Algorithmic Vulnerability in Deploying Vaccination Certificates in the European Union and China

Janet Hui XUE*

This article further develops the concept of algorithmic vulnerability. The analysis is built on empirical evidence of the Chinese Health Code System (HCS), compared to similar plans for the "COVID-19 Certificate" in the European Union (EU). Implementing the HCS has shown two-sided regulatory implications: improving social protection (a national strategy, a common mutual-recognition standard, scaled-up public–private cooperation) and increasing risks of social exclusion (non-digital and digital forms of vulnerability). This article argues that algorithmic vulnerability is caused by mismatches between biased databases, unfairly pre-designed algorithms and dynamically changed risk groups in reality in the context of COVID-19 vaccination. It contributes a framework for deploying plans for digital certificates in the EU concerning minimising the social risks associated with algorithmic vulnerability. The framework consists of (1) reinforcing existing vulnerability inherited from non-digital society (eg caused by intersectional factors of race/ethnicity, gender, age and health) and (2) introducing new forms of vulnerability generated by algorithm design and implementation (eg excluding the risk groups of individuals who are un/ mis/overrepresented in the databases, such as those defined by nationality plus COVID-19 status).

I. A TERRITORY-BASED APPROACH INTENDED TO SOLVE A TERRITORY-LESS CRISIS

COVID-19 has increased multi-level tensions regarding the governance of a territory-unbounded global crisis with territory-bounded approaches.[1] Vaccination certificates seem to offer a territory-based solution to mitigate some of these crises. As Häkli in this special issue argues, while nationality-based passports already often serve to divide and exclude people, COVID-19-based vaccination "passports" may exacerbate such divisions and exclusions through vulnerability that is both evident and hidden.[2]

1 A Alemanno, "The European Response to COVID-19: From Regulatory Emulation to Regulatory Coordination?" (2020) 11 European Journal of Risk Regulation 307.

2 J Häkli, "COVID-19 Certificates as a New Form of Mobility Control" (2021) European Journal of Risk Regulation, this special issue.

Despite the long existence of vaccination certificates and "passports", the contemporary digitised vaccine certificates cause more concern compared to their paper counterparts. The reason for this is that algorithms trigger the linking of data systems of vaccination records, COVID-19 test results, personal IDs and contact information that may enable micro-targeting of individuals for a variety of exclusionary purposes, including job rejection. The profound ever-present risk is that classifying, profiling and grouping individuals based on nationality now linked to COVID-19 status will risk further social stratification of people through systematic vulnerability. Such systematic vulnerability ultimately may not be corrected; it is hidden in the machine learning of ever-growing databases, which may further exacerbate existing vulnerability in a post-COVID-19 future and thereby disadvantage individuals in accessing employment, study and business opportunities and in processing medical insurance claims.

Existing research that theorises vulnerability often accounts for four groups of factors: biological, psychological, socio-demographic and resilience.[3] Vulnerability means that individuals are subject to less autonomy in making their decisions and to unfair treatment.[4] While technology tends to offer resilient solutions in the short term, it may bring in new types of vulnerability, which are intertwined with new sets of risks in the long run.[5] Furthermore, despite different policy responses to the COVID-19 pandemic, utilising the COVID-19 vaccination certificates in the Global South (eg China) and the Global North (eg the European Union (EU)) has shown some of the same challenges, tied to what I call "algorithmic vulnerability". I argue that algorithmic vulnerability means that subjects receive unfair treatment, suffer socioeconomic harm or lose autonomy over independent decisions due to a host of problems linked to the use of algorithms. An algorithm can produce such problems in a variety of ways, such as biased training data, where the structure of data sets is not representative of certain racial/ethnic groups of people. For example, some groups of users are unable to be vaccinated because data related to them are collected in a training database, as a result of which they are at risk of not being prioritised to receive the vaccine. Vulnerability can be caused by the design of the algorithm as its results show "an effect of the partial relations among entities", which proportionally redefines the spatial relations between the fully vaccinated and the unvaccinated. Furthermore, when these data are recorded in databases of vaccination certificates, the relations of individuals are grouped based on levels of SARS-CoV-2 and the risks imposed on others. Finally, regardless of an algorithm's design, a certain group of people may be subject to vulnerability simply because of the accuracy rate for identifying targeted individuals according to its priority list. Often in practice there is no easy way to understand how an algorithm can make or has already made mistakes.

