JUDICIAL TRAINING ON DATA PROTECTION AND PRIVACY RIGHTS

On-line Classroom, 23 April 2021

Processing of Personal Data and protection of Privacy in the Electronic Communication Sector

Spyridoula Karyda,
Judge at the Council of State,Greece
PhD researcher, Cyber and Data Security Lab, Faculty of Law and Criminology,
Vrije Universiteit Brussel (VUB)

[AD/2021/03]

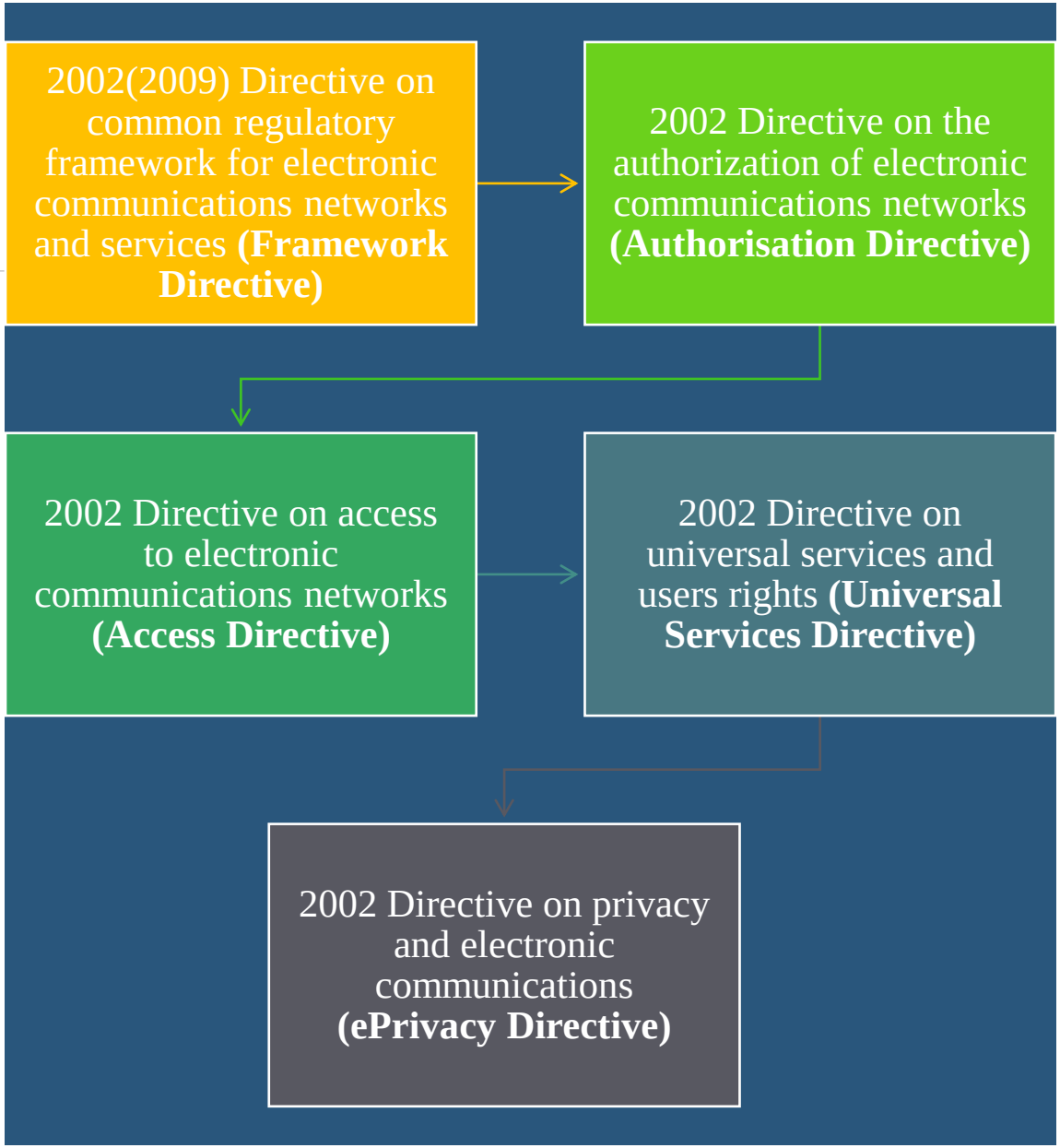
ejtn refj

With financial support from the Justice Programme of the European Union

Content

- I.Electronic Communications Regulatory Framework: Composition
- II.The difference between privacy and the right of personal data
- III.The ePrivacy Directive
- IV.GPS
- V.Covid-19 and Location Data
- VI.Draft Act:ePrivacy Regulation
- Conclusion

