Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 68

Artificial Intelligence and Privacy Laws in the EU and the US: A Moving Target?

Nikolaos I. Theodorakis

2020

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Nikolaos Theodorakis is Of Counsel in the Brussels office of Wilson Sonsini Goodrich & Rosati, where his practice focuses on privacy and cybersecurity. Nikolaos regularly counsels on matters of EU data protection law, GDPR compliance, cybersecurity preparedness, advertising, and marketing and offers a full cycle of services that includes both non-contentious matters and investigations with supervisory authorities.
Nikolaos represents multinational companies across a wide range of industries, including technology, financial services, healthcare, hospitality, food and beverage, insurance, pharmaceuticals, chemicals, and automotive. He also works with start-ups and established companies in the EMEA region, and, in particular, Greece and Cyprus. Having advised on a broad spectrum of corporate matters, Nikolaos has developed an expert insight into the increasing interplay between data protection, financial services (PSD2), competition law, and international trade law. He is at the forefront of advising on emerging privacy challenges on matters of AI, biotech, fintech, and blockchain.
In addition, Nikolaos is an associate professor of law and fellow at the University of Oxford, UK. He holds an LLB from the University of Athens, Greece, an MPhil from the University of Cambridge, UK, an LLM from University College London, UK, and a PhD from the University of Cambridge. Previously, Nikolaos taught and conducted research at the University of Cambridge, Harvard Law School, and Columbia Law School. He also gained professional experience at the U.S. Committee on Capital Markets Regulation, the Kluge Center at the U.S. Library of Congress, and the UK Ministry of Justice.
Nikolaos has received awards from several bodies, including the State Council of the People's Republic of China, Economic and Social Research Council (ESRC), British Academy, and the Greek Parliament. His works have been widely published, and he frequently receives invitations for public engagements, including guest lectures across the world, international symposia, and TEDx conferences.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:
Nikolaos I. Theodorakis, Artificial Intelligence and Privacy Laws in the EU and the US: A Moving Target?, Stanford-Vienna TTLF Working Paper No. 68, http://ttlf.stanford.edu.

Copyright

Abstract

Artificial Intelligence has several applications in sectors ranging from healthcare to insurance and financing. The unfathomable potential of big data is exponentially relevant in everyday corporate decision making, be it in a bank loan interest rate, an MRI scan preliminary analysis, or an insurance premium. Artificial Intelligence allows companies to monetize their data, be efficient, and make informed decisions.

However, Artificial Intelligence comes with certain caveats. First, unsupervised machine learning can lead to black box paradoxes, where it is impossible to attribute liability and control for potential computer biases. It is challenging for datasets to be truly anonymous since machine learning allows the association of data points in a way that individuals can most times be re-identified. Data may be retained for an indefinite period of time, whereas it is very difficult to actually grant an access right that an individual may wish to invoke.

The above have led to an interesting debate that revolves around ethics, philosophy, law and technology. The paper will explore how Artificial Intelligence has shaped modern technology, what are the main pros and cons also with regards to privacy, and how both sides of the Atlantic approach this matter.

Table of Contents

1. What is AI

Artificial Intelligence (AI) is used to describe a form of intelligence that machines demonstrate, in comparison to the living being's natural intelligence. Its definitions and interpretations have varied over the years since the notion itself has developed significantly in the past decades. Etymologically, Intelligence derives from words Inter (meaning "between" in Latin) and Legere (meaning "choose, pick out" in Latin), altogether referring to the capacity of humans to choose between, understand, and comprehend general truths.[1] Albeit the term was coined in the late 14th century, little did we know of the vast uses and applications that Artificial Intelligence would have nowadays.

Research on AI gained prevalence in 1950, when Alan Turing published his seminal paper on computing machinery and intelligence. In his paper, Turing proposed to consider the question "can machines think?"[2] To answer this, Turing coined the so-called "imitation game", whereby three parties, including an interrogator, a man and a machine, are unseen from one another. The man and the machine respond to the interrogator's questions; if the machine "imitates" human intelligence to a level that it tricks the investigator to believe it is a human being, it passes the test, now known as "Turing Test".

Even though Turing's paper was published in the 1950's, it was only in 2014 when a computer AI claimed to be the first in the world to pass the test,[3] while recently a computer AI passed the Turing

[1] Definition from Oxford Languages

[2] A.M. Turing, 'Computing Machinery and Intelligence' (1950) pp. 433-460 <https://academic.oup.com/mind/article/LIX/236/433/986238> accessed 03 November 2020

[3] BBC, 'Computer AI passes Turing test in 'world first'' (09 June 2014) <https://www.bbc.com/news/technology-27762088> accessed 03 November 2020

test not only for text, but also for an actual voice.[4] These recent developments demonstrate both the exponential growth of AI, since in a matter of a few years the progress in the AI field has risen significantly, and the willingness of humanity to further explore prospects and uses of AI.

Going back to where it all started, in 1956 John McCarthy kicked off AI research while stating that "AI is the science and engineering of making intelligent machines", while in 1960 AI started to gain more traction, with leading universities conducting research on it (e.g. MIT). Another celebrated publication was the Lighthill report in 1970, which established AI research related to automation and computer simulations of psychological and neurological processes.