---

3   See, eg, G Hufschmidt, "A comparative analysis of several vulnerability concepts" (2011) 58 Natural Hazards 621 <http://link.springer.com/10.1007/s11069-011-9823-7>; E Ligon and L Schechter, "Measuring vulnerability" (2003) 113 The Economic Journal C95 <https://academic.oup.com/ej/article/113/486/C95-C102/5060962>; L Shi and GD Stevens, "Vulnerability and unmet health care needs" (2005) 20 Journal of General Internal Medicine 148 <http://link.springer.com/10.1111/j.1525-1497.2005.40136.x>.

4   H ten Have, *Vulnerability Challenging Bioethics* (1st edn, London, Routledge 2016).

5   A Hommels, J Mesman and WE Bijker (eds), *Vulnerability in Technological Cultures* (1st edn, Cambridge, MA, MIT Press 2014). Also see M Campbell-Verduyn, "The pandemic techno-solutionist dilemma" (2021) Global Perspectives, accepted/in press.

Consequently, algorithmic vulnerability as a system's property can trigger three types of risks (see Section IV): the risks that deprive a certain group of people from being vaccinated in a timely manner as they deserve to be and thus receive vaccination certificates; the risk that the access by certain groups of individuals to medical care, jobs and insurance will be deterred; and the risk of the ambiguous assessment of virus transmission imposed on others because of uncertainty/limited information decoded from vaccination certificates.

The Chinese Health Code System (HCS; discussed in Section II) has experienced some of the challenges currently confronting the EU's proposed COVID-19 Certificate, such as promoting interoperability while ensuring ethical data use. It is valuable to draw upon the HCS's experience to help avoid potential algorithmic vulnerability when the EU rolls out its own Certificate. Instead of marginalising those individuals and risking depriving them of access to social benefits, medical care and insurance claims, the core of designing and employing algorithms should reflect collective values among people, regulatory authorities and corporate service providers. These values should respect the equality and fairness of "collective health"[6] and sustain it as a "collective public good".[7]

II. The HCS in China and the COVID-19 Certificate in the EU

According to the European Commission's (EC) current proposal of the COVID-19 Certificate, three types of certificates will be issued: a vaccination certificate, a test certificate and a certificate of recovery from previous COVID-19 infection.[8] Among the first type of certificates, algorithms to distribute vaccination will largely affect the consequences of obtaining a vaccination certificate because getting vaccinated is a prerequisite to getting a vaccination certificate. That is, an algorithm determines the allotted time and brand of vaccination to individuals depending on the risk scores (eg who might be infected most among the same age group). The worst-case scenario that could happen in the future is that automated profiling (eg the vaccinated, non-vaccinated and COVID-19 free, non-vaccinated but COVID-19 infected) may be triggered by an algorithm that makes certain groups subject to more vulnerable positions – absence from the database and thus unrecognised by the digitised vaccination certificate system. A typical example has been discussed in the concluding article of this special issue for those who receive a vaccine such as Sputnik V or Sinopharm that is not approved by the European Medicines Agency (EMA)[9] and who therefore may be not recognised by a predetermined algorithm and consequently may be prevented from entering the EU.

---

[6] B Pereira and J Stornelli, "Collective health versus individual freedom: goal centrality and political identity shape Covid-19 prevention behaviors" (2020) Journal of the Association for Consumer Research 711837 <https://www.journals.uchicago.edu/doi/10.1086/711837>.

[7] For further explanations of "collective public goods" or "collective self-rule", see L Bialasiewicz and C Eckes, "'Individual sovereignty' in pandemic times - a contradiction in terms?" (2021) 85 Political Geography 102277.

[8] European Commission, Art 3(a) Proposal on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate) COM (2021) 130 final.

[9] D Kochenov and JD Veraldi, "The Commission against the internal market and European Union citizens' rights: trying to shoot down Sputnik with the 'Digital Green Certificate'?" (2021) European Journal of Risk Regulation, this special issue.

