ALGORITHM WATCH

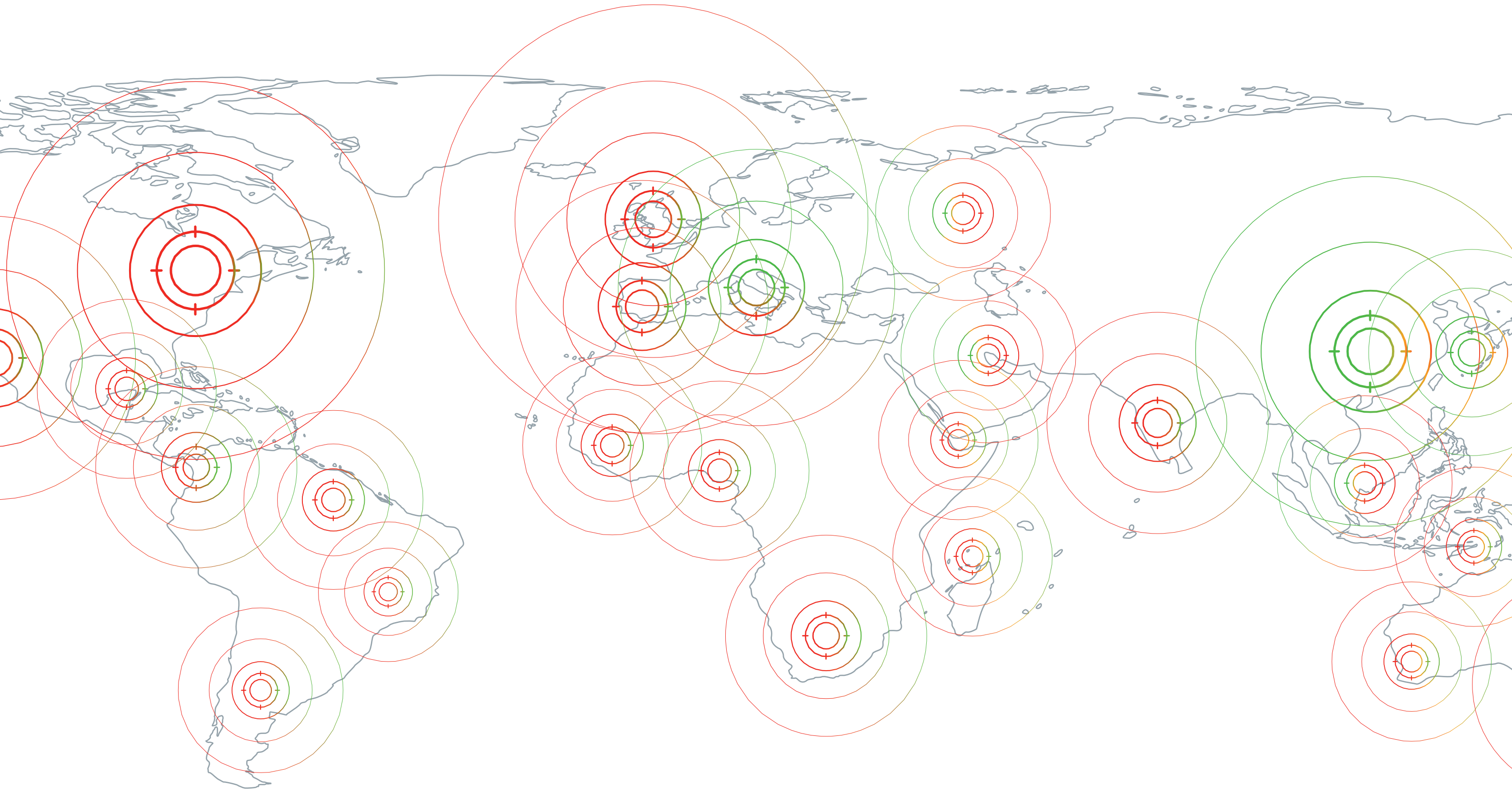
Automated decision-making systems and the fight against COVID-19 – our position

1st version (2 April 2020)

As the COVID-19 pandemic rages throughout the world, many are wondering whether and how to use automated decision-making systems (ADMS) to curb the outbreak. Different solutions are being proposed and implemented in different countries, ranging from authoritarian social control (China) to privacy-oriented, decentralized solutions (MIT's 'Safe Path'). What follows is a set of possible principles and considerations on which to ground an informed, democratic and useful discussion regarding the use of ADMS in the current pandemic.