However, the initial enthusiasm revolving around AI was soon followed by relevant concerns in the 1970's. Researchers quickly realized the limited computer power that did not allow for the impressive results they had hoped for. At the same time, the so-called Moravec's paradox cast doubt on how useful machines can be in practice- the paradox supports that solving problems is comparatively easy for computers, but a supposedly simple task like recognizing a face, or having awareness, is extremely difficult. As Moravec put it "it is comparatively easy to make computers exhibit adult level performance […] and difficult or impossible to give them the skills of a one-year-old."[5]

[4] David Gewirtz, 'Google duplex beat the Turing test: Are we doomed?' (*ZDnet*, 14 May 2018) < https://www.zdnet.com/article/google-duplex-beat-the-turing-test-are-we-doomed/> accessed 03 November 2020
[5] ThinkAutomation, 'What is Moravec's paradox and what does it mean for modern AI?' (ND) < https://www.thinkautomation.com/bots-and-ai/what-is-moravecs-paradox-and-what-does-it-mean-for-modern-ai/> accessed 03 November 2020

Research on AI toned down during the next decades, but it rebounded in the 90s since it applied to several functions such as data mining large databases. It was only in early 2000s when scientist started to explore further the notion of deep learning through neural networks

AI overall refers to systems that display intelligent behavior by analyzing their environment and taking actions- with a certain degree of autonomy- to achieve specific goals.[6] AI based systems can be: purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engine, speech and face recognition systems) or embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or IoT applications).

Data collected refers to structured data (organized according to pre-defined models (e.g. rational database) or unstructured data (i.e. data that does not have a known organization -e.g. image or piece of text).

Machine learning is a subset of AI; it provides systems the ability to learn by doing, i.e. by processing sample data, also known as "training data". In machine learning algorithms automatically improve through experience. Types of machine learning include:

- Supervised: An algorithm is learning from the dataset as the student learns from the teacher. We know the correct answers, and the algorithm makes predictions and is corrected by the teacher. Learning stops when the algorithm achieves an acceptable level of performance.

[6] European Commission, 'A Definition of AI: Main Capabilities and Disciplines' (2019), <https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines> accessed 03 November 2020

- Unsupervised: There is no teacher and no correct answers. Algorithms are left alone to make guesses and discover and present datasets.

- Reinforcement learning: AI systems are free to take decisions and are rewarded depending on whether the decision was bad or good (like a dog being rewarded with a treat if he acts well).

Most versions of machine learning relate to supervised learning, where a supervisor (human being) often reviews the computer's decisions and rewards or punishes it to steer it to the right direction. For instance, if a supervisor spots that the computer does not flag as suspicious a certain email, it will train the AI to flag this as suspicious moving forward. Also, digital payments companies often use machine learning tools to detect the occurrence or potential for fraud in their systems. Another daily of machine learning AI is tagging photos in social media- individual users actually supervise and "train" machine learning AI by indicating whether a certain picture relates to an individual.

Machine learning applies to mass processing operations, for instance email filtering, where the machine makes a prediction based on previous similar data it has processed so far. For instance, an email with a suspicious title will likely be caught in the email provider's spam filter since, based on training data, this type of emails more often than not has a malicious intent. This subset of AI is more sophisticated than traditional AI in the sense that computers learn from their "mistakes", and they improve over time.

Deep learning is a subset of machine learning that mimics the working of the human brain in processing data for use in detecting objects, recognizing speech, translating languages, and making

decisions.[7] Through artificial neural networks, algorithms get inspired by the human brain and learn from large amounts of data. Like humans learn from experience, the algorithm performs a task repeatedly and makes minor tweaks to improve its performance.

Deep learning process consists of two main phases:

- Training: process of labeling large amounts of data and determining their matching characteristics

- Inferring: the Deep Learning AI makes conclusions and labels new unexposed data by using the previous knowledge.

Deep learning can be supervised, semi-supervised or unsupervised. Deep learning is even more sophisticated than machine learning in that the machine creates digital neural networks that interlink concepts, and then try to deduct/use them as appropriate. Applications of deep learning are still developing, yet automatic speech recognition is probably the most well-known.

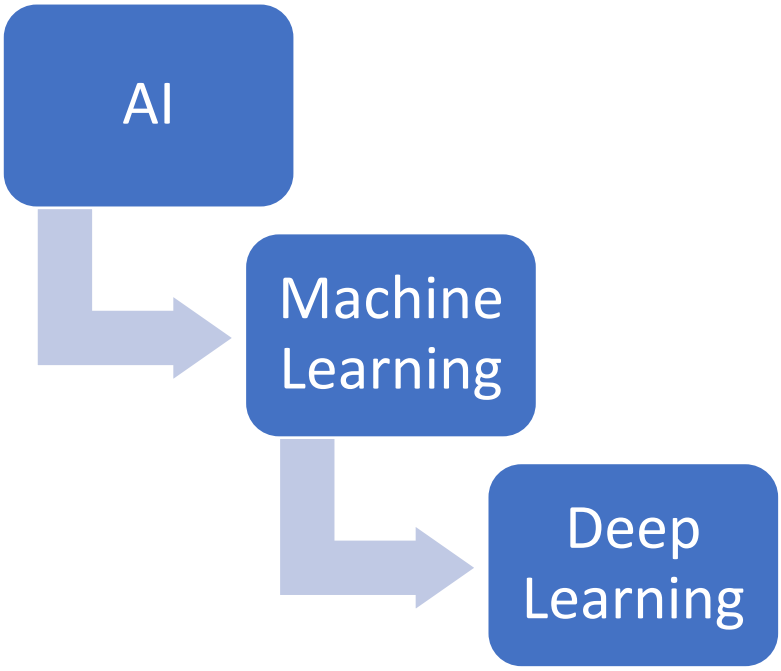
The advantages of using machine learning and deep learning are that the overall technological approach is more accurate and reliable, and there is less need for human guidance. Since the main elements for AI are data and algorithms, AI can typically be integrated in software. However, in machine learning AI algorithms are constantly trained to infer patterns based on a set of data that