The HCS started its roll out in February 2020 after the outbreak of COVID-19.[10] On 17 March 2021, the EC first announced its plan for a COVID-19 Certificate.[11] The HCS is a social-technical infrastructure that is used to identify SARS-CoV-2 infection associated with ID information. The HCS is not an official claim by Chinese governments; I use the term to summarise the key features of the system and for analytical convenience. The assessment of the HCS is computed based on three types of data: case number, travel history and risk level of origin. It issues each applicant a colour code that indicates green for COVID-19 free, yellow for COVID-19 risk and red for COVID-19 infected. The main purpose of the HCS in particular is to separate SARS-CoV-2-infected people from the rest of the population while allowing free mobility across borders inside and outside of China. It also has prepared the Chinese government to launch a digital COVID-19 certificate for international travel.[12]

Both the HCS and the EU COVID-19 Certificate have paper and digital forms, which contain a QR code. Differently, the HCS relies on aggregating data from different agencies to reach an overall assessment of an individual's health status containing the SARS-CoV-2 virus as indicated by the three colours. In contrast, the EU COVID-19 Certificate will function through verifying vaccination information via the EC's public key and links the verification results to each individual's ID.[13] In response to the debate about privileged vaccinated individuals regaining their freedom while access by the non-vaccinated public to public spaces is limited, the current proposal for the Certificate extends to add test results and statements of recovery to the framework of certificates. Since the Certificate will contain and present three types of information, its system will involve more data processors across the EU Member States, such as certificate issuers, COVID-19 test issuers, certificate verifiers, ID issuers, certificate readers and app providers. In the Chinese context, the HCS was used at public checkpoints, such as public transportation, restaurants and supermarkets. It is as yet unclear whether the EU COVID-19 Certificate will be applied only to cross-border travel or also to other public checkpoints domestically, as is the HCS, although a number of EU civil society organisations and national privacy watchdogs have already raised objections to such extended use.

III. Algorithmic vulnerability

Generally speaking, an algorithm "often uses mathematical optimisation techniques [to] perform one or more tasks such as gathering, combining, cleaning, sorting, classifying

---

[10] Gov.cn, "Zhejiang Hangzhou launches 'health code' to prevent and control the epidemic" (浙江杭州上线"健康码"防控疫情) (11 February 2020) <http://www.gov.cn/xinwen/2020-02/11/content_5477358.htm>.

[11] European Commission, Proposal on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate) COM (2021) 130 final.

[12] Minister of Foreign Affairs published news entitled "Good news! The Chinese version of 'International Travel Health Certificate' is officially launched" (好消息！中国版"国际旅行健康证明"正式上线) (8 March 2021) <http://cs.mfa.gov.cn/gyls/lsgz/fwxx/t1859289.shtml>.

[13] eHealth Network, "Guidelines on verifiable vaccination certificates - basic interoperability elements" (12 March 2021) <https://ec.europa.eu/health/sites/health/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf>.

and inferring data, as well as selection, prioritisation, the making of recommendations and decision making".[14] The stated purpose of vaccination certificates is to identify verified vaccination records that are associated with individuals rather than tracking an identified individual. Both the Chinese HCS and the proposed COVID-19 Certificate in the EU may involve rule-based algorithms and algorithms of data analytics of large sets of data. In the context of the HCS, the algorithm computes data from local medical service entities, such as the Centre for Disease Prevention and Control, local clinics, general practitioners, community centres and hospitals, to generate an up-to-date list of candidates who need to be vaccinated following a priority plan. In EU countries such as the Netherlands, studies have examined the potential use of algorithms to estimate the risks of prioritising vaccination, but there is no clear evidence that demonstrates a national- or provincial-level effect in this respect.[15]

Designing algorithms for COVID-19 vaccination distribution reflects a preferred value (eg prioritising lowering fatality and infection rates). Algorithms prioritise controlling risks over others that are designed concerning a more complex and often intersectional set of parameters such as age, underlying health conditions and occupation.[16] Yet defining the controlling risks is a moving target that depends on the progress of the virus and infection rates in the population. Since the stated goal of the EU COVID-19 Certificate rollout is to reopen the economy and recover mobility, policymakers could decide, for instance, that priority should go to high-density populations who may be infected at scale, and not to the riskiest infection groups, such as cross-border essential workers in transport or agriculture, who cannot work from home and who live in densely populated industrial regions.