EU Telecoms Package



EU Telecoms package

- Not fully harmonisation
- Subject of regulation:telecommunication networks and services for remuneration (not media and not internet)
- Key objectives
- Creation of a competitive environment for the electronic communications sector, abolition of national monopolies
- Development of infrastructure
- Protection of consumers/users
- Improvement of coordination between NRAs and EU

New European Electronic Communications Code(EECC)

- Directive (EU) 2018/1972
- Entered into force on 20 December 2018
- Aims to:
- promote connectivity, access to and take-up of very high capacity networks by all citizens and businesses of the Union
- promote competition in the provision of electronic communication networks and services
- contribute to the development of the internal market in the field of electronic communications networks and services, radio spectrum, and connectivity
- BEREC as a key player of the EECC

European Electronic Communications Code (EECC)

Key points: A broader definition of ECS including the so-called “over-the-top” (OTT) services

The category of ECS now includes:

(1) internet access services,

(2) interpersonal communications services (‘ICS’), and

(3) services consisting wholly or mainly in the conveyance of signals

EECC

EECC underlines citizen connectivity as a key objective of the EU. The idea behind this is that connectivity is important in order to guarantee freedom of expression, pluralism, democracy, culture, social cohesion, and even safety

A significant development in EU law

ICS themselves are divided into

‘number-based interpersonal communications services’ and (i.e. Skype)

‘number-independent interpersonal communications services’(i.e.WhatsApp)

Voice over Internet Protocol (VoIP) and chat services such as Whatsapp, Facebook Messenger, or Skype are now fall under the definition of ICS, and hence, under the definition of ECS

EECC

To promote the interests of European citizens

Security, protection and accessibility of end-users with special needs because of their disabilities or age are amongst the objectives stated

It will pave the way to the next generations of networks-5G

How?

Brings together the rules on electronic communications networks and services and aligns them to the recent technological developments in the field

EECC

Regulates

electronic communications networks and services (“ECN” and “ECS”),

associated facilities and services,

authorisation of networks and services,

radio spectrum use and numbering resources,

access to and interconnection of electronic communications networks and associated facilities, and

the protection of end-users

The difference between privacy and the right of personal data

Article:Judges Samouel Warren and Louis Brandeis, 'The right to Privacy',Harvard Law Review (1890)

Illustrates the essence of privacy as of *'the right to be alone'*

Privacy: a fundamental human right and the very basis of human dignity and values

UN Legal Framework

Article 12 of Universal Declaration of Human Rights (UDHR)

- The right to privacy one of the fundamental protected human rights
- Non-binding declaration
- The term 'privacy' under the 'umbrella term'

International Covenant on Civil and Political Rights (ICCPR)

- **Article 17 of the ICCPR legal instrument to introduce rules on data protection law**
- Article 17 ICCPR does not provide detailed guidance with regard to data protection legal framework / lack of specific legal tools in order to ensure data protection in practice

The UN Resolutions on the right to privacy in the digital age

- They strongly condemn mass surveillance and highlight the impact such surveillance can have on the fundamental rights to privacy and freedom of expression, and on the functioning of a vibrant and democratic society
- Non-binding declaration

The right to respect for private life and the right to personal data protection

The EU response

The right to data protection as a fundamental human right

CoE: ECHR Article 8 *'Everyone has the right to respect for his private and family life, his home and his correspondence'/ Convention 108*

EU Primary Law

Article 16 TFEU /Article 7 and 8 Charter

EU Secondary Law

GDPR/ Regulation for EU Bodies

LED (2016/680)

ePrivacy Directive/ ePrivacy Regulation

Distinct rights?

Privacy: a static, negative protection

Data protection: modern and active right which puts in place a control and weighting system to protect individuals when processing personal data relating to them

The right to ‘informational self-determination’ (*informationelle Selbstbestimmung)*

Landmark BVerfG ‘Cencus Decision’ (‘*Volkszählungsurteil’)*

Distinct rights?