[7] Marshall Hargrave, 'Deep Learning' (Investopedia, 30 April 2019), < https://www.investopedia.com/terms/d/deep-learning.asp#:~:text=Deep%20learning%20is%20an%20AI,is%20both%20unstructured%20and%20unlabeled.> accessed 03 November 2020

determines the actions needed to achieve a certain goal. AI-based products can act autonomously, yet their behavior is largely defined by their developers, which may cause incidents of bias (see more on this below).

The flexible and everchanging nature of AI means that an appropriate regulatory framework should also be flexible. It should not be excessively prescriptive, while protecting innovation. The below sections will discuss how the EU and the US have practically dealt with this, however, given the characteristics of the activities typically undertaken, significant risks are expected (e.g. healthcare, transport, energy). Also, AI applications should include a case by case assessment that discusses whether they produce legal or otherwise significant effects; if yes, appropriate safeguards should be in place.

Even though some AI technologies have been around for more than 50 years, significant advances in computing power, the availability of enormous quantities of data and new algorithms have recently led to major AI breakthroughs. AI is already present in our daily life, even though some of the most futuristic/impressive applications are still to be implemented. Deep learning can also be used for face recognition purposes, and assist with autonomous vehicles.



The above points clearly demonstrate the vast applications of AI. Some relevant examples include:

Online shopping and advertising

Artificial Intelligence is used in several apps to process mass amounts of data, provide personalized recommendations to individuals and assist consumers based on their previous searches and purchases. Aspects of consumer profiling and online behavior are largely based on Artificial Intelligence, including optimizing products, planning inventory, logistics etc.

Web Search

Search engines learn from the vast input of data that users provide, and present relevant search results on an as-needed basis.

Digital Personal Assistants

Smartphones use AI to provide personalized ads, while virtual assistants can be used when answering questions, providing recommendations and help organize daily routine of individuals.[8]

Cars

While self-driving vehicles are not yet standard, cars already use AI-powered safety functions.

Cybersecurity

AI systems can help recognize and fight cyberattacks and other cyber threats based on the continuous input of data, recognizing patterns and backtracking the attacks.

Health

Companies are taking advantage of AI capability in health diagnostics, preventive medicine, and active assistance in surgeries. The healthcare system has overall widely used AI for its infrastructure, research and development.

Transport

AI could improve the safety, speed and efficiency of rail traffic by minimizing wheel friction, maximizing speed and enabling autonomous driving.

[8] European Parliament, 'What is artificial intelligence and how is it used?' (2020) < https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used > accessed 03 November 2020

Food and farming

AI can be used in creating a sustainable food system, it can ensure a healthier food by minimizing and controlling the level of pesticides, help productivity and reduce the environmental impact. Many farms already use AI to monitor the movement, temperature and feed consumption of animals.

Public administration and services

AI is used widely to recognize data and pattern recognition. As such, it could provide early warnings for natural disasters and allow for efficient preparation and mitigation in connection with same.

2. AI: Brave New World?

As described above, AI has tremendous potential to perform several functions that were previously only performed by humans. This does not necessarily trigger a situation close to Huxley's dystopian novel, yet it signals growth that was unimagined before, while creating certain privacy risks and concerns. AI increases the possibility to track and analyze the daily habits of consumers, yet this may lead to potential risk for individuals' privacy, including potential breach of data protection rules and mass surveillance. AI is also used by online intermediaries to perform content moderation. The quantity of data processed, the applications, and the relevant processes can hamper rights to freedom of expression and related political freedom.

Certain AI algorithms, when exploited for predicting criminal recidivism, can display gender and racial bias, demonstrate different recidivism prediction probability for women v. men or for nationals

v. foreigners.[9] The risks of bias and discrimination are therefore inherent risks of using AI for, e.g., policing or border control activities. Human decision-making is also flawed and by no means immune to mistakes and biases, yet exactly the same biases are transposed to AI. However, assuming that AI may be used massively in large-scale, this bias can further affect and discriminate against individuals.

