AI and Data Security: A Euro-American Dialogue for a New Era of Regulation

Robert I. Field

In the short time since Artificial Intelligence (AI) emerged as a broadly available and widely utilized technology, it has begun to transform almost every kind of human activity. As the typewriter replaced handwriting and the pocket calculator replaced arithmetic calculations, AI is altering fundamental cognitive tasks, but it is doing so on a much larger scale. Everyone with a computer can use a number of applications to analyze complex problems based on information gleaned from across the Internet. These applications can not only analyze existing information but also generate entirely new resources based on it, ranging from legal documents to works of fiction to computer code.

Beyond applications for individuals, in the commercial sphere, businesses and professionals are seeing even more consequential uses. In manufacturing, to take one area, AI can detect product defects, program self-driving cars, and predict energy demand. In entertainment, to take another, it can analyze individual preferences, profile consumption behavior, and promote a company's favored content. In medicine, it can help radiologists to read images, oncologists to customize treatments, surgeons to guide robotic procedures, and health systems to manage essential administrative tasks. With its reach into the personal and commercial spheres, AI is touching almost every aspect of our lives.

However, along with its growing array of uses, AI brings risks that are equally profound. AI systems are trained on massive troves of data, some of which may be highly personal or proprietary. They can use the data against the wishes, or even knowledge, of data subjects. Even with information that is legitimately obtained, AI can perform functions that raise serious ethical concerns. Employers can use it to monitor minute aspects of workers' personal behavior and to select job applicants based on characteristics unrelated to objective qualifications. In the United States where employers often bear the burden of providing health insurance for their workers, it can screen job applicants based on predictions of claim costs for them and their family members. Police can use it to profile individuals based on facial features and then monitor the activities of those individuals even if they have never committed a crime. Banks can use it to predict the credit worthiness of loan applicants even if they have never encountered financial difficulties. To compound these concerns, AI analyses of actual and predicted behavior can be not only intrusive but erroneous, leading to devastating consequences for the individuals involved.

Beyond the risks to individuals, governments can use AI in nefarious ways, such as monitoring their citizens' political leanings and activities. They can use it against adversaries to manipulate populations with misinformation. In the near future, data derived from two new highly intrusive technologies, genetic profiling and brain monitoring, may enable governments to use AI to encroach on individual privacy and autonomy in even more fundamental ways.

However, while risks such as these are universal, sensitivity to them is not. It varies with social context, which in turn varies between countries, leading to differences in legal responses. Such disparity is evident in the AI policies of two jurisdictions that have been especially active in its development and oversight: the European Union (EU) and the United States (US).

In May 2025, universities in three countries in the EU and US convened a conference to explore

AI's social challenges and legal responses in these two jurisdictions entitled *AI & Data Security: A Euro-American Dialogue for a New Era of Regulation*. The host universities were Università degli Studi di Milano-Bicocca in Italy, Universite de Rennes in France, and Drexel University in the United States. This issue of *BioLaw Journal* presents the perspectives of nine speakers at that conference. Their articles present viewpoints on a range of aspects of AI from theoretical considerations based on legal philosophy to detailed considerations of existing laws and their effects.

Silvia Salardi considers the nature of AI from the viewpoint of analytical legal philosophy, using linguistic analysis to clarify the meaning of concepts. She discerns three different yet interrelated kinds of languages: institutional and political, legal, and ordinary discourse. It is through these linguistic forms that deep transformations of society are expressed and through which societal changes are collectively and individually perceived and experienced. Control over language and the concepts they express thereby forms an important guide to these transformations that is in line with a fundamental rights framework.

Carla Gulotta describes a study that seeks to enhance understanding of the effectiveness of the EU's normative framework in its response to AI. That framework seeks to shape a digital society in which AI systems do not endanger respect for fundamental rights and democratic values. Europe has prioritized these rights and values in its social and legal order since the end of the Second World War. The study will generate observations on the kinds of legal tools that might better shape a rights-oriented society capable of capitalizing on AI without compromising basic values. The study's analysis will emphasize the precautionary principle to inform the innovation process.