Implementing an algorithm relies on analytics of aggregating data retrieved from multiple certificate issuers and verifiers. Applying an algorithm may expedite the issuing of vaccination certificates in real time and at scale, but such automation may consistently and systematically exclude those certain groups of individuals from future policy focus. For instance, people with type 2 diabetes and recently immigrated workers not yet registered on medical care systems may be represented at a proportionally lower level in the entire databases. Consequently, even though immigrant workers with type 2 diabetes may be in a high-risk infection group, they may be excluded from the priority list of being stamped as vaccinated and thus receiving certificates.

---

[14] Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence MSI-AUT, Council of Europe, Addressing the impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, available at <https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf>.

[15] R Herings et al, "Development and validation of an algorithm to estimate the risk of severe complications of COVID-19 to prioritise vaccination" (8 February 2021) <https://www.medrxiv.org/content/10.1101/2021.02.05.21251197v1>.

[16] ECDC, "Overview of the implementation of COVID-19 vaccination strategies and vaccine deployment plans in the EU/EEA" (29 March 2021) <https://www.ecdc.europa.eu/sites/default/files/documents/Overview-implementation-COVID-19-vaccination-strategies-vaccine-deployment-plans.pdf>. See also, eg, A Blasimme and E Vayena, "The ethics of AI in biomedical research, patient care, and public health" in MD Dubber, F Pasquale and S Das (eds), *The Oxford Handbook of Ethics of AI* (Oxford, Oxford University Press 2020).

Differently from the four parameters that constitute vulnerability outlined at the outset of this article, this paper further develops the framework of algorithmic vulnerability,[17] which is based on the premise that algorithms can (1) reinforce existing vulnerability inherited from a non-digital society (eg intersectional factors of race/ethnicity, gender, age and health) and (2) introduce new forms of vulnerability created by algorithmic bias (eg excluding the risk group of health consumers who are un/mis/ overrepresented in the databases and, further, biases arising from the algorithm).

Regarding reinforcing existing vulnerability, intersectional factors in the context of vaccination distribution may delay certain groups of individuals from obtaining vaccination certificates in EU countries. There are a few scenarios that question the design such algorithms of vaccination when they would affect implementing the EU COVID-19 Certificate. For example, who will be vaccinated first among young people with chronic diseases, pregnant women and senior citizens without chronic diseases? Moreover, automatically generated reports fail to identify and prioritise risk groups among those who really need to be vaccinated first such as cross-border workers in essential services if these workers are unregistered with the database where the algorithm applies. Additionally, an algorithm may not recognise those who are vaccinated outside of the EU or are recorded in a database outside of the EU as having been vaccinated with vaccines not approved by the EMA (although now Member States can decide to extend their acceptable vaccine lists).

Reference to new vulnerability may be introduced by special notes referenced in the EU COVID-19 Certificate, including stages of vaccination, brands of vaccination, mutation information (eg B.1.1.7., B.1.167) and previous COVID-19 history (eg infected but not recovered, infected and recovered, infected and recovered but with severe post-COVID-19 syndromes or infected twice by different mutations). Ironically, some who were vaccinated first may have been deterred from employment opportunities because of information encoded in their vaccination records, such as those aged under twenty-five with chronic disease, for example. Finally, according to Article 2(2) of the original Proposal,[18] the Certificate will first concern EU citizens and members of their families and also non-EU nationals legally staying or legally residing in the territory of a Member State.[19] This means that people residing in the EU with a legal visa fall into the second framework of the Certificate proposal. If their test result issuers are not listed according to Council Recommendation 2021/C24/01, they cannot receive certificates and will not be permitted to cross borders. Furthermore, the vaccination rate is slow within the EU and also is progressing at varying speeds. As of 16 May 2021, 37.8% of the region's adult population had received at least one vaccine dose and 16.2% had completed a full vaccine series.[20]

---

[17]   JH Xue, "Algorithmically vulnerable consumers: redefining vulnerability in accessing health services in China" (18 December 2020), Eleventh Meeting of the UNCTAD Research Partnership Platform <https://unctad.org/system/files/non-official-document/ccpb_RPP_2020_04_Present_Janet_Xue.pdf>.

