Of data protection, AI and democracy …..

Prof. Lilian Mitrou

University of the Aegean

President of Institute for Privacy Law, Data Protection and Technology (IPL – European Public Law Organisation)

Risks for (Informational) Privacy and (Digital) Democracy

- Data protection/ Informational privacy indicates much more as informational seclusion and (protection of) confidentiality
- Unrestricted access to/use of personal data imperils virtually every constitutionally guaranteed right.
- Neither freedom of speech nor freedom of (access to) information, nor freedom of association can be fully exercised as long as it remains uncertain whether, under what circumstances and for what (lawful) purposes personal information is collected and processed.
- Refraining from exercising fundamental rights may have serious impact on democracy

Informational Privacy, Dignity and Personality

- Collection and processing of personal data, especially without knowledge or consent of the person or another legal basis, is an assault on the dignity of the person
- Claim for exercising control over one's own information (Westin) or the right to informational self-determination (BVerfG, Volkszaehlungsurteil - 1983)
- Personality, does invoke a kind of freedom allowing , each individual to realize her potential as an individual and to participate into social life.
- Privacy is grounded on dignity and personality but, at the same time, it has become a pre-requisite for the development of everyone's personality.

Data Protection and democracy

- Informational privacy offers safeguards to preserve an underlying capacity for autonomous decision - and choice-making.
- Privacy protects individuals against practices that erode individual freedom, their capacity for self-determination, and their autonomy to engage in personal and social relationships, to foster social appearance and behaviour and to participate to the public sphere
- Development of the capacity for autonomous choices and decisions is an indispensable condition for free action in society
- The autonomy fostered by informational privacy generates collective benefits because it promotes participation in public life/affairs
- Informational privacy promotes the development of both individuals and society / democracy

A legal framework to balance rights and interests

- A separate and distinct right to “protection of personal data” (“data protection”) has become recognised
- Data protection refers to a system of legal rules that structures the collection and use of personal information, the lawful and fair treatment of personal information.
- The law establishes the terms and conditions under which the processing of personal data is to be carried out so as to protect the fundamental rights and liberties of natural persons and in particular the right to informational privacy.
- Regulation aims at ensuring a (more or less fair) balance between data protection and competing fundamental rights, also embedded in Constitution such as freedom of information and/or overriding public interests, such as transparency or combatting tax evasion.

A legal framework for the digital age?

- The European Data Protection Directive (1995) was a milestone in the history of personal data protection adopted before the explosion of Internet.
- The EU legislator in the ‘90s could not predict neither the indexing, cross-referencing and profiling capabilities of Internet, nor the new communication environment, influenced by globalization of information flows, online social media and data sharing.
- Information society is no longer a parallel environment where individuals can participate on a voluntary basis, but an integrated part of our everyday lives.
- The legislator had to face a new technological landscape marked by BIG DATA analytics , cloud computing, participatory and semantic WEB, ambient and ubiquitous computing, RFIDs and geo-location devices and applications, Internet of Things or Internet of (Every)thing
- A new legislation was required to address shortcomings and technological challenge
- What was needed was to re-invent, rethink on new tools and a new architecture of data protection
- The GDPR was the response of the European legislators to these challenges

Digital identities and digital (“territorial”?) scope

- Defining personal data in line with the online reality- the “online identifier”
- Persons may be identified (directly or indirectly), associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags…..leaving digital traces

- Subject to the provisions of GDPR are data controllers/processors that they are performing activities related to
  - the offering of goods or services to data subjects in the Union or
  - the monitoring of the behaviour of data subjects insofar as their behaviour takes place within the Union

  Even if they are not established in EU territory
- Data Privacy Imperialism or legal certainty and better control for individuals?
- Difficulties to enforce the law on borderless Internet

