World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:13, No:04, 2019

Japanese and Europe Legal Frameworks on Data Protection and Cybersecurity: Asymmetries from a Comparative Perspective

Authors : S. Fantin

Abstract : This study is the result of the legal research on cybersecurity and data protection within the EUNITY (Cybersecurity and Privacy Dialogue between Europe and Japan) project, aimed at fostering the dialogue between the European Union and Japan. Based on the research undertaken therein, the author offers an outline of the main asymmetries in the laws governing such fields in the two regions. The research is a comparative analysis of the two legal frameworks, taking into account specific provisions, ratio legis and policy initiatives. Recent doctrine was taken into account, too, as well as empirical interviews with EU and Japanese stakeholders and project partners. With respect to the protection of personal data, the European Union has recently reformed its legal framework with a package which includes a regulation (General Data Protection Regulation), and a directive (Directive 680 on personal data processing in the law enforcement domain). In turn, the Japanese law under scrutiny for this study has been the Act on Protection of Personal Information. Based on a comparative analysis, some asymmetries arise. The main ones refer to the definition of personal information and the scope of the two frameworks. Furthermore, the rights of the data subjects are differently articulated in the two regions, while the nature of sanctions take two opposite approaches. Regarding the cybersecurity framework, the situation looks similarly misaligned. Japan's main text of reference is the Basic Cybersecurity Act, while the European Union has a more fragmented legal structure (to name a few, Network and Information Security Directive, Critical Infrastructure Directive and Directive on the Attacks at Information Systems). On an relevant note, unlike a more industry-oriented European approach, the concept of cyber hygiene seems to be neatly embedded in the Japanese legal framework, with a number of provisions that alleviate operators' liability by turning such a burden into a set of recommendations to be primarily observed by citizens. With respect to the reasons to fill such normative gaps, these are mostly grounded on three basis. Firstly, the cross-border nature of cybercrime brings to consider both magnitude of the issue and its regulatory stance globally. Secondly, empirical findings from the EUNITY project showed how recent data breaches and cyber-attacks had shared implications between Europe and Japan. Thirdly, the geopolitical context is currently going through the direction of bringing the two regions to significant agreements from a trade standpoint, but also from a data protection perspective (with an imminent signature by both parts of a so-called 'Adequacy Decision'). The research conducted in this study reveals two asymmetric legal frameworks on cyber security and data protection. With a view to the future challenges presented by the strengthening of the collaboration between the two regions and the trans-national fashion of cybercrime, it is urged that solutions are found to fill in such gaps, in order to allow European Union and Japan to wisely increment their partnership.

Keywords : cybersecurity, data protection, European Union, Japan
Conference Title : ICCCIS 2019 : International Conference on Cyber Crime and Information Security
Conference Location : Tokyo, Japan
Conference Dates : April 22-23, 2019