ISSN 2704-6419

# Twinning Europe and Asia in Cyberspace

## (the EU Legislation, ASEAN and its transformative power)

Prof. Melda Kamil Ariadno & Prof. Anis H. Bajrektarević

International Institute for Global Analyses

Vision & Global Trends. International Institute for Global Analyses
Piazza dei Navigatori 22, 00147 – Rome (Italy)
Analytical Dossier – N. 2/2019 – January 2019



First Edition: January 2019

Analytical Dossier – N. 2/2019

www.vision-gt.eu

*While our troposphere is dangerously polluted, one other space – that of intangible world, created by the interconnected technology – follows the same pattern: a cyberspace. Additionally, our cyberspace becomes increasingly brutalised by its rapid monetisation and weaponisation. It mainly occurs through privacy erosion. How to protect effectively individuals and their fundamental human rights, and how to exercise a right for dignity and privacy?*

*The EU now offers a model legislation to its Member States, and by its spill-over power to the similar supranational projects elsewhere (particularly ASEAN, but also the AU, OAS, SCO, SAARC, LAS, etc.), and the rest of world.*

**********

Rules and regulations to protect personal data do not trigger many sympathies. The corporate world sees it as an unnecessary deterrent; as a limit to their growth – more to pay and less or slower to yield, innovate and expand. Governments would traditionally wish the rules should apply to every societal stakeholder but themselves. And citizenry by large too frequently behave benevolent, nearly careless whether their data is harvested or safeguarded at all.

However, such legislation is needed today more than ever before. The latest round of technological advancements was rapid, global and uneven. No wonder that in the aftermath of the so-called IT-revolutions, our world suffers from technological asymmetries: assertive big corporations and omnipresent mighty governments on one side and ordinary citizenry on the other. Even in the most advanced democracies today – such as the EU, personal autonomy is at the huge risk: Everyday simple, almost trivial, choices such as what to read, which road to take, what to wear, eat, watch or listen are governed (or at least filtered) by algorithms that run deep under the surface of software and devices. Algoritmisation of 'will' is so corrosive and deep that users are mostly unaware of the magnitude to which daily data processing rules over their passions, drives and choices.

Clearly, technology of today serves not only a Weberian predictability imperative – to further rationalise society. It makes society less safe and its individuals less free.

Societies are yet to wake up to this (inconvenient) truth. In the internet age of mobile, global and instant communications, people tend to focus more on the 'here-us-now' trends: goods, services, and experiences that the IT offers. Individuals are less interested on the ways in which privacy is compromised by software, its originators and devices – all which became an unnoticed but indispensable part of modern life. Despite a wish of many to grasp and know how data processing and harvesting affects them, population at large yet has no appetite for details.

But, the trend is here to stay – a steady erosion of privacy: bigger quantities of data are harvested about larger number of persons on a daily, if not hourly basis. Corporations and the central state authorities want more data and are less shy in how they obtain and use it.

Prevention of the personal information misuse (PIM) —intended or not—is the main reason the European Union (EU) introduced the new set of provisions, as of May 2018. Hence, the General Data Protection Regulation (GDPR) – as the legislation is known – is an ambitious attempt to further regulate digital technology, especially in respect to the private data protection. It is of course in conformity with provisions of both the Universal and European Charter of Human Rights, which hold the protection of human dignity and privacy as an indispensable, fundamental human right.

The intention of legislator behind the GDPR is twofold: to regulate domestically as well as to inspire and galvanise internationally. The GDPR is meant to open a new chapter in the Internet's history at home, while creating, at the same time, a roadmap for other state and corporate sector actors beyond the EU. The challenge is clear: to reconcile the rights of individuals to data protection with the legitimate interests of business and government.

For the rest of the world, the GDPR should be predictive, inspirational and eventually obligational. Lack of acting now could open a space for the abuse of power – be it for illegitimate corporate or authoritarian gains of the hidden societal actors. In such a negative scenario – on a long run – losers are all. Historically, victimisation of individuals (through constant suspension of liberties and freedoms) ends up in a state or corporate fascism, and that one in a self-destruction of society as whole.

## COMPREHENSIVE LEGISLATION AS POWERFUL DETERRENT

The Internet age exposes individuals in an unprecedented way to the domestic or foreign predatory forces. Everybody is tempted to participate in digital economy or digital social interaction. This cannot go without revealing personal information to large state or non-state entities of local or international workings. If the field is not regulated, the moment such information leaves its proprietor, it can be easily and cheaply stored, analysed, further disseminated and shared without any knowledge or consent of it originator.

So far, neither market forces nor the negative publicity has seriously hindered companies and governments from tapping on and abusing this immense power. Nothing but a bold and comprehensive legislation is efficient deterrent, which stops the worst misuse. Only the legal provisions to protect personal data may serve a purpose of special and general prevention:
Be it in case a local or transnational corporate greed, governmental negligent or malicious official, or the clandestine interaction of the two (such as unauthorised access to personal phone and Internet records, as well as the unverified or inaccurate health and related data used to deny person from its insurance, loan, or work).

