong to the data holders' body; in that, they are a result of physical reaction in the same way as body heat, heart beating, blood pressure. These are elements consequent with bodily reactions, provoked both by mood and by physiological condition. The tools for controlling and collecting such data could be the same, usually represented by wearable devices such as smartwatches, smartphones or bracelets. Indeed, the legislative regulation must be particularly careful, in order to avoid allowing the massive collection of data relating to a data holder's feelings and behaviour, and therefore lead to a possible manipulation of the thoughts of entire populations who are the data collection source (Y. N. Harari, 2020; C. Degeling, S. M. Carter, A. M. van Oijen, J. McAnulty, V. Sintchenko, A. Braunack-Mayer, T. Yarwood, J. Johnson, G. L. Gilbert, 2020; Fairchild AL, Haghdoost AA, Bayer R, Selgelid MJ, Dawson A, Saxena A, et al. 2012). A strict regulation for limiting the data use in time and purpose is necessary.

This law-decree provides important restrictions to constitutional freedoms (especially, articles no. 13. Right to liberty, and 16. Freedom of movement) as well as to European Union law, in particular Articles No. 7 and 8 of the Charter of Fundamental Rights of the European Union. However, the regulation must comply with the provisions of art. 5 GDPR on guarantees of application of proportionate, lawful, certain, adequate and necessary measures (M. Festa, 1, 2020). Specifically, the big data should be used to design maps for identification of epidemiological situations regarding the development of infections. For this purpose, a supranational regulatory coverage is identified. In this sense Article No. 9 of the E-Privacy Directive, "*legitimizes the anonymous data treatment, even in the absence of the data subject's consent, of the location of the collected personal data*" (M. Festa, 1, 2020, cit.). However, the Italian Privacy Authority's warning specifies, sanctioned also by Article No. 15 of the same E-Privacy Directive, a necessary national regulatory intervention that must be sufficiently detailed, containing adequate and suitable guarantees, whatever the subsequent application will be. In order to achieve this goal, the Italian Government established the abovementioned Law-Decree No. 28/2020.

The specific regulation regarding COVID-19 tracking data is established by Article No. 6. It takes into account the multiple statements provided both by the Italian Privacy Authority and the European Union Data Protection Board's "*Guidelines on the processing of health data for research purposes in the context of the COVID-19 outbreak*", and "*Guidelines on geolocation and other tracing tools in the context of the COVID-19 outbreak"*. Its declared purpose is to alert people who

have entered into close contact with persons affected by COVID-19 and protect their health preventing them from spreading the contagion.

This regulation disciplines the collection of big data and management through a black box. According to Article No. 6, paragraph 1, in order to implement public health measures related to restraining the spread of COVID-19, a national platform system management alert is installed. From a legal point of view, due to the public interest for public health concerns a legislative provision is needed. This does not seem revocable, since the choice of a primary rank standard meets the requirements of art. 9, par. 2, lett. i) GDPR, thus justifying the processing of health-related health data (particular data), as well as the explicit and informed consent given by the interested party (users or citizens who have voluntarily downloaded the application on their cell phone or smart device).

3. Developing "Immuni" app between (few) lights and (some) shadows

Regarding privacy protection, this law establishes some guarantees for users, and for this purpose any person, on a voluntary basis, can download a special software application, respecting the transparency principle and providing the proper information regarding the legal framework of this data collection.

Apparently, this data processing is intended exclusively for location of the data traced, and not for further purposes. However, such data could be used for scientific and statistical research purposes, since the data are anonymous and aggregate, therefore within the limits set by the GDPR. Furthermore, data processing is carried out through the use of the "Immuni" App and is intended for recording only contacts between subjects who have also downloaded the application.

Regarding data selection, the processed data collected regards exclusively proximity contacts (proximity location), therefore neither mapping through geolocation systems nor constant tracking of the location of the subjects who have downloaded the application is permitted. Data retention is limited to the strictly necessary period and, in any case, no longer than the time allowed by the Ministry of Health.