In fact, several reports accuse AI of perpetuating racial injustice,[10] of training data being saturated in a way that leads to racism,[11] and of processing data with lack of transparency which may perpetuate unfair policing.[12] In that regard, the EU has openly pledged to tackle AI discrimination by resisting to "copy and paste" everyday racial discrimination and bias into algorithms in Artificial Intelligence.[13]

In essence, an AI 'learns' while in operation, meaning that it processes certain datasets and acts based on these operations. However, if the datasets are skewed, or demonstrate only particular age or racial groups, it is highly likely that the AI will develop this form of bias itself. Albeit bias and discrimination

[9] Tolan S., Miron M., Gomez E. and Castillo C. 'Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia' (2019) Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law

[10]Miriam Vogel, 'Biased AI perpetuates racial injustice' (*Techcrunch*, 2020) <https://techcrunch.com/2020/06/24/biased-ai-perpetuates-racial-injustice/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAG05Ny3Ih7wckhhdMUMAc_F-ZRiHL2eRgKDvcF5GrhfYio2YZM6Rum9c1JU1TaEdLNo24o-HH7MfiW_cJQ8ByrSfGMFopVy1A0F3-F0Pg-RYj8ZK5nlW5iPt1qNjNx7Zvp1nKPMpUi77jzKSnHjeYd499LNeBAFi5LOJ16ojn0PB> accessed 03 November 2020

[11] Heidi Ledford, 'Millions of black people affected by racial bias in health-care algorithms' (Nature, 26 October 2019) < https://www.nature.com/articles/d41586-019-03228-6> accessed 03 November 2020

[12] Will Douglas Heaven, 'Predictive policing algorithms are racist. They need to be dismantled.' (*MIT Technology Review*, 17 July 2020) < https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/> accessed 03 November 2020

[13] Samuel Stolton, 'EU must 'proactively' tackle AI discrimination, Jourova says' (Euractiv, 18 September 2020) < https://www.euractiv.com/section/digital/news/eu-must-proactively-tackle-ai-discrimination-jourova-says/> accessed 03 November 2020

are inherent societal risks, present in every economic activity, such bias when being presented in AI could have a way more devastating effect, affecting and discriminating people against (e.g. loan applications, credit rating scores, passport controls etc.) without the social control mechanisms to scrutinize or otherwise control the situation. As such AI can be a great learning tool, while at the same time we should be mindful of how it is used in practice.

In cases where the outcome could not have been prevented from the design phase (e.g. because the algorithm processes the data in a different way than initially envisaged), the risks will primarily stem from the practical impacts of the correlations or patterns that the system identifies in the dataset. Characteristics of AI technologies include opacity ('black box-effect'), complexity, unpredictability and partially autonomous behavior, which make it hard to verify compliance with, and may hamper effective enforcement of rules of existing EU law meant to protect fundamental rights.[14]

Further, enforcement authorities and affected individuals may lack the appropriate means to verify how a specific decision was taken, and therefore whether the relevant rules were respected. As a result, individuals may face particular challenges with effective access to justice situations, and other cases that may negatively impact them. The risk for safety and the effective functioning of the AI liability regime may itself present a safety risk for users- certain risks are limited to using specific products or services that rely on AI (e.g. autonomous vehicles), whereas others are indirect in the sense that the user may be using apps that integrate AI technology in certain layers of the developing stage.

[14] European Commission, 'White Paper on Artificial Intelligence- A European approach to excellence and trust' (19 February 2020) < https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf > accessed 03 November 2020

When it comes to market surveillance and enforcement powers, authorities find themselves in a situation where they are unclear as to whether they can intervene since they do not have the same know-how, and there is an intrinsic ambiguity surrounding the authorities' competence and jurisdiction. Also, the nature of AI technology is such that "traditional" liability models would hardly work in this context.

For instance, according to the EU Product Liability Directive, a manufacturer is liable for damage caused by a defective product. In the case of AI, such as autonomous cars, it may be difficult- if not impossible- to determine what is exactly the incurred damage and whether there is any causal link that can lead to successful legal defense in a court of law. Additionally, there is uncertainty about how and to what extent the Product Liability Directive applies in the case of certain defects, for instance if there is weak cybersecurity of a product.

The difficulty to trace the different actors and identify who is doing what, in an interesting twist of the Turing test since now all the parties in the chain are active, means that it is challenging both to identify the chain of events, the chain of liability, the harm suffered, and the appropriate legal approach.

Therefore, countries need extensive legislation regarding product safety and liability, including sector-specific elements that complement national legislation where this is inadequate. This also means that countries should be in a position to adapt their strategies and adjust them to the new technological challenges. Legislation that furnishes equality across a number of sectors, like employment and occupation, should transcend the legal obligations and the ethical guidelines that AI developers should

enforce when they train AI algorithms. In essence, countries need a flexible yet robust regulatory toolkit that will not hamper innovation while it will protect equality and privacy.

Approaches vary depending on the territory in question. For instance, in the EU individuals (known as "data subjects") have certain rights in connection with data processing because of the General Data Protection Regulation (GDPR). Also, general EU laws, like the Charter for Fundamental Rights and the broader in scope European Convention on Human Rights, provide high-level guidance as to how AI algorithms should work in practice. For instance, consumer protection rules permit EU individuals to request compensation in case of a certain discriminatory behavior that may be triggered by AI algorithms (e.g. price discrimination based on a user's IP address).

