Istituto Affari Internazionali

ISSN 2532-6570

IAI COMMENTARIES 24 | 58 - OCTOBER 2024

Balancing Privacy and Innovation in AI Adoption across the G7

by Ettore Greco

The accelerating development of artificial intelligence (AI) systems has stirred up the public debate around the most effective approaches and instruments to safeguard personal privacy. The unprecedented risks that AI poses to privacy rights require that policymakers and legislators conduct a thorough review of the existing measures and normative frameworks aimed at data protection. Most of them were established before the recent rise of AI and need, therefore, to be partly reconsidered. The rapid expansion and pervasiveness of AI, which is applied to almost every industrial sector with far-reaching social implications, make such a review a daunting challenge.

A far-sighted proactive regulatory approach that takes into consideration possible future developments of AI technologies can be seen as the most appropriate. In practice, however, this approach is hard to pursue due to the extreme difficulty, at least at this stage, in predicting the trajectory of AI systems. In dealing with the impact of AI on data privacy, regulators should therefore apply a great deal of flexibility based on a continuously updated understanding of the ongoing technological dynamics in the AI realm.

The existing consolidated body of human rights principles, of which respect for personal privacy is a key part, remains the essential source of inspiration for any regulatory effort and enforcement action. Preventing technological advancement from compromising privacy rights or eroding long-lasting commitments to protect fundamental rights of citizens should be a top priority for decision-makers. The challenge is how to obey such imperatives while avoiding to stifle innovation that can potentially bring great benefits for citizens' welfare and everyday life.

Privacy risks and regulatory challenges

Privacy risks have long been under the limelight especially after the advent of

Ettore Greco is Executive Vice President of the Istituto Affari Internazionali (IAI) and also Head of the Multilateralism and Global Governance programme of the institute.

commercial internet that makes ample use of data collection and processing. The rise of AI has greatly deepened concerns about data privacy.

Gargantuan amounts of data are collected and generated by AI systems. To feed and train their datasets, technology platforms aggregate information from a wide spectrum of sources such as traditional and social media, websites, internet navigation and shopping, and smartphone data. As a result, the individuals' control over how their personal data are collected and used is continuously at risk. By scraping personal data to train algorithms, platforms may disclose or memorise information about a person's life without their consent. This may facilitate, for example, phishing attacks, identity theft, or distorted uses of facial recognition, and introduce or reinforce bias in the screening of job candidates, the provision of benefits or loan granting.

Effective protection of personal data in the use and development of AI technologies requires rules and mechanisms that enable users to exercise adequate control on how their data are collected, stored and processed, and bind companies to delete data that can be misused. This is indeed the focus of the regulatory efforts undertaken by countries and international organisations, as will be discussed below.

Regulating AI also requires deeper attention to the whole data ecosystem that feeds AI. The supply chain for the data includes different stages, from data collection to the development of pre-trained models to the refining and optimisation of those models for specific tasks and applications. Understanding how data is handled at each stage of the AI supply chain is crucial to identifying the most appropriate mechanisms to improve AI models, ensure privacy protection and avoid bias. So far, the debate on AI regulation, both in the US and in the EU, has focused on transparency requirements regarding algorithmic systems, with scarce attention being paid to the data lifecycle. Filling this gap may help not only devise better methods and procedures to grant individuals greater control over their personal data but also distribute roles and responsibilities between AI developers and deployers.

An essential first step is removing or obfuscating personally identifiable information from training datasets. Measures of access control are also fundamental to ensure that only authorised personnel can access and process sensitive data. Checks for algorithmic fairness and bias can help prevent AI models from making decisions that unfairly impact particular groups or individuals. Testing for demographic parity, equal opportunity and other fairness metrics is important. Transparency of AI models can facilitate audit decisions on data protection. There is also the need for continuous monitoring of AI models to prevent violation of privacy or unintended use of sensitive data.