From the point of view of reciprocity of anonymity, the data that allow the tracing of the proximity location will not be shared between users/citizens, who will only receive an alert when proximity contact with a Covid-19 positive result has been found. Finally, the data controller has been identified in the Ministry of Health, which coordinates its activities according to art. 28 GDPR.

According to the Italian government, privacy protection, individual consent, and local data management were considered preferable to mandatory traceability and centralised management of the same data. Why is this so? Hypothetically, it would have been difficult to manage such a large mass of data, even using advanced technical methods and in such a short time (Trucco, cit., 5). In this regard, individual privacy would be guaranteed by "privacy by design". This technology seems to prevent third party access to personal data collected on the smartphones, by sending a package of personal information linked to a double exchange of anonymised codes. The aim of this process is to prevent the recombination of the anonymised data with the decoding keys that could be able to use biometric and personal data in order to reconstruct user identity (L. Garofalo, 2020).

With regard to strengthening the protection of users' privacy, these circumstances are of particular interest and concern the attachment/connection (in both physical and metaphorical sense) between personal data and electronic device (in this case the data owner's smartphone), as well as the fact that these data are transmitted with cryptography. This process could be described as follows. The starting point regards contact tracing, which identifies contacts between smartphones and exchanges encrypted metadata stored in each smartphone. It is possible through random, pseudo-anonymised and dynamic identifiers such as the RPI (Rolling Proximity Identifier), to transfer data once processed by secondary and random keys, i.e. the RPIK (Rolling Proximity Identifier Key).These keys are produced by primary keys, as the TEK (Temporary Exposure Key), which have a longer duration than the RPI. All the information is gathered by cryptographic algorithms developed by the backend system (Trucco, cit. 6).

This tracking methodology falls down on the "disconnection" of the tracing data from the identity of the users. This is the so-called the "inferential re-identification" (especially regarding people positive to COVID-19) by app users in order to reconstruct the contact chain backwards up to the person at the origin of the infection. On this point, it is necessary to keep in mind the Italian Privacy Authority warning, according to which it is necessary to avoid the eventuality that such proximity identifiers and short-term pseudonyms "could be detected by third parties" (Italian Privacy Authority, 2020) and associated with other user identification data, especially if the persons are positive to Covid-19 (Trucco, cit., 7).

However, it is noted that Italian law (precisely Article No 6, (1) D.L. 28/2020) allows for the collection of a large amount of personal information (big data) transferred by users to the tracking system operators (in this case Immuni) concerning real life. On one hand, this data reconstructs the digital second life of users, and on the other hand the system enables the collection of additional

data (analytics) allowed by the abovementioned law, through the same devices used for public health purposes and service improvement. Furthermore, the tracking system operators could collect other highly identifying data, but not directly useful from the health point of view such as IMEI codes, IP address, bluetooth connection data (Trucco, cit. 8).

Now, a crossroads opens up. On one hand, it may be asked whether "an act of trust" is enough to implement a tracking infrastructure that is extraneous to European jurisdiction, such as the de-centralised one proposed by Google/Apple (Calderini, 2020). This should be prevented, in favour of European Union member states' jurisdiction, since doubts emerge about the implementation of a machine learning model related to the algorithms used on big data collected by the devices contained in black boxes. Indeed, through this, it is possible to trace the person's identity, and profile his or her behaviour (Trucco, 2020, 8).

On the other hand, we may consider whether releasing an open source program code is a proper solution, enhancing the retention of data on personal devices, instead of on a platform, although the law itself (Articles 6, (3), DL 28/2020) allows such data to be used in "aggregate or anonymous form for public health, prophylaxis, statistics or scientific research purposes".

Specifically, in the Italian case, this platform is managed by the Ministry of Health which, through a "Diagnosis Server" exchanges the daily TEK identification data, associated with the positive cases, and therefore verified with the list of RPIs stored on the same Smartphones during a specific period of time. In this procedure, the Apple/Google software acts like a bridge, permitting the verification of the steps backwards by reconstructing the data collected (TEK, RPIK, RIP), in order to trace the reference device from which the contagion alert was sent.

At this point, in the event of a positive response, the people who have been alerted can decide to contact the health professionals, closing the circle of traceability of the infection.