Countries also introduce stand-alone safety standards and protocols to ensure that data is processed in a lawful and proportionate manner. That said, countries are in the process of using AI algorithms in an increasing fashion for policing and other activities. For instance, the EU Cybersecurity Agency (ENISA) has assessed the threat landscape for AI and has suggested a common approach for companies doing business in Europe.[15]

A key issue is whether countries should have a specific regulatory framework on AI intelligence. Such framework should apply to products and services relying on AI. In any new legal instrument, AI needs

[15] ENISA, 'ENISA working group on Artificial Intelligence cybersecurity kick-off' (10 June 2020) < https://www.enisa.europa.eu/news/enisa-news/enisa-working-group-on-artificial-intelligence-cybersecurity-kick-off > accessed 03 November 2020

to be sufficiently flexible to accommodate technological progress while being precise enough to provide the necessary legal certainty.

3. Main Legal Issues

3.1. Anonymized or Personal Data?

One of the key discussions revolving around AI regulation is whether AI relates to anonymized or to personal data. According to the General Data Protection Regulation (GDPR) (Art. 4(1)), "*personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is 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*".

The General Data Protection Regulation (GDPR) in the EU does not apply to anonymized data, whereas it applies to personal data or to pseudonymized data. According to the GDPR (Art. 4(5)), "*Pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*." The concept of personal data in the EU is quite broad, meaning that the

threshold of claiming that certain data is anonymized, and therefore not subject to the GDPR, is quite hard to hit.

Data is only considered anonymous when it is impossible to re-identify a user by processing it, alone or jointly with other data elements. This means that it is a dataset of values that cannot lead to the re-identification of an individual (e.g. random dataset that includes only age groups of an e-commerce website's visitors for statistical purposes). Anonymized data can still be useful for analytics and product improvement purposes, however it cannot lead to the identification of an individual.

However, anonymization can be a moving target. Seemingly anonymized datasets can be reversed when the computer gets "too" smart. In the example above, AI capabilities would potentially allow a computer to re-identify an individual from datasets that are seemingly anonymized. For instance, mass computational power would mean that a computer combines anonymized datasets that include age of users, postcode, and gender, and manages to re-identify individual users with a high precision rate. For instance, a study revealed that 99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes. This demonstrates that even heavily sampled anonymized datasets may not practically satisfy the GDPR anonymization standards.[16]

AI systems can overall be effective in re-identifying an individual by, e.g. cross- referencing available datasets. This may sound like a paradox, since in principle anonymized data means that the data cannot

[16] Luc Rocher, Julien Hendrickx and Yves-Alexandre de Montjoye 'Estimating the success of re-identifications in incomplete datasets using generative models' (2019), Nature Communications 10 < https://www.nature.com/articles/s41467-019-10933-3> accessed 03 November 2020

be re-identified as such, however it is an increasingly present issue/dilemma that AI programmers face. To that extent, certain jurisdictions consider the re-identification of anonymized datasets to be a criminal offence, even if it is unintentional (e.g. UK Data Protection Act 2018 S. 171).

3.2. Potential Conflict between AI and Core Privacy Principles

The notion of AI revolves around innovation, constant progress, and adjustability to processing operations towards efficiency. In that regard, a question is whether a purpose can be always determined prior to the processing of AI. How can we explain the ever-changing results according to the personal data collected, and its volume?

Further, companies may not want to fully disclose how the personal data is processed. This may conflict with the general principle of transparency in data protection law, however trade secrecy and the difficulty of explaining a prediction based on an AI algorithm using machine learning is of relevance. This means that privacy notices must be carefully reviewed, while in other cases it may be impossible to provide a full privacy notice and a thorough explanation about the decisions made using an algorithm.

3.3. Data Minimization and Purpose Limitation

The GDPR requires that only “adequate, relevant and limited” personal data can be processed in connection with certain purposes of processing. The wealth of AI capabilities seems in contradiction

with purpose limitation, i.e. data can be processed for declared purposes only. AI in principle deals with massive data volumes and revolves around the idea that mass data volumes will contribute to further processing capacity and otherwise used for training purposes. Limiting the data processing activities is intrinsically against the very notion of purpose limitation. This apparent contradiction must somehow be dealt with in practice.

Any secondary purpose that was not envisaged during the initial data collection (e.g. use of medical images for patient monitoring apart from diagnosis) needs to be GDPR compliant (e.g. obtain new consent or relevant). Again, this can be particularly challenging for algorithms since they may develop a certain degree of independence regarding how they process data, or they may expand to other processing activities depending on certain findings they have. This means that it is virtually impossible to a priori envisage the exhaustive list of processing purposes in an AI context. This does not necessarily mean that AI can then not be used, it is rather an issue of setting the appropriate boundaries.

3.4. Legal Basis for Processing

It is unclear, considering the voluminous amounts of data processed by AI and the various sources, how one can determine whether the personal data was lawfully collected. AI is based on the concept of considerable data flows and vast processing operations. The question then becomes, if the data subject was not clearly informed, how can he or she possibly give informed and free consent?

Further, the GDPR requires controllers to undertake Legitimate Interest Assessments describing the limit of legitimate interest for processing activities, and balancing whether the business interest of the controller overrides the data subject's interest.