Technological innovation can also play a significant role in establishing more secure AI development and deployment practices and implementing effective

IAI COMMENTARIES 24 | 58 - OCTOBER 2024 ISSN 2532-6570

measures tailored to specific AI systems and processes. Notably, the US government has mandated federal agencies to use privacy-enhancing technologies to protect personal information, acknowledging that they have the potential to ensure more effective handling of sensitive personal data.[1]

Regulatory efforts and cooperation initiatives

As the EU and US share fundamental human rights principles, regulatory alignment across the Atlantic on protection of personal privacy in the development and use of AI may seem a realistic prospect. However, Washington and Brussels have adopted considerably different approaches to AI regulation in general, and privacy protection in particular. While the EU's regulatory process has produced several pieces of legislation, the US has so far opted for voluntary guiding principles.

The US government has shied away from imposing federal privacy rules on the handling of AI-driven data. The Executive Order on Safe, Secure and Trustworthy Development and Use of Artificial Intelligence issued by the White House in October 2023 simply calls on Congress to pass bipartisan data privacy legislation, while mandating federal agencies to develop guidelines to evaluate the effectiveness of existing privacy-preserving mechanisms in the AI realm.[2]

By contrast, the EU has enacted an articulated and robust legislative body on data governance and privacy risks associated with AI, including the General Data Protection Regulation (GDPR),[3] the most comprehensive legislative piece on privacy in the world, and the Artificial Intelligence Act (AI Act),[4] enacted in July 2024, which provides a risk-based approach banning the most harmful AI systems. The transatlantic dialogue on AI regulation has developed in various frameworks, notably within the Trade and Technology Council (TTC). The TTC is working on the implementation of a joint roadmap to establish common AI benchmarks and standards based on a large convergence on fundamental principles, including those related to personal privacy.[5]

The G7's major achievement so far has been the approval of Guiding Principles on Artificial Intelligence and a voluntary

[1] White House, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 October 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[2] Ibid.

[3] European Council website: *The General Data Protection Regulation*, https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation.

[4] European Parliament and Council of the European Union, *Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, http://data.europa.eu/eli/reg/2024/1689/oj. See also the website developed by the Future of Life Institute: *EU Artificial Intelligence Act*, https://artificialintelligenceact.eu.

[5] Trade and Technology Council (TTC), *TTC Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management*, 1 December 2022, https://digital-strategy.ec.europa.eu/en/node/11380.

ISSN 2532-6570

Code of Conduct for AI developers under the so-called Hiroshima AI process launched by the Japanese Presidency of G7 in 2023.[6] Privacy protection is emphasised as a central principle in both documents. The G7 has focused, in particular, on data privacy in the context of transborder flow of data, a key aspect of data governance that requires, by definition, close international cooperation. The operationalisation of the Data Free Flow with Trust (DFFT) concept, first launched by former Japanese prime minister Shinzo Abe in 2019, which aims to reconcile the promotion of free flow of data across borders with the protection of individual privacy, has become a central subject of dialogue within the G7.[7]

Of paramount importance is also the OECD's research and standard-setting work. The OECD's AI principles, initially adopted in 2019 and updated in May 2024, to which 46 countries have adhered, emphasise international cooperation to promote AI regulation, including in order to preserve personal privacy.[8] The OECD has provided the platform for confronting stakeholders' perspectives on how various jurisdictions have addressed AI's privacy challenges and for promoting a dialogue between the AI and privacy communities. In July 2024, the OECD also started a pilot phase to monitor the application of the G7 Code of Conduct.[9]

All major regulatory initiatives to deal with privacy risks associated with AI have been accompanied by a dialogue with AI actors and stakeholders. Such a dialogue is key to identifying the privacy risks and the possible technical and regulatory measures to address them. In July 2023, seven leading AI companies announced at the White House their adherence to eight voluntary commitments on how to develop AI in a safe and trustworthy way.[10] The document includes the promise to improve the testing and transparency of AI systems and to provide information on emerging risks.[11] Self-regulation processes such

[6] G7, *Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems*, 30 October 2023, https://digital-strategy.ec.europa.eu/en/node/12130.

[7] G7 Digital and Technology Ministers, *G7 Digital and Technology Track – Annex 2: G7 Roadmap for Cooperation on Data Free Flow with Trust*, 28 April 2021, https://g7.utoronto.ca/ict/2021-annex_2-roadmap.html; Aidan Arasasingham and Matthew P. Goodman, "Operationalizing Data Free Flow with Trust (DFFT)", in *CSIS Briefs*, April 2023, https://www.csis.org/node/104969.