4. Is it a matter of worthiness choices?

From the point of view of worthiness choices, two alternatives could be kept in mind. On one hand, it might be wondered whether turning to an assumed redemptive power of technology is acceptable (Orefice, 2020), since technology should be capable of "bypassing" and resolving autonomously such legal issues, also through the authoritative power of the government (Curreri, 2020). On the other hand, the option regards the decision as to whether complying with the traditional hierarchy of legal sources, starting from the constitutional source of protection of inviolable rights, should be preferable.

In any case, the juridical form of the technological tool (i.e. the tracking app useful to trace infected people) used to tackle the emergency is important, and legitimates the legal framework that for reasons of protection of public health imposes very invasive restrictive measures on personal freedoms of each person (Sirleaf, 2018). Nevertheless, the prospective tracking app should be adopted within the limits set by the Constitution, which in these serious circumstances seem weak.

Among the most problematic issues are significant “hierarchical aspects” in the matter of sources of law, like the choice promoted by the Government of the company "Bending Spoons" in charge of designing and developing the tracking app. This choice followed a public "fast call for contribution" to develop such a tracking app called "Innova per l'Italia", which lasted three days (Orefice, cit.). This company was identified on the basis of the "spirit of solidarity" characterizing its proposal, since the company itself granted an open, free and perpetual "license of use" for the app and gave its willingness to complete IT developments for the implementation of the national digital contact tracing system (Orefice, cit.). Some scholars observed that the operation conducted by the Ministries of Health, Economic Development and Innovation, who, in cooperation with the Working Group of experts, chose the winner of the call, performed a balancing act between privacy and public health ex ante, choosing a suitable technology having regard to a greater attention to safety (Colapietro, Iannuzzi, 2020). Other scholarly opinions stressed that the winner of this call was “*pre-authorized (...) through a sub-legislative instrument (i.e., the abovementioned call) to process the personal data of any person through an application already developed, then postponing the identification, in second place, of the measures and guarantees appropriate to the decree law*” (Orefice, cit.).

Regulation 679/2016 prohibits the processing of health data; however, Article No 9, par. 2 lett. i) of the same legislation establishes an exception in the interest of public health under national law (Orefice, cit.), by virtue of the specificities of each EU Member State, whose Legislator can decide how appropriately to intervene, pursuant to Whereas No. 54 of the GDPR itself. There is a sensitive point here regarding the examination of the appropriateness of legal forms, given that, from a strictly legal point of view, the Italian Government promoted, for the purpose of collecting personal data, the abovementioned Decree Law n. 28/2020, bearing at Article No. 6 “Urgent measures for the introduction of a national alert system against national Covid-19”. However, this decree law was issued only after the choice of the application of data tracking and its developer (i.e., 30 April 2020), approved by the Special Commissioner for the COVID-19 emergency (Presidency of the Council of Ministers) with the decree of assignment of 16 April 2020.

Article No. 6 of DL 28/2020 establishes the methods of tracing that the chosen system should have followed. It was formulated in general terms ex post, almost dissimulating "the intention to introduce specific provisions addressed at an already developed application and a predetermined private subject, giving the basis of lawfulness *a posteriori* defined without assessing the risks in advance" (Orefice). This method contradicted the GDPR's own *ratio*, which requires that the assessments of the availability of operational risks should be carried out ex ante, not ex post. Such an assessment would allow for the establishment of an appropriate instrument following the appropriate consideration of the influence that each technological choice may have on each legal principle. In this regard, the European Data Protection Board stressed that the app design phase should always include a detailed examination of the app architecture with the prior assessment of the effects and possible impacts on the rights and the freedoms of the persons concerned (Resta, 2020; Orefice, cit.), in view of the effects of the increasingly invasive incidence of technological tools in the life (therefore on the rights of the personality) of the concerned persons (Resta, cit.).The technology is not neutral even if it is blind (C. Schmitt, 1929), on the contrary its blindness can lead to serious discrimination in its use, since it can generate discrimination between equals or treat equally different cases (Orefice, cit.). In this perspective, it would be necessary to assess the adequacy of the technology that is to be applied to personal tracking by detailed questions about the (actual) use of the collected and stored personal (big) data (Resta, cit.). The sensitive issue regards the fact that these data do not concern only the protection of health, but also other fundamental personal liberties and rights involved in such data processing, such as personal freedom or the right of movement and assembly (Orefice, cit.; Zeno Zencovich, 2020).

