Cybersecurity and privacy dialogue between Europe and Japan

A resume of the revised version of
the Cybersecurity Research Analysis Report for the two regions

Legal and Policy aspects

The goal of this resume is to give a quick glance at the picture of the cybersecurity and privacy in Europe and Japan, as it is more analytically shown in the report 3.2 of the EUNITY project. This resume provides the view of legal and policy aspects only. The report 3.2 analyses the priorities in both EU and Japan, in order to produce an overview on the status of cybersecurity and privacy research and innovation activities. Among others, the report elicits the legal and regulatory landscape, with special attention to the GDPR and focuses on the analysis of regulatory documents, EU directives as well as laws and legal frameworks. It elicits the common regulatory aspects of cybersecurity and privacy, for example obligations for monitoring, certification, protection of personal data and information exchange.

Main conclusions of the EU and Japan comparison

Both regions have undergone a period of substantial reforms and modernization of the existing legal frameworks with regard to privacy. In Europe, the GDPR entered into force in May 2018 and brought up a significant update of the legislation with a strict compliance bar foreseen for its enforcement. In Japan, the Act on Personal Information was recently amended. However, the so-called adequacy decision for the free mutual transfer of personal data has been adopted between the EU and Japan, which allows a mutual recognition of an equivalent level of data protection, it should be nevertheless noted that the two frameworks are not perfectly matching. For instance, the concepts of sensitive personal data, as well as some practical implications such as the diverging approach on the imposition of fines and sanctions might become a critical point for both Japanese and European businesses and organizations wanting to enter each other's digital markets.

In contrast, the cybersecurity domain is somewhat dissimilar from the one described above. At a first glance, differences might be spotted in the laws of the two regions, mostly pertaining to their scope and the stakeholders such laws apply to, thus diverging from one another in substantial elements. However, some lines of similarities can yet be pointed out. This can be observed in the room left by both policy and legal frameworks allowing EU, Member States and Japanese Government to engage in international cooperation, particularly in the fields of international norms settings and common strategy building, promotion and awareness raising of a cybersecurity culture within the respective territories and beyond.

Challenges and Gaps

A number of points that have been identified as potential blockers or issues to be addressed in order to further strengthen the cooperation between the EU and Japan in the domains of privacy and cybersecurity.

- The **scope** of the two privacy legislations differ quite significantly in their application: whilst Japanese laws include the offering of goods and services only, the EU framework extends its scope to non-European organizations offering services in Europe and to those targeting market behaviours of data subjects. For this reason, the imbalance stands on the European side, seemingly creating a burden on Japanese organizations wanting to monitor market behaviours of their potential customers.
- The **concept of personal information** is not aligned between the two regions. Whilst the EU takes a more protective and data-subject-driven perspective, (inter alia, by including within the definition IP addresses), the Japanese standpoint is more restrictive in the delineation of the contours of such definition, thus creating a potential gap. The result could be that Japanese businesses targeting EU data subjects will have to abide to data protection laws for processes that are normally excluded by such compliance in their country.
- **Information rights** result to be more articulated in the EU framework, entailing much more options for data subjects to control their personal data. For this reason, Japanese controllers would have to put in place processes to permit a number of actions (see portability for instance), which in contrast are not mandatory in the Japanese framework.

This project has received funding from the European Union H2020 Programme under grant agreement No 740507

- The **sanctionatory regime** is significantly higher in the European legislation than the one in Japan. Therefore, assessment of the advantages in entering the other region's market would definitely result more advantageous for Europeans offering services in Japan than vice versa, as far as the mere evaluation of the risk of being fined is concerned. However, the Japanese law entails some aspects of criminal liability (with prison penalties in some residual cases of privacy violations), which are not present in European law.
- With regard to **cybersecurity**, it is still too soon to provide an assessment. The draft Cyber Security Act is expected to provide substantial improvement to the current European legal framework on cybersecurity, which is currently solely constituted by the NIS Directive. However, one of the major differences observed in the comparison of the two frameworks is the fact that Japan actively addresses the conduct of the citizens with respect to cybersecurity. Such *duty of care*, lifts the burden of protecting information systems that in Europe merely stands on producers, manufacturers and other stakeholders in the supply chain. European businesses and the like will be thus conscious of such difference in their liability regime, which is potentially more advantageous in Japan.

Potential policy blockers

On a broader scale and perspective, the advent of the GDPR and the continuous reforms in terms of privacy and cybersecurity seems not to have influenced the processing of personal data solely within the territories of the European Union. Rather, its scope and impact force us to reflect on the potential effects that such a Regulation may cause on the broad global business at large.

Whilst many commentators brought forward the undoubtable benefits of the GDPR on the strengthening of the protection of personal data as a high standard for information security practices, it is worth mentioning that such requirements might become obstacles for services and businesses that operate on a much wider scale than the mere regional ones (EU or Japan, for instance).

Under such auspices, the following examples are explanatory of those businesses and practices that might be impacted by the policies implemented by the GDPR and its Japanese counterpart, APPI. The selection of such examples took into account two of the major cases on internet governance and related services with a significant jurisprudential importance for privacy and data protection in a GDPR context. The other examples can be found in the report 3.2 itself:

- **Processing of IP addresses.** As extensively analysed in the EUNITY policy analysis, from a privacy perspective, the European Union data protection framework considers IP addresses as personal information, hence falling under the legal regime disciplined by the EU privacy reform package. In a EU-Japanese collaboration perspective, this could become a potential blocker for future projects which include the collection and the processing of IP addresses of European citizens by Japanese businesses or research entities. Cybersecurity, telecommunication and market research are only three of the sectors which could be impacted by the extensive scope of the GDPR. The misalignment between Japan and the European union on the definition of personal information therefore substantiates with a great extent and magnitude in the case of IP addresses. Such a difference in legal interpretation may become a great obstacle in terms of future cooperation in the research domain, as well as in the provision of digital services and the achievement of future partnerships between the two regions.
- **National GDPR implementations.** Whilst the GDPR is a strong legal instrument which imparts automatic implementation to the EU Member States, a number of provisions in its text still needs national specification. This, alongside a number of other exceptions derogated to Member States' decision, may create legal fragmentation and uncertainty, which may constitute, particularly from the Japanese side, a blocker in the engagement of business and policy initiatives between the two regions and between Japan and EU Member States.
- **Concerns around the respect for the human the right to privacy in Japan in criminal intelligence, investigation and prosecution of terrorist case.** On a broader scale, issues with regard to the adequate standard of protection of privacy as a human right has been raised and may constitute a potential blocker for future policy collaboration between the two countries.