Major changes introduced by GDPR

- Responding to technological challenges by a synergy between law and technology – Data Protection by Design : Built-in
- Fostering Data Protection Principles, including Information Security as a principle and legal requirement
- Risk based approach – The GDPR contains a number of mandatory rules that may require a judgement, especially when it comes to identify and assess risks, the nature, likehood and severity of them defines the obligations of data controller
- Another approach with regard to compliance
  - Accountability- able to demonstrate compliance
  - Data Protection Impact Assessment – to identify and mitigate risks
  - Data Protection Officer as internal monitoring and compliance mechanism
- Very high fines as sanctions
- Enhancement of Transparency
  - Data Breach Notification requirements
  - Information of the Data Subject

Artificial Intelligence as a new challenge

- A surge of interest in machine learning, algorithmic decision making and offering of cognitive services.
- to be attributed to the exponential growth of “datafication”
- In its interplay with Big Data, ambient intelligence, ubiquitous computing, Internet of Things and cloud, AI augments the existing major, qualitative and quantitative shift with regard to the processing of personal information
- Profiling and classification algorithms: Designed to anticipate outcomes about the behaviour of a person?
- Able to derive the intimate from the available
- Lack of transparency - “opacity of algorithms”

Artificial Intelligence and GDPR

- GDPR does not specifically address AI.
- The GDPR applies both in the phase of AI development and with regard to its use for analyzing and decision making about individuals.
- The rules and principles of GDPR, such as the notion of identifiability of the data subject, are flexible enough to respond to AI challenges.

A technology neutral framework?

- Technology (especially nowadays AI and Robotics) are advancing more rapidly than the process of finding answers to ethical, legal and societal questions –
- Regulations like the GDPR will always fall behind new advances in technology
- A vicious circle as technology changes also during the consultation and negotiation procedures, thus posing the risk to result into legal uncertainty.
- GDPR as a technology-neutral framework
- Technology independent rules are regarded as a means to stand firm with technological turbulences, to deal with the unforeseeability of the technological developments
- Emphasis is not on the technology used for data processing but on the effects to be regulated, on the risks and impacts on fundamental rights that are to be faced.

AI, Accountability and Data Protection Impact Assessment

- Accountability: - to check and be able to demonstrate that the algorithms developed and used by machine learning systems “ are actually doing what we think they’re doing and aren’t producing discriminatory, erroneous or unjustified results”
- Assessing risks for rights and freedoms
- Despite the uncertainty of “high risk threshold” , it is highly likely that most AI/ machine learning applications will fall into the category of processing for which a Data Protection Impact Assessment should be conducted

Data protection by design

- Synergy of law and technology as key element of GDPR mirrored in the enhanced role of technology in the context of security and privacy by design provisions
- To be able to protect fundamental rights, research, design and development of new technologies, such as robotics and “autonomous” systems should be guided by an authentic concern for research ethics, social accountability of developers and privacy conscious design
- to anticipate impacts of technology

Is GDPR AI-proof ?

- Does GDPR deal sufficiently with AI?
- Is AI controllable and subject to regulation?
- Are artificial intelligence and data protection incompatible?
- The potential of AI is likely to result to – non predictionable – penetrating data processing
- “applications of AI and robotics should not pose unacceptable risks of harm to human beings, and not compromise human freedom and autonomy
- AI technologies not binding to basic constitutional principles would led to a “widespread culture of disregard of the law and put democracy in danger”

Responsible Research and Innovation

- AI technologies should “be designed, developed and used in respect of fundamental human rights and in accordance with the fairness principle
- To be able to protect fundamental rights, research, design and development of AI, robotics and “autonomous” systems should be guided by an authentic concern for research ethics, social accountability of developers, and global academic cooperation
- Conscious engineering and Responsible Research and Innovation
- Key elements of an RRI approach is being anticipatory, reflective, collective, responsive and transparent

Of Fundamental Rights and AI Ethics

- Enhanced accountability and transparency requirements of GDPR pose technical challenges for AI developers to mitigate adverse effects of AI
- Tools to support the protection of values and principles while developing and using AI technologies
- The current trend in addressing the ethical and legal aspects of AI and machine learning is to focus on fairness, autonomy, responsibility and ethical principles.
- A clear need for a collective, wide-ranging and inclusive process towards a commonly acceptable framework for the design, production, use and governance of AI, robots and “autonomous” systems