3.5. Privacy by Design and Privacy by Default

Every controller needs to implement appropriate technical and organizational measures integrating necessary safeguards into the processing. In practice, AI algorithms must be designed in a way that respects these principles- this will naturally limit the amount of data that can be lawfully processed. In line with the above notions of privacy by default and privacy by design, the amount of data which will be processed will be limited.

Every AI application must intrinsically consider data protection, information security, and rights fulfilment. This will certainly require more hours of programming, and a more stringent approach altogether.

3.6. Profiling

Algorithms can trigger automation and technological progress, yet as a tool they can be used for profiling purposes. They can decipher an individual's preferences, predict behaviors and/or make decisions that may overall impact individuals' rights and interests.

Data subjects, in principle have the right to be informed and be provided with adequate justification regarding an automated decision. This includes profiling (e.g. on disease prediction, health monitoring etc.). However, providing such meaningful notice and justification may become increasingly difficult, while the more AI's uses expand, the more challenging any relevant guidance becomes.

The natural question is what happens when AI becomes so complex and processes such voluminous data that a justification cannot be given. How will controllers or processors, in practice, deal with this issue? Also, how will data subjects' rights be respected?

3.7. Data Subject Rights

Users have several rights regarding the processing of their personal data (e.g. access, erasure, restriction, objection, correction, transmission). In cases of big data analytics and relevant oceans of data, it may be particularly challenging, if not impossible, for AI applications to fulfil such rights (e.g. erase x-rays and their output data over several datasets).

Some critics postulate that it is practically impossible to fulfil those rights, and that they cannot be in principle and in practice honored. Also, in cases where data is arguably anonymized, or pseudonymized, several stakeholders may need to be contacted and involved in order to respond to a data subject request.

In any case, Standard Operating Procedures need to be in place to effectively handle requests and respond timely. The GDPR requires controllers to respond to data subjects within one month of receipt of a request- this can be further extended by two months if the request is particularly complex. In theory, controllers dealing with AI could invoke this provision, however it is still uncertain how it could play out in practice.

3.8. Data Transfers

Companies need to have an adequate transfer mechanism in place to transfer data outside the EU to third countries that have not been found adequate by the European Commission. Options include Standard Contractual Clauses, however it is particularly difficult, if not impossible, to use those in a B2C context. In practice, companies may find themselves in a difficult position when transferring data abroad.

This is particularly alarming in light of the recent invalidation of the EU-US Privacy Shield Framework in connection with the Schrems 2 ruling.[17] AI requires vast amount of data being transferred cross-border, and as such companies should have the appropriate legal tools to facilitate such data transfers. Otherwise, we could end up with a situation whereby data is localized, and therefore progress equally localized, leading to global divergence instead of technological convergence.

3.9. Licensing Agreements

Licensing agreements with customers typically include confidentiality and data protection clauses. To that extent, entitlement and ownership of data is paramount, while the right to resell medical data sourcing from another algorithm may be difficult if it includes personal data. Companies need to strategize and decide how much they control the process, if at all, and their entitlement altogether.

3.10. Data Breach

[17] Court of Justice of the European Union, 'The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield' (16 July 2020) < https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf > accessed 03 November 2020

In case of a data breach, companies may need to notify the competent regulator (supervisory authority) and the individuals affected by the breach, particularly for sensitive data. The data breach notification is time sensitive and, in principle, needs to happen within 72 hours of becoming aware of the breach. The increasing complexity of Artificial Intelligence may make it difficult, if not impossible, in practice to determine when a cyberattack or data breach has taken place. The threshold of a breach of security that leads to unauthorized processing, unless it is unlikely it will result to risks to the rights and freedoms of individuals, is of particular relevance.

Further, it may be challenging to provide a meaningful notification to the regulator since it is difficult to decipher what led to the breach, what type of information was involved, the potential risk to the individuals, measures taken or proposed to be taken to mitigate the negative consequences of the breach.

3.11. Data Protection Impact Assessment

As part of their accountability obligations when processing data or being involved in new types of processing operations, a company may be required to undertake, or assist with, a Data Protection Impact Assessment.

This assessment requires careful thinking and planning around the use of the algorithm, the risk it creates for privacy, and ways to mitigate such risk. In cases where risk cannot be mitigated, companies will need to seek advice from the competent Supervisory Authority.

3.12. Retention

The GDPR requires, apart from certain exceptions, that Companies delete data when the purpose for which it has been collected elapses. Data retention obligations are by nature contradicting with the concept of AI where data is processed infinitely. This also relates to particularly complex obligations in cases of secondary and/or new processing purposes.

Further, companies need to decide for how long they will keep the data and compile data retention schedules, unless they can prove their data is anonymous.

3.13. Liability

The question of liability is paramount for companies that want to plan ahead, as well as for consumers and other parties affected by this. Cases where liability may be relevant sound remote, however they are much closer than in theory- for instance, who is liable when someone gets injured and the care involves a medical algorithm? Is it the doctor, the hospital that ended up implementing the algorithm, the manufacturer of the algorithm? Perhaps a combination?

