Capik A.
M.A.S. (European Integration),
Executive M.B.L.-HSG
External Lecturer in European Law

PUBLIC PRESENCE WITHIN PRIVATE SPHERE – PROTECTION OF FUNDAMENTAL RIGHTS IN THE INFORMATION SOCIETY

A right to protection of an individual's private sphere against intrusion from others,especially from the state, was laid down in an international legal instrument for thefirst time in the provisions of Article 12 of the United Nations (UN) Universal Declaration of HumanRights (UDHR) of 1948 on respect for private and family life.No need to say that the UDHR considerably influencedthe further development of other fundamental rights instruments in Europe, which gradually took place over past decades [5, 14].Technological progress and globalization, however, have profoundly changed the scope of fundamental rights of individuals, in particular by the way private data is nowadays collected, accessed and used. Safeguarding these fundamental rights in today's information society is, therefore, has increasingly become a key issue for the EU as more and more individuals use information and communications technologies (ICT) in their daily lives both professional and private [7, 3].

Inevitably, this growing use of ICT creates fundamental rights challenges, particular with regard to potential misuse of personal data electronically processed online. Consequently, everyone nowadays may, at some point, face violations of their fundamental rights, particularly such as right to privacy. Having said this, it does not wonder that public bodies at both European and domestic level are more and more concerned in drawing attention to this phenomenon in their legislative activities, while taking an approach that, despite the specific challenges posed by the increasing use of digital technologies, it is essential to ensure that fundamental rights are promoted and protected online in the same way and to the same extent as in the offline world [7].The Cybersecurity Strategy of the EU has underlined the impact of ICTs – and in particular the Internet – stating that "[*o*]*ur daily life, fundamental rights, social interactions and economies depend on information and communication technology working seamlessly*. (…) *Fundamental rights, democracy and the rule of law need to be protected in cyberspace.*" Furthermore, in the Code of EU Online Rights, the European Commission has underlined that "*the fundamental rights and freedoms of natural persons as guaranteed by the Charter of Fundamental Rights of the European Union, the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the general principles of EU Law shall be respected in this context*."[7, 1].

Considering the foregoing, the aim of this piece at hand is to provide an overview of several legislative steps recently taken at the European level with regard to data protection on the one hand and asses their potential impact on the other.

In this new digital environment, individuals have the right to enjoy effective control over their personal information[Data protection is a fundamental right in Europe, enshrined in the provisions of Article 8 of the Charter of Fundamental Rights of the European Union (CFR), as well as of Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), and needs to be protected accordingly.The EU CFR provides that everyone has the right to personal data protection in all aspects of life: at home, at work, whilst shopping, when receiving medical treatment, at a police station or on the Internet. Broadly speaking, Personal data constitutes any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.The right to protection of personal data forms moreover part of the rights protected under Article 8 of the ECHR, which guarantees the right to respect for private and family life, home and correspondence and lays down the conditions under which restrictions of this right are permitted.This gave the European legislator new responsibilities to protect personal data in all areas of EU law, including police and judicial cooperation, although, notably, the legislation on data protection has been in place since 1995(i.e. Data Protection Directive (95/46/EC).

Considering the foregoing, it should be underlined that EU data protection rules aim in general to protect the fundamental rights and freedoms of natural persons, and in particular the right to data protection, as well as the free flow of data. Since the earlier existing rules provided neither the degree of harmonization required, nor the necessary efficiency to ensure the right to personal data protection, the European Commission took an initiative in proposing a fundamental reform of the European data protection framework late 2010, setting out a strategy to strengthen EU data protection rules, whereas the main goals were to protect individuals' data in all policy areas, including law enforcement, and guaranteeing the free circulation of data within the EU [2, 141-147]. The reform ended up in two legal instruments, namely (a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and (b) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, both adopted 2016. While the GDPR will enter into force on 24 May 2016, it shall apply from 25 May 2018. The Directive enters into force on 5 May 2016 and EU Member States have to transpose it into their national law by 6 May 2018.