Using these data, is it possible to imagine an algorithmic risk assessment, by sending an automated alert, or a preventive screening carried out by health authorities? In the first case, does the quarantine requirement become automatic until the diagnostic test is carried out? In the second case, are the instruments used for this screening sufficient and effective in terms of pandemic containment?

From these questions a complex issue could emerge: on one hand it is focused on the data processing itself, and on the other hand it regards the health infrastructure management.

On the first point, the basic problem raised by the abovementioned questions concerns the choice of the personal data collection model and the relative compression of personal information freedom of self-determination (Resta, cit.), which is stronger in intensity and effects when computer technologies are involved (H. Cho, S. Ippolito, Y. W. Yu, 2020).

Indeed, any automated processing of data requires a prior assessment of the proportionality of the interference: therefore, the depersonalization introduced in the process of identifying contacts is related to the problem of the effects to which they can be traced. Hence, this issue regards what influences such detection, and what consequences it may have with respect to the matching carried out by the algorithm, and so the related alert signal sent by the tracking app itself (G. Resta, cit.).

Given the inaccuracy of the proximity collection (G. Resta, cit.), the data entered in the black box could be influenced by the fact that such proximity tracing "has the defect of producing a not marginal number of false positives, not being able to give reliable information about the situational context of the contact" (G. Resta, cit.).

This is one of the most significant problems related to the use of a decentralized app, and here the second problematic point emerges, because, entrusting the identification of standardized contacts carried out by the software on the basis of “ex ante” proximity parameters, decontextualized from space and time criteria, users may be led to avoid contacting not contact their doctor or may decide not to download the application (G. Resta, cit.).

As of January 24 2021, Immuni has been downloaded 10,214,893 times, with a strong increase in recent weeks, sending 85,155 notifications and reporting 9,442 positive users (source: https://www.immuni.italia.it/dashboard.html). These data suggest that scholars who feared that the rate of utilization (and of feedback in the tracing of positives) was scarce did not express entirely unfounded opinions. There is also a clear imbalance in contact tracing numbers. Indeed, it reveals a serious problem concerning the ability to trace, and thus isolate, the contacts of positive persons. This is an essential step for the containment of the pandemic, which at the moment seems to be a crucial point in Italy.

5. Short Bibliography

Calderini, B., Covid-19, tra diritto alla salute e tutela della privacy: la scelta che l’Italia deve fare, https://agendadigitale.eu, 24.3.2020;

Cho, H., Ippolito, S., Yu, Y. W., Contact Tracing Mobile Apps for Covid-19. Privacy Considerations and Related Trade-offs, 25.3.2020, https://arxiv.org/abs/2003.11511;

Christovich, M. M., (2016), Why Should We Care What Fitbit Shares?: A Proposed Statutory Solution to Protect Sensitive Personal Fitness Information, 38 Hastings Comm. & Ent. L.J. 91;

Colapietro, C., Iannuzzi, A., App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali, in Dirittifondamentali.it, 2, 2020);

Cortez, N., The Mobile Health Revolution? (June 24, 2013). UC Davis Law Review, Vol. 47, 2014;

Cosgriff, C. V., Ebner, D. K., Celi, L. A., Data sharing in the era of COVID-19, The Lancet, Digital Health, 2020, 2, E22, https://doi.org/10.1016/S2589-7500(20)30082-0;

Curreri, S., L'attività parlamentare ai tempi del Covid-19: fiat iustitia et pereat mundus? In laCostituzione.info, 11.3.2020);

De Falco, D., Maddalena, M. L., La politica del tracciamento dei contatti e dei test per covid-19 alla luce delle ultime direttive OMS: nessun ostacolo giuridico impedisce di utilizzare il "modello coreano" anche in Italia, Federalismi.it, 28.3.2020;