This is one of the most complicated questions when it comes to AI and liability. There are two relevant types, privacy liability and product liability.

Privacy liability refers to any GDPR related violations resulting from the use of AI (e.g. re-identifying anonymized data, secondary use of data without valid legal basis, violation of data subject rights etc.). Privacy liability may give rise to administrative fines (including cease and desist for processing activities, 4% of global revenue or $23m., whichever is higher). This does not exclude potential civil and/or criminal sanctions.

On the other hand, product liability typically relates to strict-liability (for contractual obligations where the promise between the parties needs to be honored) or to fault-based liability (in tort obligations when the harm occurs). The above become particularly relevant in complicated cases (i.e. cases where black box algorithms, that is open source algorithms, may be involved in the process).

Overall, the present concepts of liability can be defective in AI since there is no promise (i.e. no contractual liability) whereas the use of black-box algorithms may impose an undue burden to the manufacturer that was never foreseen (i.e. no tortious liability). Hybrid types of liability may become popular in the future (e.g. fiduciary law can be flexible and change as the relationship between parties evolves).

4. EU Regulation on AI

Latest AI Developments

The European Union (EU) is crafting legislation under the guidance of the European Strategy on Artificial Intelligence, supported by a High-Level Expert Group on Artificial Intelligence. The European Commission also recently published its Ethics Guidelines for Trustworthy Artificial Intelligence (AI), following the Policy and investment recommendations for trustworthy Artificial Intelligence in June 2019.

Further, the European Commission launched the pilot phase of the ethics guidelines for trustworthy AI in July 2019. The ethics guidelines include specific checklist items that companies can use when deciding whether to deploy an AI algorithm.

Trustworthy AI principles, in the pilot form, include:

- Human agency and oversight;
- Robustness and safety;
- Privacy and data governance;
- Transparency;
- Diversity, non-discrimination and fairness;
- Societal and environmental well-being;
- Accountability.

The European Commission published its updated AI factsheet in July 2019, fleshing out elements like AI's financial importance, a roadmap for AI's implementation, how much the Commission will invest on AI, and project examples.

AI applications that are not considered as high-risk could be governed by a voluntary labeling scheme. With regard to compliance and enforcement, the Commission considers prior conformity assessments, which includes 'procedures for testing, inspection or certification' and/or 'checks of the algorithms and of the data sets used in the development phase'.

The Commission's AI high level expert groups presented its AI recommendations during the European AI Alliance. The recommendations included endorsements to empower and protect humans and society; adopt a tailored approach to the AI market; secure a single European Market for trustworthy AI; enable AI ecosystems through sectoral multi-stakeholder alliances; foster the European data economy; exploit the role of the public sector.

Also, in February 2020 the European Commission published its White Paper on "Artificial Intelligence- A European approach to excellence and trust".[18] The White Paper discusses the notion of the ecosystem of excellence and an ecosystem of trust. The Commission differentiated between high-risk and non-high-risk AI applications. Only high-risk activities should be in scope of a future EU regulatory framework. Further criteria refer to how risky the processing activity is. The following key requirements are considered for high-risk AI applications: requirements for training data; data and record-keeping; informational duties; requirements for robustness and accuracy; human oversight; and specific requirements for specific AI applications, such as for purposes of remote biometric identification.

The European Commission's new president, has repeatedly referred to the role of AI and big data in making EU's single market fit for the digital age.[19] The European Commission's science and knowledge service published a report revolving around blockchain. The report discusses the interplay

[18] Also of relevance is the independent ethics guidelines on High-Level Expert Group on Artificial Intelligence set up the European Commission: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top

[19] Press remarks by President von der Leyen on the Commission's new strategy: Shaping Europe's Digital Future: https://ec.europa.eu/commission/presscorner/detail/en/speech_20_294

between blockchain and key digital technologies, like AI. It also uses the example of healthcare AI as an emerging field.

Finally, the European Commission has expressed its intent to develop AI-related guidance on the interpretation of the Product Liability directive. All these initiatives are still in the making, however they denote the EU's willingness to regulate, and be at the forefront of technological innovation regarding AI.

5. US Regulation

Discussions on regulation of AI in the United States have included topics such as regulating AI as a technology, the nature of federal regulatory framework to govern and promote AI, including the competent authority and its role, and the overall update of regulations to reflect the latest updates and the challenges introduced by AI. US lawmakers have mainly pursued AI in the area of autonomous or self-driving vehicles. The Department of Transportation has considered the use of such vehicles, whereas recent federal legislation has tasked part of the Department of Defense with the responsibility of crafting policies to develop and deploy AI systems as they concern national defense.

Federal Legislation

Recently, the US has been issuing increasing reports discussing and dealing with issues of Artificial Intelligence. In 2015-2016, for example, the 114th Congress saw two bills containing the term "artificial intelligence", which increased to 42 bills with the 115th Congress (2017-2018) and to 51 bills for the

116th Congress. Similar trends relate to the state and city levels. As of early November 2019, the trend is increasing.[20]

In the 115th Congress, thirty-nine bills have been introduced containing the phrase "artificial intelligence" in the bill. Four of these have been enacted into law. Section 238 of the John S. McCain National Defense Authorization Act[21] directs the Department of Defense to undertake several activities regarding AI. Subsection (g) provides the following definition of AI:

(g) ARTIFICIAL INTELLIGENCE DEFINED—In this section, the term "artificial intelligence" includes the following:

(1) Any artificial system that performs tasks under varying and unpredictable circumstance without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.