[18]   ibid, 11.

[19]   The Council of the European Union, "COVID-19: Council agrees its negotiating mandate on the Digital Green Certificate" (14 April 2021) <https://www.consilium.europa.eu/en/press/press-releases/2021/04/14/covid-19-council-agrees-its-negotiating-mandate-on-the-digital-green-certificate/>.

[20]   ECDC, "Key figures on the vaccine rollout in the EU/EEA as of week 19, 2021" (16 May 2021) <https://covid19-vaccine-report.ecdc.europa.eu/>.

The following groups of individuals will be lower in the priority list in practice: non-EU citizens or their families yet to receive certificates and EU citizens and their families residing outside of the EU who have received vaccinations not approved by the EMA.

IV. Reflection on the Chinese HCS in Comparison with the COVID-19 Certificate of the EU

The core challenges in rolling out the COVID-19 Certificate in the EU show many similarities to those faced in China's deployment of the HCS: (1) how to strike the balance between a rapid rollout and minimising the risks of algorithmic vulnerability; (2) how to roll out certificates quickly inside and outside the space covered by the certificate; and (3) how to accomplish interoperability in order to ensure the same standard of accuracy and authentication.

The Chinese central government responded to these challenges quickly, which has shown two sides of the social implications. Positively, as shown from the above, utilising the HCS improves overall social protection through a national strategy, a common recognition standard and scaled-up public–private cooperation. A central policy promoted the national strategy and leadership through operating a national gateway. On 9 February 2020, the Chinese national regulator – the Cyberspace Administration of China (CAC) – issued the "Notice on the Protection of Personal Information and Using Big Data to Support Joint Prevention and Joint Control Work".[21] Serving as a central piece of national legislation outlining a national strategy, the policy also legally defined the relationship between Chinese governments and two major corporate service providers. In facing the problems concerning various local versions of the health code in the initial stage, the Chinese central government quickly promoted health code apps provided by two companies, Tencent and Alipay. Tencent launched its first health code app in Guangzhou on 31 January 2020. By 18 March 2020, Tencent claimed to have covered more than 300 cities and counties and nearly 900 million people.[22] Furthermore, the State Administration for Market Supervision (National Standards Committee) issued the national standard "Personal Health Code" on 29 April 2020 to ensure compatibility between different health codes.[23] As it has shown, mutual recognition is realised through WeChat's existing large population of users inside and outside of China. Finally, by legitimising service on governmental demand, the Chinese central government can rapidly unify services operated by the same mini-programme and accessed by the national gateway via a QR code through the national gateway.

The interoperation plan was also able to be implemented based on years of effort in digitising health resources and services. By relying on the available technical

---

[21] Cyberspace Administration of China, "Notice on protecting personal information and using big data to support joint prevention and joint control" (25 February 2020) <http://www.cac.gov.cn/2020-02/09/c_1582791585580220.htm>.

[22] Tencent, "Tencent Health Code" (腾讯防疫健康码) (2020) <https://www.tencent.com/zh-cn/business/health-code.html>.

[23] Gov.cn, "The national standard for the personal Health Code is released" (个人健康信息码国家标准发布) (2 May 2020) <http://www.gov.cn/xinwen/2020-05/02/content_5508190.htm>.

infrastructure, verifying information contained in the code across databases of different local operators was feasibly achieved in the short term. The Chinese Council initiated a national plan of e-health among other digitising plans starting in 2018 to improve access to universal health insurance, medicine supply and mobile payment to improve their services. Approximately 711 online hospitals nationwide provided COVID-19-related enquiries,[24] one example of which is WeDoctor, a mobile application to allow people access to healthcare from home, whether that be urban or rural. WeDoctor started making a name for itself as introducing "China's first Internet-based hospital". Currently, its platform has grown to more than 2700 hospitals in mainland China and 27 million monthly active users.[25] Various e-health services in use already before COVID-19 have allowed a large population to access essential health resources. This has also served to reduce risks due to unnecessary mobility and hospital visits and also limited scenarios of the health code to very essential needs. The National Health Commission of the People's Republic of China also facilitated the use of online medical care to ease the burden on hospitals. The available e-health service enables individuals with chronic diseases or pregnant women to access regular medical care and receive medicine without visiting hospitals.