Degeling, C. Carter, S. M., van Oijen, A. M., McAnulty, J., Sintchenko, V., Braunack-Mayer, A., Yarwood, T., Johnson, J., Gilbert, G. L., Community perspectives on the benefits and risks of technologically enhanced communicable disease surveillance systems: a report on four community juries, BMC Med Ethics 21, 31 (2020);

Edwards, L., Tracking the debate on COVID-19 surveillance tools, Nature Machine Intelligence, 2, June 2020, 301;

Fairchild A. L., Haghdoost A. A., Bayer R., Selgelid M. J., Dawson A., Saxena A., et al. Ethics of public health surveillance: new guidelines. Lancet Public Health. 2017;2(8):e348–e9;

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker M., Bonsall, D., Fraser, C., Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing, Science, (2020), 10.1126/science.abb6936;

Festa, M., (1) Mappe Epidemiologiche, sorveglianza e Contact Tracing: i chiarimenti del Garante, Quotidiano Giuridico, 10.4.2020;

Festa, M., (2), Ultimo capitolo della saga IMMUNI: l'App, autorizzata dal Garante, è finalmente negli store, Quotidiano Giuridico, 1.6.2020;

Frosini, T. E., Anonimato, privacy, niente obbligo: le salvaguardie ora ci sono, 5.5.2020, https://www.ildubbio.news/2020/05/05/anonimato-privacy-niente-obbligo-le-salvaguardie-ora-ci-sono/;

Gibney, E., *Whose coronavirus strategy worked best? Scientists hunt most effective policies*, Nature 581, 15-16 (2020);

Harari, Y. N., The World After Coronavirus, Financial Times, 20.3.2020;

Hartzog, W., Selinger, E. (2013), Big Data in Small Hands, 66 STAN. L. REV. ONLINE 81;
Iaselli, M., (2015) Internet of Things, droni e robotica. Problemi giuridici e possibili soluzioni, Altalex Editore;
Kilker, S. J., Effectiveness of Federal Regulation of Mobile Medical Applications, 93 WASH. U. L. REV. 1341 (2016);
Lu, N., Cheng, K. W., Nafees Qamar, P., Huang, K. C., Johnson, J. A., Weathering COVID-19 Storm: Successful Control Measures of Five Asian Countries, AJIC: American Journal of Infection Control (2020), doi: https://doi.org/10.1016/j.ajic.2020.04.021;
Orefice, M., L'app Immuni: salute, privacy e trasparenza, in Liber Amicorum per Pasquale Costanzo, 2020, http://www.giurcost.org/studi/index.html;
Resta, G., La app "Immuni": pregi e limiti del tracciamento digitale dei contatti, Medialaws, 15.6.2020;
Schmitt C., The Age of Neutralizations and Depoliticizations (1929), in Telos 1993(96):130-142;
Segura Anaya, L. H., Abeer A., Costadopoulos, N., Prasad P. W., (2017), Ethical Implications of User Perceptions of Wearable Devices, Sci Eng Ethics, Doi: 10.1007/s11948-017-9872-8;
Shu Wei Ting, D., Carin, L. Dzau, V., Wong, T. Y., *Digital technology and COVID-19,* Nature Medicine volume 26, pages459–461(2020);
Shu Wei Ting, D., Carin, L. Dzau, V., Wong, T. Y., Digital technology and COVID-19, Nature Medicine volume 26, pages459–461(2020);
Sirleaf, M., Responsibility for Epidemics, in 97 TEX.L.REV. 285, 2018, 109 ss.;
Trucco, L., App. Immuni una storia stran(ier) e incompiuta, 25.5.2020, www.giustiziainsieme.it
Van Woense, L., Archer, G., (2015), Ten technologies which could change our lives, Potential Impacts and policy implications, European Parliamentary Research Service;
Zeno Zencovich, V., I limiti delle discussioni sulle "app" di tracciamento anti-Covid e il futuro della medicina digitale, in Medialaws, 26.5.2020.