1. **The COVID-19 is not a technological problem.** Analyses of actual responses to the outbreak show that successful interventions are always grounded in broader public health policies. Singapore, South Korea and Taiwan, frequently cited as role models in keeping the epidemic in check, all had plans in place, most of them designed after the 2003 SARS outbreak. Preparedness for an epidemic reaches beyond technical solutions: it means having resources, competences, plans, and the political legitimacy and the will to quickly deploy them when needed.

2. **There is no one-size-fits-all solution to the COVID-19 outbreak.** Success in the fight against the virus requires testing, contact tracing and confinement. However, no two contexts are identical. A country where the virus has been circulating undetected for months (e.g. Italy) is different from a country that identified carriers of the virus early on (e.g. South Korea). Social, political and cultural differences also matter when it comes to enforcing public health policies. This means that the same technological solution might yield very different results in such different contexts.

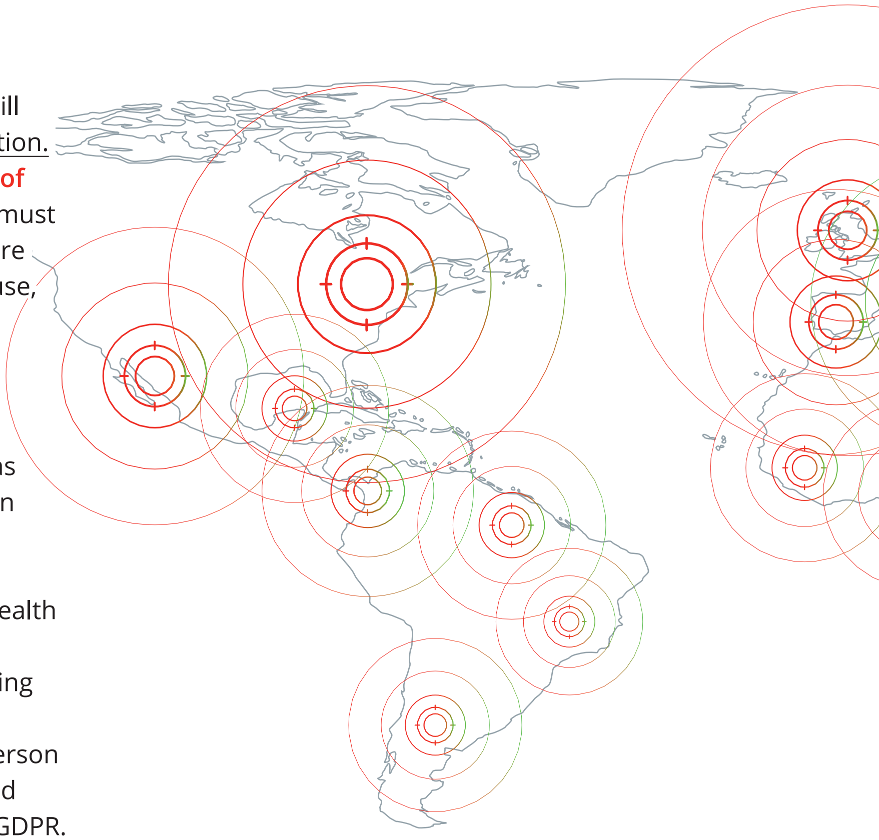


3. Consequently, **there is no need to rush into mass digital surveillance to fight the COVID-19 disease.** It is not just a matter of privacy — although privacy remains a fundamental right and needs to be respected. Before considering the data protection implications of digital contact tracing apps, for example, we should ask: ***do they work, at all?*** Results from literature and past epidemics are currently mixed and depend heavily on context. Rights must be balanced with the expected benefits (saving lives). But there is no need to sacrifice our fundamental liberties if this serves no purpose.

