Comments to Inception Impact Assessment regarding a potential proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence

(from privacy/data protection perspective)

This opinion only reflects the views of its author.

1. The European Commission published an Inception Impact Assessment,[1] in which – after a White Paper[2] on similar issue – outlines options of regulating the AI. These options are the followings (according to the Inception Impact Assessment):

a) Option 1: EU soft-law (non-legislative approach) to facilitate and spur industry-led intervention,
b) Option 2: EU legislative instrument setting up a voluntary labelling scheme,
c) Option 3: EU legislative instrument establishing mandatory requirements for all or certain type of AI application,
d) Option 4: Combination of any of the option above taking into account the different levels of risk that could be generated by a particular AI application.

2. Although there are considerable pros and cos regarding any of the options above, one thing cannot be forgotten: as the White Paper did, this Inception Impact Assessment also just repeats – among others – that there is legal uncertainty around AI but refrains from stating clearly that the *most considerable legal uncertainty around the AI is the data protection related uncertainty*, i.e. whether current EU data protection legislation (GDPR and Law Enforcement Data Protection Directive) allows the use of AI at all.[3]

Unfortunately, the current text of the GDPR, as well as its interpretation represent a constant risk of non-compliance with the GDPR: the *necessity* of use of AI can always be challenged, as well as its *proportionality*, or the compliance with any other principles (e.g. data minimization, storage limitation etc.).[4] In order to support the use of AI (and to invest in AI solutions) such uncertainties should be eliminated. It might happen in two ways:

a) interpretation of the current legal framework (GDPR, Law Enforcement Data Protection Directive) but neither the provision of the said legal instruments, nor the restrictive interpretation is promising;[5]
b) sectoral EU legislation. The GDPR [Art. 22(2)(b) and 23(1)(e)] refers to such possibility.

If the EU intends to regulate AI, that would be a good opportunity to regulate these privacy related issues as well. The form of such provisions – because the privacy rules now are in an EU regulation – cannot be else but another EU regulation, i.e. a piece of sectoral legislation that provides a comprehensive legal framework of the privacy related aspects of the AI.[6] This legal act should – while preserving the *principles* of the privacy (e.g. GDPR) –, surely, deter

[1] Ref. Ares(2020)3896535 - 23/07/2020 – downloadable from https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements

[2] White Paper on Artificial Intelligence – A European approach to excellence and trust (COM(2020) 65 final) - https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

[3] See e.g. Center for Data Innovation Report: The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy – https://www.datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/

[4] *"[M]any EU policymakers are resistant to [the] idea [of mending, not ending, the GDPR] because they consider the GDPR to be an ethical commitment they cannot walk away from, and any attempt at improvement would be seen as an admission of a mistake."* – Center for Data Innovation Report

[5] This is, partially, due to the fact that the GDPR is, from technological point of view, a bit outdated.

[6] As there are other sectoral legislative acts, e.g. the draft e-Privacy Regulation, and many references to possible EU legislation all around in the GDPR.

from the *rules* of the GDPR to the necessary extent in order to provide AI-tailored privacy provisions. Therefore, Option 3 above seems to be the best option.[7] A separate piece of sectoral legislation could cover other aspects of AI (product safety and product liability, consumer protection etc.) as well.

3. The followings could be – from privacy perspective – topics of an AI-related sectoral legislative act (taking also into account the principle laid down in recital 4[8] of the GDPR):

a) Declaration of the possibility of use AI solutions that meet the requirements of the given legislative act – this would create the legal ground (different from the GDPR) for the use of AI;
b) Limitation on the potential use (i.e. the purposes) of AI solutions (either "blacklist" – i.e. forbidden use, or "white list" – i.e. allowed use), including the special conditions to be met. On the other hand, the new legislative act should adapt specific rules *"to permit organizations to repurpose data already collected, as long as doing so poses only minimal risk of harm to individuals and does not involve the transfer of data from one controller to another"*;[9]
c) Special rules for some data processing activities, e.g. general permission for use of personal data as training data – with no or limited possibility to opt out. In this way, the future legislation might ease the strict interpretation of "data minimization" principle as well;
d) Specific rules on transparency, inc. the minimum set of information to be shared with data subjects on the "logic" of AI;
e) If necessary, some limitations on the data subject rights (e.g. on erasure or objection to ensure the availability of the data for the purpose of training of AI);
f) AI-specific data security measures (e.g. compulsory pseudonymization or anonymization, other rules stricter than the general ones);
g) Allocation of obligations on those actors who are *"best placed to address any potential risks"*. It means that the personal scope of the new legislative act should not be limited to data controller and data processors, but should "*include the developer, the deployer (the person who uses an AI-equipped product or service) and potentially others (producer, distributor or importer, service provider, professional or private user)"* – with carefully allocated adequate responsibilities. [10]

By Zsolt Bartfai

[7] It is worth mentioning that even the Inception Impact Assessment seems to prefer this option by outlining sub-options (according to the scope of the to-be legal instrument).

[8] *"The processing of personal data should be designed to serve mankind. The right to the protection of personal data is* ***not an absolute right****; it must be considered in relation to its function in society and* ***be balanced against other fundamental rights****, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information,* ***freedom to conduct a business****, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."*

[9] Center for Data Innovation Report

[10] White Paper, p. 22