EUROPEAN LAW BLOG
NEWS AND COMMENTS ON EU LAW

ELB Blogpost 37/2024, 16 July 2024
Tags: AI governance, AI regulation, data protection law, privacy by design, algorithmic accountability
Topics: Artificial Intelligence, Data Protection and Digital Governance

The AI Act and a (sorely missing!) right to AI individualization; Why are we building Skynet?

By Vagelis Papakonstantinou

The industry has tricked us; Scientists and regulators have failed us. AI is developing not individually (as humans become individuals) but collectively. A huge collective hive to collect, store and process all of humanity's information; a single entity (or a few, interoperability as an open issue today as their operation itself) to process all our questions, wishes and knowledge. The AI Act that has just been released ratifies, for the moment at least, this approach: EU's ambitious attempt to regulate AI deals with it as if it was simply a phenomenon in need of better organisation, without granting any rights (or participation, thus a voice) to individuals. This is not only a missed opportunity but also a potentially risky approach; while we may not be building Skynet as such, we are accepting an industry-imposed shortcut that will ultimately hurt individual rights, if not individual development per se.

This mode of AI development has been a result of short-termism: an, immediate, need to get results quickly and to make a 'fast buck'. Unlimited (and unregulated, save for the GDPR) access to whatever information is available for processing obviously speeds things up – and keeps costs down. Data-hungry AI models learn faster through access to as-large-as-possible repositories of information; then, improvements can be fed into next-generation AI models, that are even more data-hungry than their predecessors. The cycle can be virtuous or vicious, depending how you see it.

In 1984 iconic film *The Terminator* humans fought against Skynet, "*an artificial neural network-based conscious group mind and artificial general superintelligence system*". Skynet was a single, collective intelligence ("group mind") that quickly learned everything

that humans knew and controlled all of the machines. Machines (including, *Terminators*) did not develop independently, but as units within a hive, answering to and controlled by a single, omnipresent and omnipotent entity - Skynet.

Isn't this exactly what we are doing today? Are we not happy to let Siri, Alexa, ChatGPT (or whatever other AI entity the industry and scientists launch) process as a single entity, a single other-party with which each one of us interacts, all of our information through our daily queries and interactions with them? Are we not also happy to let them control, using that same information, all of our smart devices at home or at the workplace? Are we not, voluntarily, building Skynet?

But, I do not want to be talking to (everybody's) Siri!

All our AI end-user software (or otherwise automated software assistants) is designed and operates as a single, global entity. I may be interacting with Siri on my iPhone (or Google Assistant, Alexa, Cortana etc.), asking it to carry out various tasks for me, but the same do millions of other people on the planet. In essence, Siri is a single entity interacting simultaneously with each one of us. It is learning from us and with us. Crucially, however, the improvement from the learning process goes to the one, global, Siri. In other words, each one of us is assisted individually through our interaction with Siri, but Siri develops and improves itself as a one and only entity, globally.

The same is the case today with any other AI-powered or AI-aspiring entity. ChatGPT answers any question or request that pops in one's mind, however this interaction assists each one of us individually but develops ChatGPT itself globally, as a single entity. Google Maps drives us (more or less) safely home but at the same time it catalogues how all of us are able to move on the planet. Amazon offers us suggestions on books or items we may like to buy, and Spotify on music we may like to listen to, but at the same time their algorithms learn what humans need or how they appreciate art.

Basically, if one wanted to trace this development back, they would come across the moment that software transformed from a product to a service. In the beginning, before prevalence of the internet, software was a product: one bought it off-the-shelf, installed it on their computer and used it (subject to the occasional update) without having anything to do with the manufacturer. However, when each and every computer and computing device on the planet became interconnected, the software industry, on the pretence of automated updates and improved user experience, found an excellent way to increase its revenue: software became not a product but a service, payable in monthly instalments that apparently will never stop. Accordingly, in order to (lawfully) remain a service, software

needed to remain constantly connected to its manufacturer/provider, feeding it at all times with details on our use and other preferences.

No user was ever asked about the "software-as-a-service" transformation (governments, particularly from tax-havens, happily obliged, offering tax residencies for such services against competitive taxation). Similarly, no user has been asked today whether they want to interact with (everybody's) Siri. One AI-entity to interact with all of humanity is a fundamentally flawed assumption. Humans act individually, each one at their own initiative, not as units within a hive. The tools they invent to assist them they use individually. Of course it is true that each one's personal self-improvement when added up within our respective societies leads to overall progress, however, still, humanity's progress is achieved individually, independently and in unknown and frequently surprising directions.