Different historic origins

divergent obligations

serve mismatched scopes

Right to respect private life creates a negative gesture, thus ‘nothing to do’ and so consists of a general prohibition of interference, subject to some public interest criteria

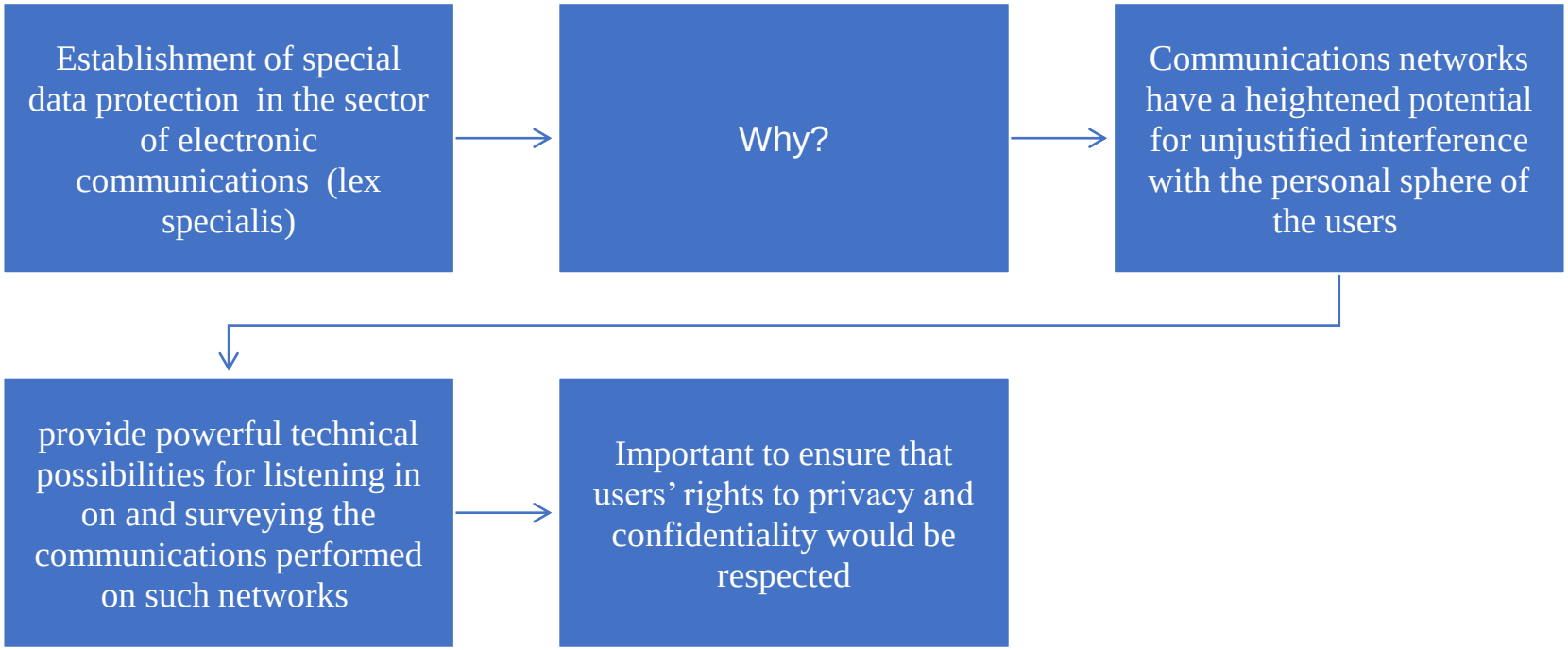
Distinct rights?

Data protection has an essential procedural nature

Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR and Hartmut Eifert : AG Sharpston in her Opinion distinguished between the two rights suggesting that privacy is a ‘classic right’ protected under Article 8 ECHR and data protection is a ‘modern right’ protected by the provisions of the Convention 108

ePrivacy Directive

Directive on privacy and electronic communications



Scope of the ePrivacy Directive

(Art.1)

Harmonisation of the national provisions

Ensure an equivalent level of protection of fundamental rights and freedoms

In particular the right to privacy and confidentiality of communications enshrined in Art.7 of the Charter and the right to personal data protection enshrined in Art.8 of the Charter

Where?