On the downside, the HCS still faces the same challenges that the EU is facing: (1) sustaining trust between the general public and governments; (2) using a transparent approach to ensure the fair design of the algorithm and data use; and (3) initiating a plan to ensure data security during the COVID-19 pandemic and an exit plan to prevent the repurposing of data collected for vaccination certificates. The HCS also increases risks of social exclusion caused by both non-digital and digital forms of social discrimination. Concerning the long-term effect of preventing unfair or even forged data use beyond COVID-19 prevention purposes, it is necessary to clarify the liability between governments and private service providers regarding the misuse of data involved in data collection, data sharing and data processing between WeChat and the local data entities that provide the data.

V. A FRAMEWORK FOR POLICYMAKING MINIMISING ALGORITHMIC VULNERABILITY IN THE LONG RUN

Both China and the EU have announced that the HCS and the COVID-19 Certificate are temporary solutions for the pandemic moment. China has stated that the data retention period will end when the pandemic ends, while the EC has announced that the Certificate system will be suspended once "the World Health Organization (WHO) declares the end of the COVID-19 international health emergency".[26] However, it is not easy to exclude completely the repurposing of a similar infrastructure for a similar purpose, or its expansion to other areas. The Chinese Zhejiang government has already started to

[24]   XY Xu et al, "Assessment of Internet hospitals in China during the COVID-19 pandemic: national cross-sectional data analysis study" (2021) 23(1) Journal of Medical Internet Research e21825.
[25]   H Vo, "China's healthcare revolution: WeDoctor" (24 February 2019) <https://digital.hbs.edu/platform-digit/submission/chinas-healthcare-revolution-wedoctor/>.
[26]   European Commission, "Questions and answers – Digital Green Certificate, questions and answers" (17 March 2021) <https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1187>.

consider linking the health code to future medical insurance. Similarly, the EC has stated that "if the WHO declares a new international public health emergency caused by COVID-19, a variant of it, or a similar infectious disease, the system could be reactivated". Should we accept the normalisation of these kinds of emergency plans as part of the social-technological infrastructure in our future society?

Using such a social-technological infrastructure after COVID-19 may lead to the development of a systematic bias towards certain groups that is not obvious from the algorithm's description itself. The bias caused by algorithms, even though they are not necessarily machine learning algorithms, may generate adverse social consequences that cannot be corrected. In the short term, such a digital infrastructure that may link digitising health system ID systems across the EU could potentially become "a widespread system of vaccine microtargeting".[27] In the long run, the general public that is in greater need of services but not represented in the database may be excluded from the focus of future policymaking and policy interventions.

1. From eliminating algorithmic venerability during COVID-19 to minimising systematic vulnerability after COVID-19

As mentioned above, long-term vulnerability may arise once the digital infrastructure deploys and is repeatedly utilised for future public crises until it is normalised in our lives. However, the algorithm-caused vulnerability has not been properly addressed in current policies both in the EU and in China. In the paragraphs below, I sketch out a framework concerning algorithmic vulnerability for the EC and counterpart regulators in each Member State.

First, it is essential not only to minimise data collection to limited purposes, but also to minimise data disclosure and usability scenarios. Since both the Chinese central government and the EC stress the principle of minimal data collection, many certificate issuers and verifiers are involved. Consequently, the risk of data breach and data forgery is high. The former has been documented in China with, for instance, the leak of personal information of more than 7000 returnees from Wuhan,[28] while the latter has occurred in EU Member States, with booming sales of fraudulent negative COVID-19 test certificates.[29] Once such sensitive information related to the COVID-19 infection is leaked, algorithmic vulnerability will become real, and long-term social harm may damage this group of data subjects for the rest of their lives. This chilling effect may discourage people from being vaccinated or obtaining certificates.