On the contrary, scientists and the industry are offering us today a single tool (or, in any case, very few, interoperability among them still an open issue) to be used by each one of us in a recordable and processable (by that tool, not by us!) manner. This is unprecedented in humanity's history. The only entity so far to, in its singularity, interact with each one of us separately, to be assumed omnipresent and omnipotent, is God.

The AI Act: A half-baked GDPR mimesis phenomenon

The biggest shortcoming of the recently published AI Act, and EU's approach to AI overall, is that it deals with it only as a technology that needs, better, organisation. The EU tries to map and catalogue AI, and then to apply a risk-based approach to reduce its negative effects (while, hopefully, still allowing it to, lawfully, develop in regulatory sandboxes etc.). To this end the EU employs organisational and technical measures to deal with AI, complete with a bureaucratic mechanism to monitor and apply them in practice.

The similarity of this approach to the GDPR's approach, or a *GDPR-mimesis* phenomenon, has already been identified. The problem is that, even under this overly protective and least-imaginative approach, the AI Act is only a half-baked GDPR mimesis example. This is because the AI Act fails to follow the GDPR's fundamental policy option to include the users (data subjects) in its scope. On the contrary, the AI Act leaves users out.

The GDPR's policy option to include the users may appear self-evident now, in 2024, however it is anything but. Back in the 1970s, when the first data protection laws were being drafted in Europe, the pendulum could have swinged towards any direction: legislators may well have chosen to deal with personal data processing as a technology only in need of better organisation, too. They could well have chosen to introduce only

high-level principles on how controllers should process personal data. However, importantly, they did not. They found a way to include individuals, to grant them rights, to empower them. They did not leave personal data processing only to organisations and bureaucrats to manage.

This is something that the AI Act is sorely missing. Even combined with the AI Liability Directive, still it leaves users out of the AI scene. This is a huge omission: users need to be able to participate, to actively use and take advantage of AI, and to be afforded with the means to protect themselves from it, if needed.

In urgent need: A (people's) right to AI individualisation

It is this need for users to participate in the AI scene that a right to AI individualisation would serve. A right to AI individualisation would allow users to use AI in the way each one sees fit, deliberately, unmonitored and unobserved by the AI manufacturer. The link with the provider, that today is always-on and feeds all of our innermost thoughts, wishes and ideas back to a collective hive, needs to be broken. In other words, we only need the technology, the algorithm alone, to train it and use it ourselves without anybody's interference. This is not a matter simply of individualisation of the experience on the UX end, but, basically, on the backend.-The 'connection with the server', that has been forced upon us through the Software-as-a-Service transformation, needs to be severed and control, of its own, personalised AI, should be given back to the user. In other words, We need to be afforded the right to move from (everybody's) Siri to each one's Maria, Tom, or R2-D2.

Arguably, the right to data protection serves this need already, granting us control over processing of our personal data by third parties. However, the right to data protection involves the, known, nuances of, for example, various legal bases permitting the processing anyway or technical-feasibility limitations of rights afforded to individuals. After all, it is under this existing regulatory model, that remains in effect, that today's model of AI development was allowed to take place anyway. A specific, explicitly spelled-out right to AI individualisation would address exactly that; closing existing loopholes that the industry was able to take advantage of, while placing users in the centre.

A host of other considerations would follow the introduction of such a right. Principles such as data portability (art. 20 of the GDPR), interoperability (art. 6 of EU Directive 2009/24/EC) or, even, a right to be forgotten (art. 17 of the GDPR) would have to be revisited. Basically, our whole perspective would be overturned: users would be transformed from passive recipients to active co-creators, and AI itself from a single-entity monolith to a billion individualised versions, same as the number of the users it serves.

As such, a right to AI individualisation would need to be embedded in systems' design, similar to privacy by-design and by-default requirements. This is a trend increasingly noticeable in contemporary law-making: while digital technologies permeate our lives, legislators find that sometimes it is not enough to regulate the end-result, meaning human behaviour, but also the tools or methods that led to it, meaning software. Soon, software development and software systems' architecture will have to pay close attention to (if not be dictated by) a large array of legal requirements, found in personal data protection, cybersecurity, online platforms and other fields of law. In essence, it would appear that, contrary to an older belief that *code is law*, at the end of the day (it is) *law* (that) *makes code*.