In the electronic communication sector

Applicable to subscribers natural and legal persons

Aims to ‘particularise and complement’ the provisions of GDPR

Specific exemptions: national/public security,Law Enforcement Activities

ePrivacy in a nutshell

Sets out rules on the:

- security of personal data in electronic communications networks (Art.4)
- notification of personal data breaches (Art.4)
- confidentiality of communications (Art.5)
- bans unsolicited communications (often referred to as ‘spam’), unless the users have given their consent (Art.13), and
- contains rules on the storage of ‘cookies’ on computers and devices (Art.5.3)

Key Point

The application of ePrivacy Directive is limited to communication services in public electronic networks

General Material scope of the ePrivacy Directive

(Art.3)

ePrivacy Directive applies

Electronic communications services (ECS) as defined by Art. 2(4) of the EECC including OTT services

When?

The service is offered over an electronic communication network

The service and network are publicly available

The service and network are offered in the EU

The extended material scope of ePrivacy Directive

Art. 5(3) and Art.13: Applicable to providers of ECS

website operators (e.g.for cookies)

other businesses (e.g. for direct marketing)

(2)Examples

Search engine services which store or access cookies on the device of a user fall within the extended material scope of article 5(3) ePrivacy Directive

Unsolicited electronic mail sent by a website operator for the purposes of direct marketing also fall within the extended material scope of article 13 ePrivacy Directive

The interplay between the ePrivacy Directive and the GDPR

- Art. 1(2) ePrivacy Directive and Art. 95 GDPR

- establishment of the lex specialis lex generalis relationship between them
- **particularise**: when ePrivacy renders more specific the rules of the GDPR, the specific provisions of the ePrivacy shall as 'lex specialis' be applicable
- example: processing of traffic data
- **complement**: ePrivacy protects both natural and legal persons
- Recital 173 of the GDPR stipulates that, in respect of the processing of personal data to which the specific obligations of the ePrivacy do not apply, the GDPR shall remain applicable

Categories of data

ePrivacy Directive as amended by the Civil Rights Directive (2009/136/EC)

provides for four (4) types of data

Art. 5 Content data (strictly confidential)/Cookies

Art. 6 Traffic data/information about the communications parties,time and duration of the communication/data relating to subscribers and users

Art.9 Location data other than traffic data/metadata/about the location of the users of the communications devices/users of mobile communication devices

Art.13 unsolicited communications

Legal bases for data processing under ePrivacy Directive

- **Content data**
- **Art. 5 (1) and (2)**
- Strictly Confidential/ except when legally authorised to do so in accordance with Article 15(1)
- May be processed, in private sector, based on:
- 1.User's consent,under the strict conditions set forth by the GDPR (art. 2f and recital 17 ePrivacy Directive)
- 2.Its storage only if it is necessary for the conveyance of a communication without prejudice to the principle of confidentiality
- 3.Recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication

Legal bases for data processing under ePrivacy Directive

- **Cookies**
- Art. 5 (3)
- User's consent, under the strict conditions set forth by the GDPR (art.2f and recital 17 of the ePrivacy Directive)
- **or**
- Criterion A:cookie is used 'for the sole purpose of carrying out the transmission of a communication over an electronic communications network'
- Criterion B:cookie is 'strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service'

C-673/17 *Planet49 GmbH* Consent and Cookies

- Facts: Planet49 organises promotional lottery in website and is using pre-ticked box to obtain the consent of users with regard to the collection of information for the purposes of advertising. Users would have to deselected the box in order to refuse consent.
- Court's judgment: consent is invalid.
- An action is required, as consent in accordance with GDPR must be unambiguous
- 'the consent referred to in Article 2(f) and in Article 5(3) of Directive 2002/58, read in conjunction with Article 4(11) and Article 6(1)(a) of Regulation 2016/679, is not validly constituted if the storage of information, or access to information already stored in the website user's terminal equipment, is permitted by way of a pre-ticked checkbox which the user must deselect to refuse his or her consent'
- Consent must be informed, notably about duration and third party access
- irrelevant if not personal data

Legal bases for data processing under ePrivacy Directive

- **Traffic data**
- Art.6
- May be processed only:
- for the purpose of subscribers billing and interconnection payments
- for the purpose of marketing electronic communications services or for the provision of value added services, as long as it is necessary for the marketing service and the user has given his or her prior consent
- Value added service:means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof

- example: Giving information in relation to the user's location about the next metro station or a store or the weather forecast for this location
- Key remark: anonymization the moment where it is no longer needed for the purpose of the transmission or communication

