Alessandro Palmieri

The fundamental right to privacy and the challenges of the platform economy

*

* Flensburg – 28-29 May 2019

The Law of Everything ?

Personal data

any information relating to an identified or identifiable natural person ('data subject')

The law of everything. Broad concept of personal data and future of EU data protection law

Nadezhda Purtova

Associate Professor, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, The Netherlands, P.O. Box 90153. 5000 LE Tilburg

Identifiable natural person

'personal data' means any information relating to an identified or identifiable natural person ('data subject');

one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Breyer case [ECJ, 2016]

IT IS NOT NECESSARY "THAT ALL THE INFORMATION ENABLING THE IDENTIFICATION … MUST BE IN THE HANDS OF ONE PERSON"

a dynamic IP address *registered by an online media services provider* when a person accesses a website that the provider makes accessible to the public constitutes personal data, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the Internet service provider has about that person

Personal data in the onlife world

The contribution, having examined the notion of personal data in EU data protection law, concludes that in the onlife world of data-driven intelligence which is firmly on its way, everything will soon fall within the definition of personal data as interpreted by the EDPB (formerly WP29) and the Court of Justice

The term 'onlife' was coined by Luciano Floridi and refers to 'the new experience of a hyperconnected reality within which it is no longer sensible to ask whether one may be online or offline' (Luciano Floridi, '*Introduction*' in Stefana Broadbent et al., *The online manifesto. Being human in a hyperconnected era* (Luciano Floridi ed, Springer 2015), 1).

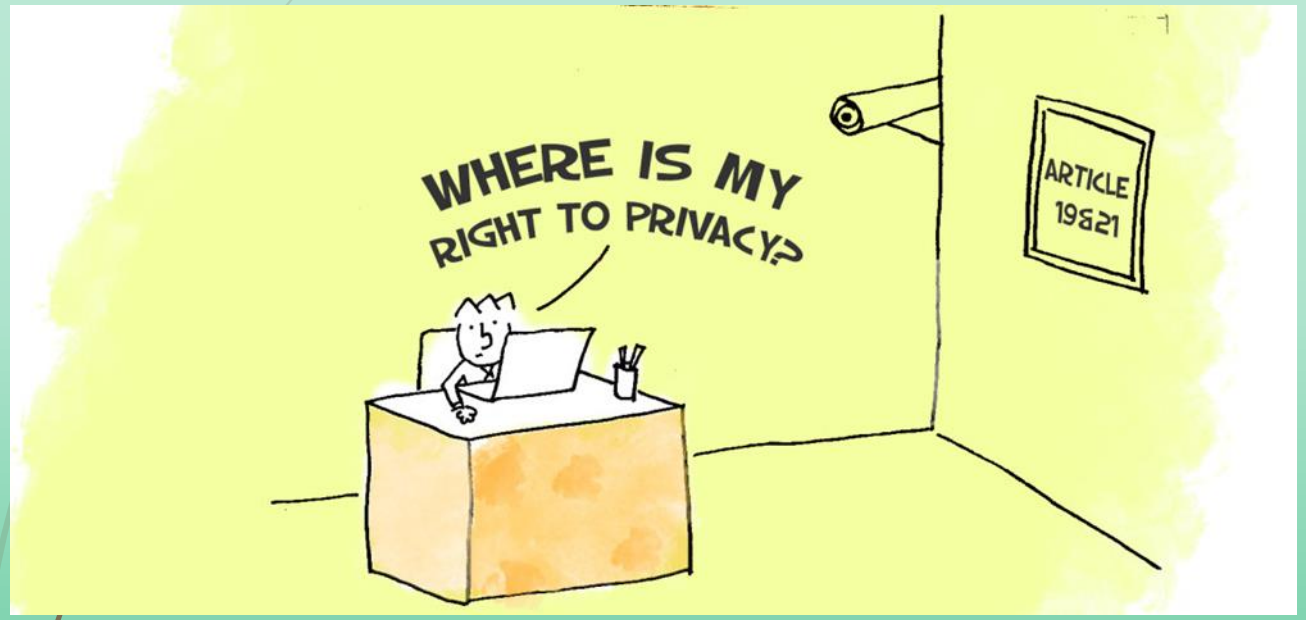
Datafication

Everything is being converted to data

Digitization was the process of taking the analog world to the digital environment; it allowed society to store more information and process it more rapidly

The next step is to datafy information, to “put it in a quantified format so it can be tabulated and analyzed”. Datafication allows analysis of information in more sophisticated ways and allows analyses across large data sets