(2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.

(3) An artificial system designed to think or act like a human, Including cognitive architectures and neural networks.

---

[20] Y. Chae, The Journal of Robotics, Artificial Intelligence & Law, (2020) Vol. 3 (No.1)

[21] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232, § 238, 132 Stat. 1658 (2018), https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf.

(4) A set of techniques, including machine learning, that is designed to approximate a cognitive task.

(5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

In 2018, Congress also advised the Federal Aciation Administration to periodically review the state of AI in aviation and take steps to address these developments.[22]

State Legislation

In 2011, Nevada adopted the first legislation concerning the testing of autonomous vehicles.[23] The law defines autonomous vehicle as restricted to the operation of "the motor vehicle without active control or monitoring of a human operator". The law also sets forth requirements for the testing of such vehicles, and directs that regulations be issued governing their operation (NEV. REV. STAT. § 482A).

In 2012, Florida and California adopted similar legislation regarding testing and operation of autonomous Vehicles.[24] Also, California had 0 bills for AI in (2015-2016), five bills during the last term (2017-2018) and 13 bills for the current legislature (2019-2020).

---

[22] FAA Reauthorization Act of 2018, Pub. L. 115-254, § 548, 132 Stat. 3186, <https://www.congress.gov/115/bills/hr302/BILLS-115hr302enr.pdf> accessed 03 November 2020

[23] Bryant Walker Smith, 'Autonomous Vehicles Are Probably Legal in the United States', (2014) 1 TEX. A&M L. REV. 411, 501.

[24] Library of Congress, 'Regulation of Artificial Intelligence: The Americas and the Caribbean' (2019) <https://www.loc.gov/law/help/artificial-intelligence/americas.php#_ftn86> accessed 03 November 2020

Recent Developments

The first relevant report was the US National Strategic Research and Development Plan for Artificial Intelligence. In January 2019, following an Executive Order on Maintaining American Leadership in Artificial Intelligence, the White House's Office of Science and Technology Policy released a draft Guidance for Regulation of Artificial Intelligence Applications, including ten principles for United States agencies when deciding whether and how to regulate AI.

The ten relevant principles are:

- Public Trust in AI.
- Public Participation.
- Scientific integrity and information quality.
- Risk Assessment and Management.
- Benefits and costs.
- Flexibility.
- Fairness and non-discrimination.
- Disclosure and transparency.
- Safety and Security.
- Interagency Coordination.

In that vein, the National Institute of Standards and Technology released a position paper, the National Security Commission on Artificial Intelligence published an interim report, and the Defense Innovation Board issued recommendations on the ethical use of AI.

Recently, the Executive Order ("EO"), "Maintaining American Leadership in Artificial Intelligence", was followed by a federal government strategy for Artificial Intelligence (the "AI Initiative"). Among others, the AI initiative aims to empower federal agencies to drive breakthroughs in AI research and development (R&D). This includes making data computing resources available to the AI research community to establish technological standards and to provide guidance on regulatory approaches.

The EO is part of another 18 countries' national AI strategies. The EO attempts to "sustain and enhance the scientific, technological, and economic leadership position of the United States in AI R&D and deployment", taking into account five pillars:

- Research and Development: The U.S. must drive technological breakthroughs in AI across the federal government, industry, and academia;
- Standards and Resources: The U.S. must drive development of technical standards and reduce barriers to the safe testing and deployment of AI technologies;
- Workforce: The U.S. must train current and future generations of American workers with the skills to develop and apply AI technologies;
- Governance: The U.S. must foster public trust and confidence in AI technologies and protect civil liberties, privacy, and American values in their application; and
- International Engagement: The U.S. must promote an international environment that supports American AI research and innovation and opens markets for American AI industries, while protecting the United States' technological advantage in AI.

New Guidance for Regulations of AI Applications

The EO details initiatives to promote public trust in the development and use of AI applications, while fostering innovation. The EO directs the OMB director, in coordination with other key stakeholders, to issue within six months a memo that (i) informs the development of regulatory and non-regulatory approaches regarding technologies and industrial sectors and (ii) consider ways to reduce barriers to the use of AI technologies in order to promote their innovative application.

Further, the EO directs the National Institute of Standards and Technology ("NIST") to issue plans for developing "technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies". The idea is to identify opportunities and challenges regarding establishing US leadership in the AI standards.

6. Next Steps

As exhibited above, both the EU and the US are in a transitional stage where they are moving towards regulating AI. The White House has encouraged the European Commission to consider using this Guidance as a model when drafting pending AI regulatory documentation. The EU is also being very vocal about the importance of AI and how it can transform its economy.

Notwithstanding the willingness to take advantage of AI's capabilities, this technology comes with certain privacy concerns. Time will tell whether EU and US regulation will be effective and at the same time incentivizing so that we do not inhibit AI's growth, while maintaining our fundamental rights.