Legal bases for data processing under ePrivacy Directive

- **Location data**
- Art. 9
- May be processed only:
- with the user's or subscriber's consent to the extent and for the duration necessary for the provision of a value added service
- or
- made anonymous
- **Unsolicited communications**
- Art.13
- use of automated calling machines, fax or e-mail for the purposes of direct marketing
- only if subscribers or users has given their consent

Restrictions

- Art 15 of the ePrivacy Directive and Art.23 of the GDPR
- ‘Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC’ [Art.23 GDPR]
- Article 15(1) of the ePrivacy Directive allows Member States to adopt legislative measures that restrict the scope of confidentiality and data privacy rights enshrined in this Directive for the purposes of national security, public security and combatting crime

Restrictions

- Classification on how restrictions to be regarded in accordance with Articles 7,8 and 52 of the Charter
    1. ‘respect of essence of the fundamental rights and freedoms’ and to ‘the conducting each time of the necessity and proportionality test’
    2. imposed restrictions should be prescribed by law and thus foreseeable
- the power conferred on Member States may be exercised only in accordance with the requirement of proportionality, according to which derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary
- Case C-623/17 *Privacy international* [Grand Chamber,6 October 2020]
- Case C-511/18 *La Quadrature du Net and Others* [Grand Chamber, 6 October 2020]
- Case C-746/18 *H.K. v Prokuratuur* [Grand Chamber,2 March 2021]

Case C-207/16 *Ministerio Fiscal* [Grand Chamber,2 October 2018]

- Framing the principle of proportionality
- The objective pursued by national legislation governing access to personal data must

- be proportionate to the seriousness of the interference with the fundamental rights that that access entails

- Serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of combatting crime which must also be defined as 'serious'
- On the contrary, when the interference is not so serious, that access is justifiable

Data Retention Directive (2006/24/EC)

The Data Retention Directive required communication service providers to retain metadata was annulled by the CJEU

- Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland ltd and Others* [Grand Chamber, 8 April 2014]

By imposing such obligations on those providers, Directive 2006/24/EC constituted a particularly serious interference with the fundamental rights to respect for private life and the protection of personal data, guaranteed by Articles 7 and 8 of the Charter

The retention of data for possible transmission to the competent national authorities genuinely satisfied an objective of general interest, namely the fight against serious crime and, ultimately, public security.

Data Retention Directive

- However
- Court found that, by adopting the directive on data retention, the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality. Accordingly, it declared the directive invalid, on the ground that the wide-ranging and particularly serious interference with fundamental rights that it entailed was not sufficiently circumscribed to ensure that that interference was limited to what was strictly necessary
- Data Retention Directive covered, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting serious crime
- The directive did not fully ensure control by an independent authority of compliance with the requirements of protection and security, as explicitly required by the Charter

Data Retention

- Case C-203/15 *Tele2 Sverige AB v Post-och telestryrelsen and Secretary of State for the Home Department* [Grand Chamber, 21 December 2016]
- EU law precludes national legislation that prescribes general and indiscriminate retention of data
- EU law does not preclude the targeted retention of traffic and location data for the purpose of fighting serious crime provided that the retention of data is limited to what is strictly necessary

Case C-623/17 *Privacy international* [Grand Chamber,6 October 2020]

- Triggering the ‘national security’
- National legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security falls within the scope of the ePrivacy Directive
- EU law must be interpreted as precluding national legislation enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security

Case C-511/18, C-512/18 and C 520/18 *La Quadrature du Net and Others* [Grand Chamber, 6 October 2020]

- Set forth possibilities for legislative measures for the retention of data
- Safeguarding national security/ existence of a genuine or foreseeable danger
- Limited in time to strictly necessary
- Decision of retention is subject to effective review
- Set forth strict safeguards to protect the personal data

GPS (Global Positioning System) Surveillance

- Privacy and data protection in view of Article 8 ECHR
- Art. 8: a negative obligation of the ‘right to be alone’
- Art. 8 (2): interference allowed
- when?
- the exercise is in accordance with the law
- have a legitimate aim (national security, public safety, safety of the economy well being of the country , the prevention of disorder or crime or the protections of the rights and freedoms of others) and
- it is necessary in a democratic society to achieve these aims