While totally absent elsewhere, early European attempts to legislate a comprehensive regulatory system of personal data protection have tired its best. Still, the EU's Data Protection Directive of 1995 was falling short on several deliverables. (It was partly due to early stage of internet development, when the future significance of cyberspace was impossible to fully grasp and anticipate). Hence, this instrument failed to comprehensively identify the wrongdoings it sought to prevent, pre-empt and mitigate. The 1995 text also suffered from a lack of (logical and legal) consistency when it came to directing and instructing the individual EU member states (EU MS) on how to domesticate data privacy and promulgate it the body of their respective national legislation. Finally, the GDPR solves both of these problems.

This instrument of 2018 clearly stipulates on discrimination combating (including the politically or religiously motived hate-contents), authentication-related identity theft, fraud, financial crime, reputational harm (social networks mobbing, harassments and intimidation). Moreover, the European Commission (EC) has stated that the GDPR will strengthen the MS economies by recovering people's trust in the security and sincerity of digital commerce, which has suffered lately of a numerous high-profile data breaches and infringements.

However, the most important feature (and a legal impact) of the GDPR is its power of being a ***direct effect*** law. This means that individuals can invoke it before the MS courts without any

reference to the positive national legislation. That guaranties both speed and integrity to this supranational instrument – no *vocatio legis* and no unnecessary domestication of the instrument through national constituencies. Conclusively, the 2018 instrument is further strengthened by an ***extra-territorial reach*** – a notion that make is applicable to any entity that operates in the EU, even if entity is not physically situated in the EU.
This practically means that each entity, in every sector and of every size, which processes personal data of the EU citizens, must comply with the GDPR. It obliges governments and their services (of national or sub-national levels); health, insurance and bank institutes; variety of Internet and mobile telephony service providers; media outlets and other social data gathering enterprises; labour, educational and recreational entities – in short, any subject that collects digital information about individuals.

The GDPR further strengthens accountability principle. The state and commercial actors hold direct and objective responsibility for a personal data collecting, storing and processing (including its drain or dissemination). Clearly, this EU instrument strengthens the right for information privacy (as a part of elementary human right – right to privacy) by protecting individuals from misappropriation of their personal data for a harvesting, monetisation or (socio-political) weaponisation purpose.

Namely, the GDPR gives individuals the right to request a transfer of their personal data (account and history information) from one commercial entity to another (e.g. from one bank or phone provider to another). Another right is to request – at short notice and for an unspecified reason – the commercial enterprise to stop both the data collection and the marketing dissemination, or to demand clarification on a marketing methods and nature of services provided. This instrument also offers individuals the right to request that their personal data are deleted (being zipped and sent back to its proprietor beforehand) – as stipulated in art.17 (the right to be forgotten).

The GDPR calls upon all operating entities to hire a data protection officer as to ensure full compliance with the new rules. It also invites all data collecting entities to conduct impact assessments – in order to determine scope frequency, outreach and consequences of personal data harvesting and processing. (For example, if certain entity wished to introduce biometric authentication for its employees and visitors entering daily its premises, it would need at first to run an assessment – a study that answers on the necessity and impact of that new system as well as the exposures it creates and possible risk mitigation measures.)

The GDPR obliges every entity that gathers data to minimise amount and configuration of personal data they harvest, while maximizing the security of that data. (For instance, if the auto dealer or travel agency requires potential customers to fill out the form to request a price quote, the form can ask only for information relevant to the product or services in question.)

The new legislation also mandates data gathering entities to notify the authorities – without any delay – whenever they suspect or witness a personal data breach. Conclusively, the GDPR obliges entities to present the public with clean and through information about the personal data they harvest and process—and clearly why they do so.

On the sanction side, the GDPR supports the regulators with new enforcement tools, including the norm setting, monitoring of and enforcement of compliance. For a non-compliance, the instrument prescribes steep fines.

To answer adequately the accountability standards enacted by this EU legislation will certainly invite large data gathering entities to bear significant investments. However, for the sake of credibility outreach and efficiency, they will have stimuli to introduce the new procedures and

systems within the EU, but also beyond – wherever their operations are present. Complementary to it, the GDPR stipulates that if an entity transfers personal data out of the EU, it must safeguard that the data is handled in the new location the same way like within the EU. By this simple but far-reaching and effective spill over notion, the standards embodied by the GDPR will be delivered to the rest of the world. Hence, this instrument is not (only) an inner code of conduct that brings an outer appeal; it is a self-evolving and self-replicating standard of behaviour for our common (digital) future.

## ASEAN, INDO-PACIFIC, ASIA

It is obvious that the stipulations of the GDPR would serve well interests of Republic of Indonesia (RI). That is actually in line with a very spirit of the 1945 Constitution, which obliges the state to protect, educate and prosper the Indonesian people. This supreme state act clearly proclaims that the respecting individual personal data is resting upon the two principles of the Pancasila. Namely these of; Fair and Civilized Humanity. Mutual grant and observance of everyone's elementary rights is an essence of freedom and overall advancement of society.