4. Lockdowns cannot last indefinitely. **We have to think of how to gradually go back to "normal".** Most scenarios involve some kind of digital surveillance, which appears to become necessary once specific aspects of COVID-19 are taken into consideration: the existence of asymptomatic patients who can however be infectious, the 14 days incubation period, the fact that there is no existing cure or vaccine to the disease yet). Civil society organizations have to be ready to contribute to the discussion regarding the monitoring solutions under consideration, in order to assist in coming up with adequate approaches.

5. **Protection against COVID-19 and protection of privacy are not mutually exclusive.** Solutions such as the one developed by the MIT ('Safe Paths') and the Pan-European Privacy Preserving Proximity Tracing initiative couple digital contact tracing with an open, decentralized and more rights-preserving approach. This is also the way in which countries such as Singapore are tackling the issue (eg. through the 'TraceTogether' app), which is different from the approach taken by South Korea and Israel.

6. **Any solution must be implemented in a way that is compatible with democracy.** Democracy does not stand in the way of halting the pandemic: it is the only hope we have of tackling it rationally and respecting the rights of all. Transparency should be paramount in 1) the technological solutions being worked on, 2) the teams of experts or ad-hoc institutions created to work on them, 3) the evidence as to why it should actually be implemented, 4) who will eventually build and deploy them, especially if private entities are involved. Only transparency will ensure that civil society and parliamentarians are able to hold decision-makers to account.



7. The datafication that comes with the development of ADMS to fight the virus will create new social categories at risk of discrimination. **Governments must prevent the stigmatization of individuals** landing in the wrong categories and must preserve the rights of individuals who do not score high enough on the scales that are being put in use, especially regarding triage in healthcare.

8. Even when shown to be actually useful, **digital surveillance solutions should be firmly grounded in data protection principles:** as recently clarified by the European Data Protection Board in a statement, necessity, proportionality, purpose limitation and the rule of law in general must be respected, even in the face of a public health emergency. Citizens must be able to appeal any decision taken by an automated system concerning COVID-19 (especially apps determining whether someone has been in contact with an infected person and must undergo quarantine). Governments and contractors must abide by the provisions of the GDPR.

9. **Pre-existing ADM solutions should not be repurposed and adopted for COVID-19 responses,** as automated systems that rely on training data from the past cannot, by design, handle a sudden change in the conditions in which they are deployed. Predictive policing, automated assistance to judges, credit scoring and scores of other ADMS could produce outcomes that fall far short of their normal range (e.g. regarding the error rates). Such systems should be urgently audited, or suspended.

10. **A pandemic is global by definition. There needs to be a set of global, diverse and coordinated responses to it.** A global network of civil society organizations working together should monitor the responses to the pandemic. Previous emergencies taught us that emergencies give unscrupulous political leaders the perfect excuse to legitimize mass surveillance infrastructures that needlessly — and indefinitely — infringe on the rights of all. Resistance to this has been (partly) successful only when it was global, coordinated, and strongly worded, with clarity and evidence on our side.

11. Lastly, **we should ensure that this debate about COVID-19 surveillance does not happen in a vacuum.** Some ADMS, most notably face recognition, already proved to be problematic. The current state of emergency cannot be used to justify their deployment: on the contrary, all issues highlighted during “ordinary” times — lack of accuracy, systematic bias in its prescriptions, broader concerns about possible abuses of biometric data etc. — become even more important during exceptional times, when the health and safety of all are at stake. We should not only make sure that this crucial debate is not led by technologists or technologies, but also ensure that the technologies involved are proven to benefit society. The suspension of in-person communications provides an opportunity to move even more welfare and other fundamental services online, where ADMS often replace caseworkers. This could have catastrophic consequences for citizens who have no access to or no means to critically understand digital tools. We have to make sure this will not happen.

Lead author: Fabio Chiusi, with the cooperation of Nicolas Kayser-Bril