MALTA IT LAW ASSOCIATION

Resolving the tension between stopping the coronavirus and safeguarding legal freedoms.

Digital tools play an important role in addressing the COVID-19 pandemic. They can help model infection trajectory, socio-economic impact, monitor physical distancing and aid contact tracing. However, these technologies can increase surveillance and possibly impact societal values such as privacy and human agency. Navigating the tension between legal norms, ethical principles and public health requirements in this crisis is critical. MITLA feels it can play a part in this discussion by bringing a degree of academic insight into IT-law matters. The COVID-19 Self-Assessment tool announced by Minister Fearne late last week, and originally developed by the Estonian Health Board, is a good starting point, however it already presents its own issues. Our perspectives are based on the imperative to stop the virus without sacrificing our political or legal freedoms. This in turn creates the right social environment for future societies that inclusively and holistically increase human wellbeing.

Value-Based design

Digital solutions will be adopted by citizens if they are trusted, and this further in line with the European Data Protection Board's (hereinafter the 'EDPB') Guidelines 03/2020 and 04/2020, wherein it stipulated that the use of any such applications by the general public should be voluntary, rather than compulsory. In this light, careful consideration of stakeholder and societal values must be taken into consideration. Decisions on the design and form of any application should therefore be tied to the benefit it creates within society and more importantly, the efforts towards limiting the exposure of the COVID-19 virus. Any such decisions should be based on the formulation of relevant questions or identification of potential problems. One should therefore question what manner of implementation of the tool will yield the most accurate results and will be the most effective step to achieving the objective?

- Is the tool accessible to those with disability?
- Does it discriminate against users with lesser abilities?
- Does it provide the expected benefits that our population expects with minimal impact on privacy?
- Does the tool incorporate safeguards to prevent stigmatisation?

Transparency

The principle of transparency means that personal data shall be processed fairly and in a transparent manner in relation to the data subject. The data subject must therefore be able to understand how and why the tools works, and this in order to be fully aware and informed. Compliance with this obligation arises out of numerous pieces of regulation, perhaps most clearly from Regulation [EU] 2016/679 (hereinafter the 'GDPR'), and recently highlighted in the European Commission's Recommendation (EU) 2020/518 which discusses the use of technology and data to combat and exit from the COVID-19 crisis. It must be noted that the aforementioned COVID-19 Self-Assessment provides absolutely no information to the user which data, if any, is captured, how the data is captured, where it is stored, or for how long it is stored.

Explainability

In basic terms, this is defined as "why is this happening?". Any tool implemented should provide a degree of information and explanation of the tool's outputs and predictions. By providing such explanations as to why the tool predicts COVID-19 infection or lack thereof, the general public as well as interested third parties, such as researchers, can understand why the tool provides a specific output. Ensuring explainability also provides the opportunity for the improvement of the tool as well as allows the identification of required solutions, if any. Linked to this, the EDPB has stated the source code for any such applications should be made publicly available.

Data Sovereignty

This crisis provides a crucial opportunity to re-focus on sovereign data technologies, policies, and mindsets so individuals can create and curate the terms and conditions regarding access to their identity and personal data. This is a basic tenet of informational self-determination which itself is based on the understanding that data is safe, specific and used for a finite time-limited purpose. The location of the data store should also be made known in an effort to increase openness and transparency.

Data Minimisation, Security & Other Data Protection Principles

Although the present tool in Malta is not designed for contact tracing yet, it is useful to reflect on such eventuality. It has been stated, by both the EU Commission and the EDPB, that in the implementation of contact tracing apps, the processing of location data is not a requisite, and should in fact be avoided. Instead, proximity data should be used as less intrusive but effective measure in order to reduce unnecessary risks to security, and also compliance with the principle of data minimisation.

Any digital tools developed must be fully compliant with data protection and privacy rules within the EU. For compliance with the GDPR, the app's author (or publisher) should identify who the data controller is. The European Commission is of the view that such digital tools should be designed in a manner that the national health authority is the data controller. This would further enhance trust among the app's users. More so it will ensure that the digital tool is being used for its intended purpose of protecting public health. Furthermore, such apps should be based on anonymised data in order to alert people who have been in proximity to an infected person for a certain duration to get tested/ self-isolate without revealing the identity of the infected person.

Trustworthiness

As highlighted above, the important prerequisite for the development, acceptance and up-take of such apps by individuals is trust. People must have the certainty that compliance with fundamental rights is ensured and that the apps will be used only for the specifically defined purposes, that they will not be used for mass surveillance, and that individuals will remain in control of their data. It is therefore of essence that such apps provide the necessary information relating to the processing of personal data, the individual's rights under GDPR (particularly access, rectification and deletion), that free, specific, explicit and informed consent is given by the individual for any information to be accessed on the individual's device and the storage time limits of the individual's data. The European Commission issued a number of recommendations to ensure the security of the data, including the use of state-of-the-art cryptographic

techniques to encrypt and pseudonymise the personal data stored on the terminal device of the individual. These recommendations should be considered and implemented.

In light of the fact of the increased involvement and participation of the number and type of entities in the handling of the COVID-19 outbreak, it is crucial that appropriate technical and organisations measures, such as the undertaking of data protection impact assessments, are implemented in order to fulfil the principle of integrity and confidentiality.

The driving force behind MITLA is to assist local technological empowerment through technology-neutral legal frameworks by providing a specialized forum where legal developments within the ICT sector can be studied, discussed and championed. You can reach MITLA by sending an email to: info@mitla.org.mt with your thoughts and questions.

www.mitla.org.mt
info@mitla.org.mt
SmartCity Malta, SCM 1001, Ricasoli, Malta

MALTA IT LAW
ASSOCIATION