FROM THE RIGHT TO PRIVACY TO THE RIGHT TO DATA PROTECTION



Right to privacy

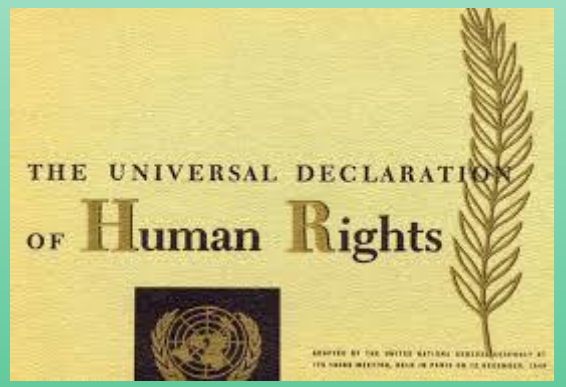
INTERNATIONAL INSTRUMENTS

The right to privacy became an international human right before it was a nationally well-established fundamental right

UNIVERSAL DECLARATION OF HUMAN RIGHTS (1948)

Article 12

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks



INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS (1966)

Article 17

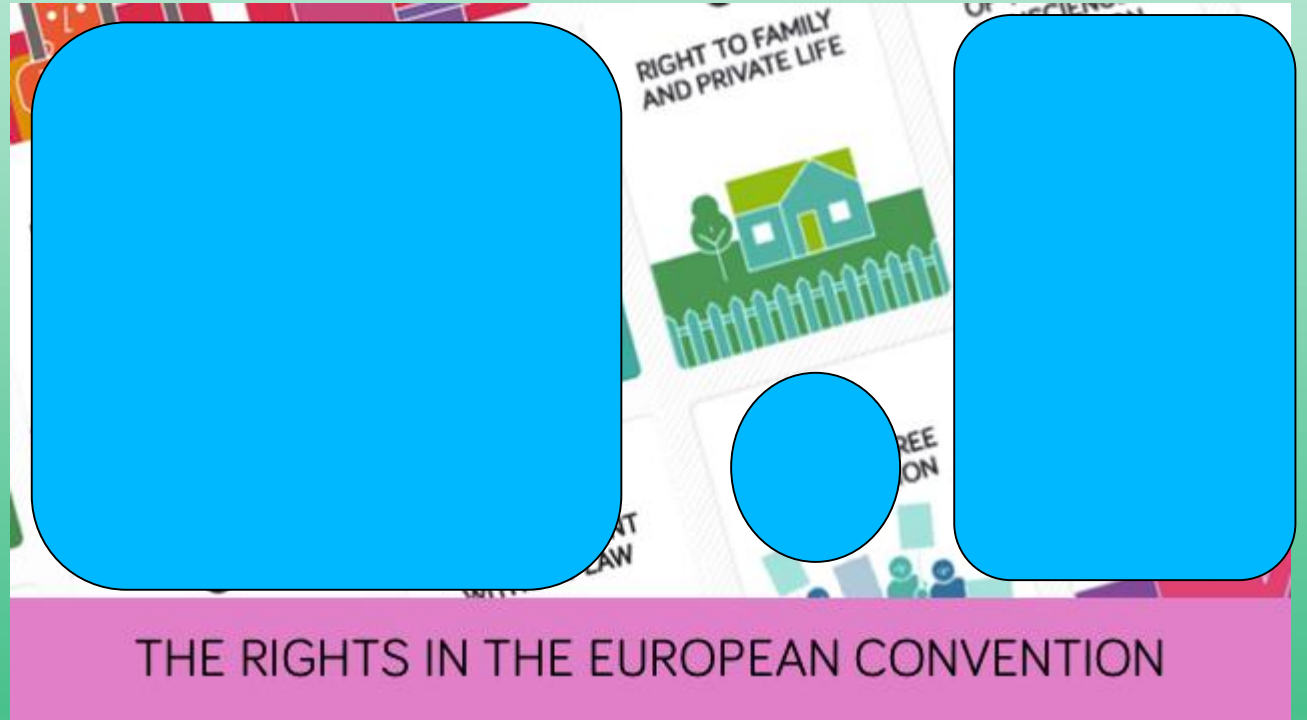
1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

The sole difference between the two norms is that Article 17 of the ICCPR not only prohibits 'arbitrary' interferences with one's privacy and with more specific aspects of the private sphere, but also 'unlawful' ones

EUROPEAN CONVENTION ON HUMAN RIGHTS (1950)

Article 8(1)

Everyone has the right to respect for his private and family life, his home and his correspondence.



AMERICAN CONVENTION ON HUMAN RIGHTS (1969)

Article 11(2)

No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.

