Foreword

Věra Jourová, European Commissioner for Justice, Consumers and Gender Equality

When the European Community adopted its first data protection directive in 1995, the Internet was in its infancy. The personal data that legislators had in mind was in paper filing systems or static electronic databases of public institutions like ministries, hospitals and schools or private companies.

More than 20 years later, the scale and means of data processing have undergone a technological revolution: the Internet and cloud computing allow for easier transfer and use of data, including personal data, across the globe. It is in this context that Europe equipped itself with a new General Data Protection Regulation, which will enter into application in May 2018.

The EU’s new data protection rules update existing concepts, harmonize their application across the Member States, and provide for stronger enforcement including through financial sanctions for non-compliance. The revised rules aim to strengthen individual rights in a digital age, while creating a level playing field for companies in Europe’s Digital Single Market.

One of the novelties of the General Data Protection Regulation is that it will explicitly apply also to companies based outside the EU if their data processing activities relate to the offering of goods or services or the monitoring of behaviour in the EU. Moreover, important safeguards will continue to apply for transfers of personal data from the EU to other parts of the world; the aim being that the protection must “travel with the data”.

The right to protection of personal data is enshrined as a fundamental right in the EU. However, it is not unique to Europe. More and more countries around the world are adopting legislation on the protection of personal data, in order to both protect their citizens and equip their economies for digital transformation.

At this juncture, the work of Radim Polčák and Dan Svantesson provides very timely insights into the relationship between data protection and privacy law with key principles of international law, both public
and private. Polčák and Svantesson explore the origins and nature of data protection law (and how it relates to the broader notion of privacy), explore the notion and meaning(s) of jurisdiction, and point to the inherent challenges in cross-border enforcement of laws, including data protection laws.

On the topical question of privacy versus security, Polčák and Svantesson dispel the idea of a simplistic trade-off between the two, given the increasing interlinkage between the right to privacy and the need for security (e.g. data security, security for cyberattacks). Moreover they point out that protecting one person’s privacy (e.g. from cyberstalking) may require interference in the privacy of another.

Above all, Polčák and Svantesson remind us that it is not the personal data as such that deserves protection, but the individuals to whom it pertains, and whose human dignity must not be endangered. (Indeed, the full title of the EU’s data protection law refers to ‘the protection of natural persons with regard to the processing of personal data’.)

This is more than a question of semantics, as shown by situations where the mass processing of relatively trivial pieces of personal information can result in serious interference with individuals’ lives, whether it is influencing their credit rating or their democratic choices. Polčák and Svantesson call it the ‘risk associated with extensive presence and availability of informational footprints’.

Tackling these risks will require individual awareness and responsibility, but also the courage of politicians to weigh the benefits of technological changes against the threats and ethical dilemmas they bring.

As Europe proceeds with implementing the General Data Protection Regulation, EU policymakers are turning their attention to another complex issue: the (cross-border) access to electronic evidence for criminal investigation and prosecution. Prosecutors in EU Member States increasingly rely on evidence stored in cloud servers abroad even to prosecute entirely ‘domestic’ crimes (committed in the same country by and against residents of that country) without any cross-border component. While judicial cooperation between EU Member States is becoming more efficient and routine, access to electronic evidence raises new questions about jurisdiction and territoriality in cyberspace.

Again, Radim Polčák and Dan Svantesson make a very timely contribution to this debate, by exploring relevant concepts of international law and how they link to national criminal procedure laws. In doing so, they provide crucial academic groundwork for one of the key policy challenges facing Europe’s justice ministers today.