[27] USA TODAY, "Could we save lives by assigning each American a place in line for vaccines?" (14 April 2021) <https://www.usatoday.com/in-depth/news/2021/04/14/vaccines-medical-records-could-decide-your-place-line/7115621002/>.

[28] Nanfang Daily, "超七千武汉返乡者信息泄露，被短信骚扰谩骂！相关登记方称未披露" (More than 7000 returnees from Wuhan spread information and were harassed and abused by text messages!) (27 January 2020) <https://m.mp.oeeee.com/a/BAAFRD000020200127254378.html>.

[29] EUROPOL, "Early warning notification – the illicit sales of false negative COVID-19 test certificates" (1 February 2021) <https://www.europol.europa.eu/early-warning-notification-illicit-sales-of-false-negative-covid-19-test-certificates>.

Second, it is not entirely clear whether the expected usability of certificates is for cross-border travel only or for returning to public lives, including work, school, supermarkets and places of entertainment. This raises the question as to whether the algorithm also needs to determine the types of information disclosure according to the usability setting. For instance, a restriction may vary from an airport for international travel to everyday businesses, such as public transportation, workplaces and schools, and to occasional businesses, such as restaurants, supermarkets and entertainment events. If a vaccine certificate must be presented at workplaces and schools wherever people check in, the minimal data principle will apply not only to collection but also to disclosure.

Third, if a certificate is widely demanded to enter public spaces and join public events, it is essential to decide how much information the verifier at each checkpoint can read. To ease the public's concern about social discrimination associated with privacy intrusion, an overall assessment similar to the colour code of the HCS may be applicable instead of the detailed full disclosure of all COVID-19-related health information. If a similar plan is considered, a further discussion must occur about designing an algorithm to aggregate data, analyse data and issue an overall assessment based on a common standard.

2. From regional interoperability to a return to a formerly familiar globalised society

The Chinese experience has shown that ensuring interoperability across the borders of provinces was critical to implementing the entire HCS successfully. The EC's plan also urged the realisation of interoperability between the different technical solutions being developed by the Member States. The key question, indeed, is: under what internationally recognised standard can people who have been vaccinated be recognised equally when crossing a national border? On 27 January 2021, the EU eHealth Network adopted guidelines on proof of vaccination for medical purposes, which it updated on 12 March 2021.[30] These guidelines, in particular the preferred code standards, should form the basis for the technical specifications adopted for the purpose of the COVID-19 Certificate proposal.[31] It is essential to increase awareness among regulators, algorithm developers and operators as to how algorithms can affect their policymaking regarding a regional consensus on common standards. These common standards help determine the scope of data collection, the standard of data aggregation, the duration of data retention, the security measures of data storage and data sharing, and data verification and assessment. As Milan et al in this special issue also emphasise, proper design is key to optimising equality among international certification systems.[32]

Importantly, efforts that aim to verify data across databases located in various jurisdictions will need to tackle multiple challenges, including integrating data standards and compliance with data protection laws and other soft laws related to

---

[30] ibid, 13.

[31] ibid, 11.

[32] S Milan, M Veale, L Taylor and S Gürses, "Promises made to be broken: performance and performativity in digital vaccine and immunity certification" (2021) European Journal of Risk Regulation, this special issue.

pandemic prevention and control. It took years of effort within China to achieve this goal. The current COVID-19 Certificate proposal shows a plan to achieve mutual recognition within the EU.[33] Given growing political and legal concerns about data protection, it will be difficult to achieve verifying systems across the EU Member States or even internationally in the foreseeable future. An EU-wide gateway portal will function as a coordinating mechanism to share lessons and experiences learnt not only from the Member States but also from non-EU states. Despite differing national and regional policy responses to the pandemic, reducing vulnerability should be a shared value among human beings. The artificial boundaries created by vaccination certificates, which now delimit both nationality and COVID-19 status, risk creating further exclusion rather than remedying vulnerability. Rather, regional cooperation and sharing of lessons and practices to reduce vulnerability should be the starting points in reconnecting the world.

---

[33]   eHealth Network, "Outline, interoperability of health certificates trust framework" (12 March 2021) <https://ec.europa.eu/health/sites/health/files/ehealth/docs/trust-framework_interoperability_certificates_en.pdf>.