Jordan Fischer explores the different attitudes of the EU and US as the two dominant jurisdictions regulating AI, which was a central theme of the conference. She considers how each jurisdiction has approached AI regulation and the legal frameworks they have produced. Their experiences may hold lessons for the next wave of AI development and oversight.

Erwann Picart-Cartron describes administrative procedures before the EU's supervisory authority and the authority's ability to act under liability law and under the EU's two main laws regarding AI and data security: the AI Act and the General Data Protection Regulation (GDPR). On the one hand, the supervisory authority has a somewhat contradictory role as it operates at the intersection of market regulation and the protection of fundamental rights, combining both ex-ante and ex-post powers. On the other hand, liability law must also be considered as a tool for ensuring the enforcement of these regulations, especially given its preventive function. By analyzing these remedies, he highlights the importance of the GDPR as a key component in ensuring the effectiveness of the AI Act and points to ways in which AI requires a new perspective on data protection law.

Elena di Carpegna Brivio examines the relevance of the constitutional concept of dignity in the digital society. Digital technologies are redefining the concept of human personality, employing a quantitative approach that considers human behavior through a statistical lens. The idea of dignity can be a useful tool for creating a new approach to juridical reasoning by drawing a continuous line through a person's physical, psychic, relational, and digital existence, and continuing that line to the AI Act. This reasoning could underly the beginning of a new regulatory philosophy of technological development that would be more anthropocentric.

Giovanni Zaccaroni considers media freedom and argues that AI poses both challenges and opportunities for the media in Europe. EU legislation, including the Media Freedom Act, the AI Act, and the Political Advertising Regulation, along with the European Charter and European Convention on Human Rights, seek to protect media pluralism and democracy amid rapid digital transformation. AI's growing role in content creation and distribution raises concerns over media autonomy and editorial independence, and these laws aim to promote transparency, AI literacy, and safeguards against undue influence. He argues that cooperation between the EU and the Council of Europe through frameworks such as the AI Convention is especially important in creating a safe approach to innovation that promotes digital autonomy.

Marta Sosa Navarro analyzes the implications of neurotechnologies used in the workplace for international human rights principles and labor law. She distinguishes between brain-reading devices, which process neural data and implicate the rights to privacy and to freedom of thought, and brain-altering technologies, which have the potential to affect mental integrity. Mapping the international, regional, and International Labor Organization frameworks, she highlights gaps in protection created by fragmented regulation. She argues that the precautionary principle, soft-law instruments, and anticipatory regulation are essential to address these challenges and concludes that safeguarding dignity in the digital workplace requires a principled and proactive governance model to prevent cognitive surveillance and exploitation.

Francesca Mattassoglio describes an important ruling of the European Court of Justice on AI techniques for calculating credit scores. She sees the ruling as especially helpful as a guide, because the judge addressed the activities of specific credit-scoring companies, including Germany's Schufa and the US's Dun & Bradstreet. Similar disputes that require courts to weigh the interests of parties whose scores are calculated against those of the companies that calculate those scores will likely increase over the next few years. In adjudicating them, judges will have to balance the right of individuals to maintain control over their information with the right of companies to use algorithms as an efficient way to analyze it.

Philippe Pierre describes the responsibilities of legal professionals concerning the use of digital technology. He observes that the nature of responsibility for proper use of digital tools is far from clear. In most cases, the use of digital tools will prove neutral for the legal professionals' commitment to responsible conduct, as it leaves unchanged both the paradigm of good professional practice and the protection of clients. Nevertheless, in some circumstances, the digital environment may expand this responsibility in ways that may paradoxically work to the benefit of the practitioner. This will be the case, for example, for the two classic sources of liability for legal professionals: failing to provide advice and committing legal errors.

With this range of perspectives, this issue of BioLaw Journal represents an important resource for understanding the unique legal and societal challenges posed by what may be the most consequential new technology of our time. It is especially valuable in assessing the contrasting approaches of two of the most important jurisdictions in regulating it. Such an analysis is essential if a harmonized global strategy for maximizing the benefits of AI while minimizing the risks is to be achieved.