GPS Surveillance

- ECtHR, Uzun v Germany [2010] App. no 35623/05

  Surveillance via GPS
- No violation of Article 8 of the Convention
- The GPS surveillance and the processing and use of the data thereby obtained had admittedly interfered with the applicant's right to respect for his private life
- pursued the legitimate aims of protecting national security, public safety and the rights of the victims, and of preventing crime
- Also been proportionate

GPS

- ECtHR, Ben Faiza v France [2018] App.no 31446/12
- violation of Article 8 (right to respect for private life) of the Convention as regards the real-time geolocation of the applicant's vehicle by means of a GPS device
- Why?
- not prescribed by law
- fighting serious crime necessary in a democratic society

US Supreme Court: The 'Carpenter Case'

- CSLI is more about revealing a person's physical movements
- An '*intimate window into a person's life, revealing not only his particular movements, but through them his familiar, political, professional, religious and sexual associations*'
- Comparing mobile phone tracking with GPS monitoring, US Supreme Court considered the former more intrusive
- '*as persons and phones become inseparable, the government may achieve 'near perfect surveillance' with CSLI*
- '*whoever the suspect turns out to be, he has effectively been tailed every moment of every day for years*' with only the few without mobile phones being able to escape the '*tireless and absolute surveillance*'

Use of location data: The fight against COVID -19 pandemic

- The use of data driven solutions as part of the fight against to the Covid -19 pandemic emerged the significance of location data and contacts tracing but simultaneously raised considerable thoughts with regard the compliance of those methods with the strict EU data protection legal framework
- EC and the EDPB reacted fast and launched guidelines
- processing of personal data is necessary for managing the COVID-19 pandemic, data protection is indispensable to build trust, create the conditions for social acceptability of any solution, and thereby guarantee the effectiveness of these measures
- efforts should focus of anonymized location data and not of personal data.
- consent as an acceptable legal basis (sensitive data)

Use of location data:The fight against COVID -19 pandemic

- Processing of location data is allowed when such processing is necessary for reasons of public interest in the area of public health, meeting the conditions of Article 9(2)(i) GDPR
- or
- for health care purposes as described in Article 9(2)(h) GDPR
- Depending on the legal basis, it might also be based on explicit consent (Article 9(2)(a)GDPR)
- In accordance with the initial purpose, Article 9(2)(j) GDPR also allows for health data to be processed when necessary for scientific research purposes or statistical purposes

Use of location data:The fight against COVID -19 pandemic

- Security of data
- implementation of several functional requirements such as the data minimization or State-of-the-art cryptographic techniques to secure the data stored in servers and applications, exchanges between applications and the remote server
- Mutual authentication between the application and the server must also be performed.
- Controller: national health authorities (or entities carrying out tasks in the public interest in the field of health) given the sensitivity of the personal data at hand
- individuals remain in control of their data
- Commission further insisted that a common approach should be adopted on behalf of all EU Member States.

ePrivacy Regulation

- Commission, 'Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' (Proposal) COM/2017/10 final
- The regulation will adapt the previous ePrivacy Directive provisions to new technologies and market reality and build a comprehensive and consistent framework with the GDPR
- On February 2021 the Council of EU reached an agreement on the ePrivacy Regulation

ePrivacy Regulation

- Key points
- Broad scope of application, including OTTs
- Extraterritorial effect
- Cookies: regulates the storage and collection of information in and user's terminal equipment (PC, smartphone, laptop)
- Consent standard: the high standard of GDPR, applicable to legal persons

ePrivacy Regulation

- Alignment with the GDPR sanctions
- Art.23 Draft ePrivacy Regulation: Article 83 of the GDPR shall apply ***mutatis mutandis*** to infringements of this Regulation
- National Security Activities
- Art. 2 (2) (a) Draft ePrivacy Regulation 'This Regulation does not apply to**:**
- (a) activities, which fall outside the scope of Union law, and in any event measures, **processing activities and operations** concerning national security and defence, regardless of who is carrying out those activities **whether it is a public authority or a private operator acting at the request of a public authority**'

Conclusion

Privacy: *ultimum refugium*

High sophisticated driven technology gives rise to powerful tools that may be served for good and evil

What ever elements we choose to integrate in the notion of ‘privacy’

we need to feel that our private life is well-protected and in this respect as author Anthony Burgess quote:

‘To be left alone is the most precious thing one can ask of the modern world’

Thank you!

With financial support from the Justice Programme of the European Union