With regard to the regulatory scope and application,these two legal instruments set out relatively comprehensive framework governing data protection at the European level. The GDPR constitutes undoubtedly an essential step to strengthen (“digital”) fundamental rights of individuals, while at the same time facilitating business by simplifying rules for companies within the Digital Single Market. It enablesindividuals to better control their personal data, while at the same time it modernizes and unifies rules allowing businesses to make the most of the opportunities of the Digital Single Market by benefiting from reinforced

consumer trust.The Directive for the police and criminal justice sector protects individuals' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities. It aims at ensuring that the data of victims, witnesses, and suspects of crimes, are duly protected in the context of a criminal investigation or a law enforcement action. It should be underlined that more harmonized laws will also facilitate cross-border cooperation of police or prosecutors to combat crime and terrorism more effectively across Europe, the latter obviously calling for price under actual (geo)political circumstances.

It is argued that, in general, the new set of rules address strengthening the existing rights and empowering individuals with more control over their personal data, including in particular (a) easier access to own data, while providing in clear and understandable way more information on how the data is processed; (b) a right to "data portability", simplifying transfer of personal data between service providers and providing that the copy of the data electronically processed can be obtained in a commonly used interoperable electronic format; (c) clarified "right to be forgotten", provided that whenever there are no legitimate grounds for retaining it, the data will be deleted, upon request; (d) the right to be informed without undue delay of a personal data breach [4, 65-66].

While awaiting the entry into force of the legal instruments mentioned above, some considerations can be, nonetheless, put forward towards a potential impact of the new regulatory framework within the field of data protection at the European level. Firstly, regarding the question of protecting personal data within the area of law enforcement, it is argued that a better cooperation between law enforcement authorities is enshrined. It should be particularly underlined that the law enforcement authoritiesat the domestic level of EU Member States will be able to exchange information necessary for investigations more efficiently and effectively, improving cooperation in the fight against terrorism and other serious crime across Europe. Additionally, the new Directive takes furthermore into account the specific needs of law enforcement, respecting especially the different legal traditions in Member States on the one hand, and is fully in line with the provisions of the CFR, constituting primary law source of the European legal order on the other hand. Secondly, significantly improved protection of individuals' data should be noted. Individuals' personal data will be better protected, whenprocessed for any law enforcement purpose including prevention of crime. The new set of rules protects everyone – regardless of whether they are a victim, criminal or witness. Noteworthy, all law enforcement processing in the European Union must comply with the principles of necessity, proportionality and legality, with appropriate safeguards for the individuals. Furthermore, supervision is ensured by independent national data protection authorities, and effective judicial remedies must be provided.All in all, this new framework within data protection field provides clear rules for the transfer of personal data by law enforcement authorities outside the EU, to ensure that the level of protection of individuals guaranteed in the EU is not undermined [4, 65-66].

Certainly, it remains today an open question as to whether the future application of this framework by and among all the Member States will prove equally positive as the rules itself. The ball, however, is much more at the domestic level, therefore, the future practice depends mostly on ability of national authorities not only to legislate but first and foremost to comprehensively cooperate within domestic legal systems across the EU. More important in the given context appears, nevertheless, exactly what has given a rise to legal considerations on

privacy protection nearly 70 years ago, namely the interference of public bodies into a (individual) private sphere. Consequently, one may, thus, ask whether we are indeed moving forward or switching from a real to a virtual world only, without properly balancing the two – concurring with and complementing each other at the same time–legal realities, whereasthe constructive development of the 'right to be forgotten', as protected already by the jurisprudence of the Court of Justice of the European Union should not constitute solely wishful thinking.

LITERATURE AND SOURCES:

1. Ian Brown, The challenges to European data protection laws and principles, Oxford 2010
2. Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer 2014
3. VasilikiKosta, Fundamental Rights in EU Internal Market Legislation
4. OrlaLynskey, The Foundations of EU Data Protection Law, OUP 2015
5. SPECIAL EUROBAROMETER 359 - Attitudes on Data Protection and Electronic Identity in the European Union,
6. European Union's Agency for Fundamental, Handbook on European data protection law, Luxembourg 2014
7. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
8. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
9. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 2012/0011 (COD)
10. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)