African Charter on Human and Peoples' Rights [Banjul Charter) (1981)

Although it is evident that the African Charter is tailored specifically to the African context, it is contentious due to its strong emphasis on social, economic and cultural rights and the inadequate coverage of civil and political rights. An example of this inadequacy is the

lack of explicit recognition of the right to privacy

[Lucinda Patrick-Patel (2014)]

PRIVACY AS FREEDOM FROM SOCIETY v. PRIVACY AS DIGNITY

Historical roots

Evolution

Towards "decisional privacy"

Historical roots

Conception of privacy as the ‘right to be let alone’

[Warren and Brandeis (1890)]

Evolution

Conception of privacy as control over personal information

[Westin (1967): “the claims of individuals or groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others”;

advancement in electronic spying devices has presented increasing threats to privacy in society]

Towards "decisional privacy"

non-informational aspects

individual's entitlement to make its own decisions

RIGHT TO DATA PROTECTION

The expression ‘data protection’ (derived from the German word *Datenschutz*) is most commonly used in continental European jurisdictions.

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

Article 7 - Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 - Protection of personal data

1. *Everyone has the right to the protection of personal data concerning him or her.*
2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
3. *Compliance with these rules shall be subject to control by an independent authority.*

TREATY ON THE FUNCTIONING OF EUROPEAN UNION

Article 16

1. *Everyone has the right to the protection of personal data concerning them.*
2. *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

TREATY ON EUROPEAN UNION

Article 39

In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter [common foreign and security policy], and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

Regulation (EU) 2016/679

[General Data Protection Regulation]

Explicitly mentions "the right to data protection"

Interaction between Internet of Things and big data

Almost all platforms operating online (e.g. Amazon, Google, Facebook, Ebay) develop software applications that run on users smart devices (e.g. phones, tablets, smart-TVs, watches) with a large market penetration

Furthermore, products and objects supporting services offered through these platforms are more and more connected and can provide direct communication among them and feedback to the platform itself

All this contributes to the Internet of Things ("IoT"), which brings about a significant capability to "harvest" personal data on a large scale, coupled with increasing computing power ("big data“).

DATA PROTECTION LAW

is it still good enough

to perform the assigned task?

Autonomous algorithmic processes

Some critical issues

Data analytics

Digitalization of everyday life

→ ***insufficient safeguards***

Distinction between personal and non-personal data

→ ***not very useful***

Right to privacy needs to be complemented with other legal mechanisms

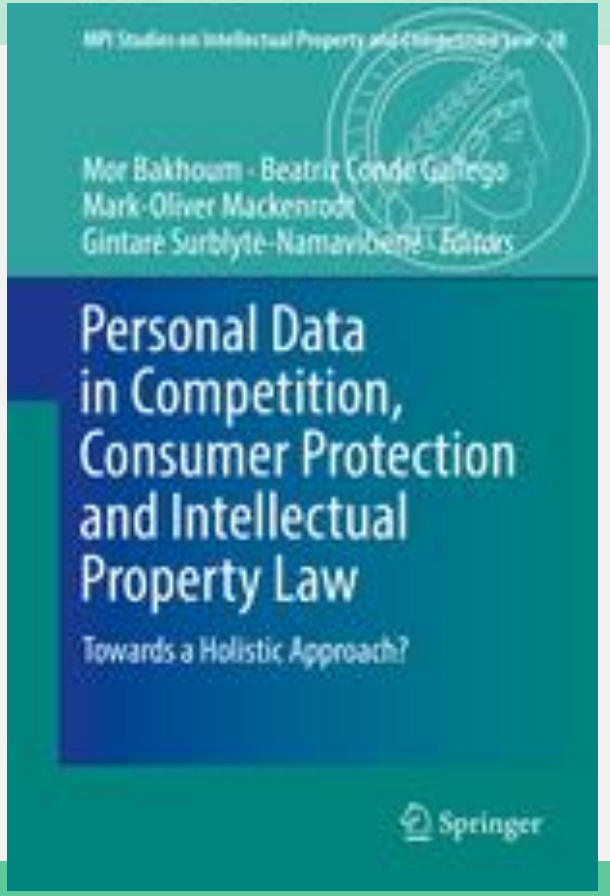
Alternative system of legal protection against data-driven harms?

Consumer protection

Competition

An integrated approach of different fields of law

synergies and tensions



Unfair commercial practices
ICA investigation (1)

6 April 2018

The Italian Competition Authority has launched investigations against Facebook Inc. over alleged unfair commercial practices, regarding:

i) **the information provided by the company during the registration to the Facebook platform, with reference to the methods for collecting and using the users' data for commercial purposes, including information generated by Facebook users while using apps belonging to the group and by accessing third party websites / apps;**

Unfair commercial practices
ICA investigation (2)

ii) the **automatic activation of the platform for the exchange of personal data from/to third parties** for every time the user accesses or uses third party websites and apps, with general authorization validity devoid of user consent, only providing an opt-out option. In particular, the option available to the user to renounce to this method or to proceed would be pre-set as the box to consent to the transfer of data is already ticked.