The government, with the mandate of its authority to protect the public (public trust doctrine), must manage the personal data fairly and accountably. The GDPR also encourages the formation of an independent personal data protection supervisory institution so that it can correct the policies and rules of the bureaucracy and state administration to act accordingly in managing the personal data of the population. Moreover, every democratic government should be more proactive in protecting society when comes to the management of the personal data of its residents.

Interestingly, the Indonesian legislation already has instruments that follow notion of the GDPR. Thus, the Law No. 11 on Information and Electronic Transactions of 2008 (by a letter of its article 2) emphasizes the principle of extra-territorial jurisdiction. (In this particular case, it is related to the cross-border transactions. Indonesia should always safeguard its national interests: the RI jurisdiction stretches on any legal action that apply in Indonesia and/or carried out by Indonesian citizens. But it also applies to legal actions carried out outside of Indonesian jurisdiction by Indonesian citizens or a foreigner legally residing in RI, or Indonesian legal entities and foreign legal entities that produce legal effects in Indonesia.

This of course assumes the very nature of a use of Information Technology for Electronic Information and Electronic Transactions, which can be cross-territorial and even universal. What is assumed by this Law as "harming the interests of Indonesia" goers beyond pure national economic interests, protecting strategic data, national dignity, defense and security, the state of sovereignty, citizens, and Indonesian legal entities.)

When comes to the Right to be Forgotten (Right for Privacy and Right for Dignity), Indonesia must see it as a principle of real protection that is in the best interests of data owners. Further on, such a right should be strengthened by the principle of 'without undue delay', as to avoid the administrative obligation to request a court decision to uphold the right. On a long run, it will surely benefit businesses far more than the personal data originators themselves.

## LEADING BY EXAMPLE

In line with the Right to Portability Data elaborated by the GDPR, Indonesia also needs to closer examine the EU instruments. Hence, the EU Regulation No.910 / 2014 concerning electronic identification, authentication and trust services (eIDAS) offers an idea how to harmonize the provision of digital identity and personal data in realm of electronic communications. (Electronic identification and authentication is a technology process that has an economic value. Such a business opportunity should be reconciled with a safety and security standards when comes to use of and traffic with of personal data for commercial interests.)

Regarding security, Indonesia must immediately have a clear policy on Cryptography to protect personal data. Cryptography is a double-use process; it can be utilised for civilian purposes, but it can also be used for the vital national interests, such as defense and security. Therefore, privacy and cybersecurity protection is a complementary concept of protection. Holistic approach strengthens the both rights of individuals as well as protection of national interests, rather than it ever conflicts one over the other.

Finally, the ASEAN Declaration of Human Rights in its article 21 stipulates that the protection of personal data is elementary part of Privacy. As one of the founding members, a country that even hosts the Organisation's HQ, Indonesia must observe the notions of this Human Rights Charter. That is the additional reason why RI has to lead by example.

The EU's GDPR clearly encourages a paradigm shift within the public services and government administration services on national, subnational and supranational level for all the ASEAN member states. It is to respect the fundamental freedoms and liberties, a quality that will shield population from random and ill-motivated arbitrary judgments of individual rights under the pretext of public interest.

Indonesia and ASEAN can take a lot of learning from the dynamics of the EU's regulation of GDPR and e-IDAS as to its own benefit – to foster its own security and to elevate a trust in regional e-commerce within the ASEAN economic zone. Since the ASEAN (if combined) is the 4$^{th}$ largest world economy, this is a call of future that already starts now. After all the EU and ASEAN – each from its side of Eurasia – are twin grand projects of necessity, passion and vision.

Naturally, for anyone outside, Indonesia and ASEAN are already seen as the world's e-commerce hub, of pivotal importance far beyond the Asia-Pacific theatre.

***Vienna/Jakarta 28 DEC 2018***

## About the authors:

Prof. Melda Kamil Ariadno (SH, LLM, PhD) is a Professor of International Law at the Faculty of Law Universitas Indonesia, Jakarta. She is currently the Dean of the Faculty of Law Universitas Indonesia and the Head of Center for Sustainable Ocean Policy. She obtained her bachelor's degree from Universitas Indonesia in 1992. Then, she received both her LL.M. and Ph.D. from the University of Washington in 1995 and 2011, respectively.

She has served as legal expert for several governmental bodies among others the Ministry of Marine Affairs and Fisheries.


**Prof. Anis H Bajrektarevic** is chairperson and professor in international law and global political studies, Vienna, Austria. He has authored six books (for American and European publishers) and numerous articles on, mainly, geopolitics energy and technology. For the past decades, he has over 1,200 hours of teaching on the subject International Law. Two of his books are related to cyber space, cyber law and cyber wrongdoings.

Professor is editor of the NY-based GHIR (Geopolitics, History and Intl. Relations) journal,
and editorial board member of several similar specialized magazines on three continents.
His 7th book is to be realised in New York in December.