[8] OECD AI Policy Observatory website: *OECD AI Principles*, https://oecd.ai/en/ai-principles.

[9] OECD, *OECD Launches Pilot to Monitor Application of G7 Code of Conduct on Advanced AI Development*, 22 July 2024, https://www.oecd.org/en/about/news/press-releases/2024/07/oecd-launches-pilot-to-monitor-application-of-g7-code-of-conduct-on-advanced-ai-development.html.

[10] White House, *Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI*, 21 July 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai; *Voluntary AI Commitments*, September 2023, https://www.whitehouse.gov/wp-content/uploads/2023/09/Voluntary-AI-Commitments-September-2023.pdf.

[11] For an assessment of the implementation of the commitments undertaken by the seven companies one year on see Melissa Heikkilä, "AI Companies Promised to Self-Regulate One Year Ago. What's Changed?", in *MIT Technology Review*, 22 July 2024, https://www.

IAI COMMENTARIES 24 | 58 - OCTOBER 2024 ISSN 2532-6570

as the one promoted through the White House commitments can play a crucial complementary role with respect to the regulatory efforts undertaken by governments and international organisations and significantly contribute to trust building around data handling and flow.

A complex and multi-faceted process

Building a safe and trustworthy AI ecosystem where privacy rights are adequately protected is a complex challenge that requires convergent efforts by governments, international organisations and major AI actors. Dialogue with stakeholders of the various industrial sectors has also become of growing importance as the pervasive nature of AI technologies has brought into sharp relief the ever-expanding variety of challenges and opportunities involved.

The growing concerns about the risks arising from AI developments highlight the need for new mechanisms that grant individuals increased control over their personal data and ensure greater transparency and accountability in the handling of data by AI developers and deployers.

A better understanding of the lifecycle of data collected and generated by advanced AI systems can lay the groundwork for the adoption of effective privacy-protection measures and the sharing of roles and responsibilities between AI developers and deployers.

AI advanced technologies can provide valuable instruments to enhance privacy, in particular for the handling of sensitive personal data. AI developers and deployers should make a pro-active and transparent use of available technologies that can contribute to protecting private rights through tailor-made measures.

Convergent efforts across the Atlantic to advance AI regulation remain of paramount importance. Despite their different approaches to regulation, the EU and the US have a deep-rooted attachment to human rights that facilitates cooperation on privacy issues. The Trade and Technology Council provides a valuable platform for developing common solutions at the transatlantic level that may serve as blueprints in wider cooperation frameworks.

The implementation of the G7 Code of Conduct can be another key component of international cooperation to promote innovation while protecting privacy rights through the involvement of private AI actors.

The G7 has also established as a valuable platform to promote the implementation of the DFTT initiative aimed at ensuring the free flow of data across borders through appropriate safeguards for privacy and other public interests. The operationalisation of DFTT can pave the way for greater interoperability of legal frameworks based on privacy-related criteria of trust.

9 October 2024

technologyreview.com/2024/07/22/1095193.

ISSN 2532-6570

ISSN 2532-6570

IAI COMMENTARIES 24 | 58 - OCTOBER 2024

Istituto Affari Internazionali (IAI)

The Istituto Affari Internazionali (IAI) is a private, independent non-profit think tank, founded in 1965 on the initiative of Altiero Spinelli. IAI seeks to promote awareness of international politics and to contribute to the advancement of European integration and multilateral cooperation. Its focus embraces topics of strategic relevance such as European integration, security and defence, international economics and global governance, energy, climate and Italian foreign policy; as well as the dynamics of cooperation and conflict in key geographical regions such as the Mediterranean and Middle East, Asia, Eurasia, Africa and the Americas. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*AffarInternazionali*), two book series (*Trends and Perspectives in International Politics* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via dei Montecatini, 17
I-00186 Rome, Italy
Tel. +39 066976831
iai@iai.it
www.iai.it

Latest IAI COMMENTARIES

Editor: Leo Goretti (l.goretti@iai.it)