Unfair commercial practices
ICA investigation (3)

6 April 2018

Closed the investigation → fines for a total of 10 million euros

Misleading practice

The information provided is in fact general and incomplete and does not adequately make a distinction between the use of data to personalize the service (in order to connect "consumer" users with each other) and the use of data to carry out advertising campaigns aimed at specific targets

Unfair commercial practices
ICA investigation (3)

6 April 2018

Closed the investigation → fines for a total of 10 million euros

Misleading practice

The information provided is in fact general and incomplete and does not adequately make a distinction between the use of data to personalize the service (in order to connect "consumer" users with each other) and the use of data to carry out advertising campaigns aimed at specific targets

Unfair commercial practices
ICA investigation (4)

6 April 2018

Closed the investigation → fines for a total of 10 million euros

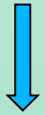
Aggressive practice

undue influence caused by the pre-selection of the broadest consent to data sharing

When users decide to limit their consent, they are faced with significant restrictions on the use of the social network and third-party websites / apps, which induce users to maintain the pre-selected choice

Interaction between data protection and competition rules

Existence of specific data protection mechanisms



does not make competition law irrelevant

competition authorities should be allowed to consider privacy policies from a competition standpoint whenever these policies are liable to affect competition

* European Commission

mergers of *Google/DoubleClick* and *Facebook/WhatsApp*

considered the implications for market power of the transactions for the availability of data in the markets for online advertising and communications services

Power asymmetries in the marketplace for personal data

Companies monetise personal data by exploiting indirect network effects

Power asymmetries between users and service providers: consumers are unaware of the collection of personal information and how they are used

Data protection framework is inadequate to address the privacy concerns arising in the digital market

Can data protection concerns be incorporated into competition policy?

There are two provisions whitin the TFEU by which data protection, as a non-economic goal, could be integrated into competition analysis:

** Articles 12 and 16 TFEU*

Common objectives of competition law and data protection

* *Protection of individuals*

* *tackling power asymmetries*

The proposition about the incorporation of data protection into competition law has not been unanimously welcomed: competition law is focused on economic efficiency and its nature would be at risk of being distorted

The German investigation

Bundeskartellamt

2016:

launched an investigation against Facebook, on suspicion of having abused its market power by infringing data protection rules

attacked the way the social network giant scoops up information on how users surf to drive its advertising revenue

2017:

issued a preliminary legal assessment in the abuse of dominance proceeding

The background of the Bundeskartellamt's investigation

The German antitrust authority, by linking the article 102 TFEU, in its reference to "unfair traiding condictions", to data law breaches, would provide a

novel type of anti-competitive conduct in the digital market:

the collection of personal data

The dominant market position of Facebook

A choice between accepting the whole Facebook package

or

not using at all.

Exploitative business terms

The use of online services of a dominant company is conditional upon the extensive permission of users to use their personal data

Civil law principles can be applied to determine wheter business terms are exploitative

The objective is to ensure that users can decide freely and without coercion on how their personal data are used

FOCUS OF THE INVESTIGATION

Terms that make the access to the social networking service dependent on users' consent to a limitless collection of their personal data

Facebook is said to collect its users' data not only from services that the company directly owns (such as Whatsapp or Instagram), but also from secondary websites and applications of other operators with embedded Facebook APIs

Unilateral imposition of terms susceptible of infringing data protection rights

Unilateral imposition of unfair terms

Abuse of a dominant position

The harm for competition

-Facebook's services are for free

-the users are not able to control how their personal data are used

-Facebook can use them to improve its advertising activities

EDPS

Proposal: Digital Clearing House

Opinion 8/2016. EDPS Opinion on coherent enforcement of fundamental rights in the age of big data. 23 September 2016

an urgent need for coherent enforcement of digital rights in all domains of law regulating online markets

6 February 2019 Decision

imposed on Facebook far-reaching restrictions in the processing of user data

* Facebook services (such as WhatsApp or Instagram) can continue to collect data for their services.

** However, Facebook may only combine these data and assign them to a Facebook user account if users give their voluntary consent to this practice.

***In the case of data from third party websites, voluntary consent by the user is already required for their collection.

'Voluntary' means that the use of Facebook's services must not be subject to the users' consent. If users do not consent, Facebook may no longer combine data in the comprehensive manner described above, or only to a highly restricted extent.

The Digital Clearing House as a tool to enforce digital rights

Voluntary network of regulatory bodies to share information about abuses in the digital ecosystem and to find the most effectively way of tackling them

Jens-Erik Mai(2016) *[The Information Society]*

"The age of big data calls for a reconceptualization of the notion of privacy. Previous models of privacy limit their focus on collection and gathering of data as the central mechanism of the privacy concern.

Accordingly, privacy is seen as the ability to restrict access to information or the ability to control the flow of personal information.

In the age of big data, a significant concern is how new personal information is produced by businesses and organizations through predictive analytics"

Thank you very much for your kind attention