

|                             |                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title                       | 'Red-lines': How do global legal systems respond to the risks of Artificial Intelligence?                                                                                                                                                                                                                                                                                     |
| Authors                     | Lynch, Nessa                                                                                                                                                                                                                                                                                                                                                                  |
| Publication date            | 2025-12-04                                                                                                                                                                                                                                                                                                                                                                    |
| Original Citation           | Lynch, N 2025, "'Red-lines': How do global legal systems respond to the risks of Artificial Intelligence?", Irish Studies in International Affairs, vol. 36, no. 1, pp. 1-18. <a href="https://doi.org/10.1353/isia.0.a977501">https://doi.org/10.1353/isia.0.a977501</a>                                                                                                     |
| Type of publication         | Article (peer-reviewed)                                                                                                                                                                                                                                                                                                                                                       |
| Link to publisher's version | <a href="https://doi.org/10.1353/isia.0.a977501">10.1353/isia.0.a977501</a>                                                                                                                                                                                                                                                                                                   |
| Rights                      | © 2025, the Author. This is an open access article under the terms of the Creative Commons attribution license, which permits use, distribution and reproduction in any medium, provided the original work is properly cited. Open Access funding provided by IReL. - <a href="https://creativecommons.org/licenses/by/4.0/">https://creativecommons.org/licenses/by/4.0/</a> |
| Download date               | 2026-10-31 02:41:24                                                                                                                                                                                                                                                                                                                                                           |
| Item downloaded from        | <a href="https://hdl.handle.net/10468/19477">https://hdl.handle.net/10468/19477</a>                                                                                                                                                                                                                                                                                           |



PROJECT MUSE®

---

## 'Red-Lines': How do Global Legal Systems Respond to the Risks of Artificial Intelligence?

Nessa Lynch

Irish Studies in International Affairs, Preprint Articles, (Article)

Published by Royal Irish Academy

DOI: <https://doi.org/10.1353/isia.0.a977501>



This is a preprint article. When the final version of this article launches, this URL will be automatically redirected.

➔ For additional information about this preprint article

<https://muse.jhu.edu/article/977501/summary>

# ‘Red-Lines’: How do Global Legal Systems Respond to the Risks of Artificial Intelligence?

Nessa Lynch\*

*School of Law, University College Cork*

---

## ABSTRACT

Artificial intelligence (AI) use is growing rapidly across a range of sectors, including defence, national security, policing, healthcare, education and delivery and planning of state services. There is acute concern around the impact on individual and collective human rights. Though the progress and implementation of AI has until recently far outstripped the development of regulatory systems, there are now attempts, particularly in European Union law and through the international human rights system, to constrain those uses of AI which most impact human rights. This contribution is primarily intended for a non-specialist Irish audience who wish to gain an understanding of the risks of AI to human rights and the challenges of regulating this technology. It discusses the impact of AI on human rights, regulatory approaches to limiting harm, and concludes by commenting on Ireland’s role in the global regulatory system.

## INTRODUCTION

This contribution reflects on the theme of the constraint and regulation of artificial intelligence (AI) in the contemporary international legal order. AI use is growing rapidly across a range of sectors, including defence, national security, policing, healthcare, education and delivery and planning of state services. There is acute concern around the impact on human rights and human values. Though the progress of development and implementation of AI has until recently far outstripped the development of the regulatory system, there are now attempts, particularly in European Union law and through the international human rights system, to constrain uses of AI that most impact human

---

\*Author’s e-mail: [nessa.Lynch@ucc.ie](mailto:nessa.Lynch@ucc.ie)

*Irish Studies in International Affairs*, Vol. 36, No. 1 (2025), 1–18. © 2025 The Author

This is an open access article under the terms of the Creative Commons attribution license, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.  Open Access funding provided by IReL.

rights and human values. Yet, geopolitical tensions are encouraging increased use of AI, and promoting innovation, perhaps at the expense of regulation.

The regulation and constraint of AI is a broad and multi-faceted subject, which is evolving in real time. This article is primarily intended for a non-specialist Irish audience who wishes to gain an understanding of the risks of AI to human rights and the challenges of regulating this technology. My discussion is centred around three key questions. Firstly, what are the cross-cutting global issues in relation to the impact of AI on human rights, particularly those forms of AI that as a global society we may want to ban entirely ('red-lines')?<sup>1</sup> How is the global regulatory system reacting to these risks, and is it responding adequately? I will use the examples of regulation of remote biometric surveillance systems, and the situation of the impact of AI on children's human rights as case studies to illustrate the challenges of regulating intrusive uses of AI on a global and regional level. Finally, I will reflect on Ireland's role in this regulatory system, particularly in the current geo-political tension between innovation and regulation.

## WHAT IS AI?

### *A definition of AI*

The increasing use and potential risks of AI are prevalent issues in contemporary public discourse.<sup>2</sup> The term 'AI' is worth defining to begin with. 'AI' describes a technology on a spectrum from simple algorithms to very complex almost autonomous systems. A generally accepted definition is that contained in the European Union's Artificial Intelligence Act 2024. Chapter 1 (1) of that Act defines an AI system as:

a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

Defining technology in regulation is a significant challenge, given the speed at which technology advances, when compared to the pace of regulatory development

<sup>1</sup>Red lines is a term which is in common usage in technology regulation to discuss boundaries or limits that should not be crossed. More recently it was used in the Global Call for AI Red Lines, an open letter signed by numerous scientists, global leaders and other prominent voices in AI development and regulation, and released in September 2025. Available at <https://red-lines.ai/> (last accessed 25 November 2025).

<sup>2</sup>Department for Science, Innovation and Technology & Centre for Data Ethics, 'International survey of public opinion on AI safety: A new survey of public opinion in nine countries shows widespread support for AI safety testing', 27 October 2023. Available at: <https://www.gov.uk/government/publications/international-survey-of-public-opinion-on-ai-safety>; N. Dreksler, H. Law, C. Ahn, D.S. Schiff, K.J. Schiff, Z. Peskowitz, 'What does the public think about AI? An overview of the public's attitudes towards AI and a resource for future research' (2025), Centre for the Governance of AI. Available at: [https://cdn.governance.ai/What\\_does\\_the\\_public\\_think\\_about\\_AI.pdf](https://cdn.governance.ai/What_does_the_public_think_about_AI.pdf) (25 November 2025).

(particularly at a regional and international level). Definitions need to be relatively neutral, while broad enough to encompass new use-cases.<sup>3</sup>

Familiar contemporary categories of AI systems include *generative artificial intelligence*, which can be prompted to generate images or chunks of text. This type of system includes large language models (LLMs), which are becoming increasingly prevalent in generating website copy, images and other forms of writing.<sup>4</sup> *Machine learning* is a type of AI that analyses data and learns from the data, enabling the system to make predictions or decisions.<sup>5</sup> Recommender systems, such as those that make recommendations on music or video-streaming platforms, or which suggest contacts on social media platforms, operate on this system. Chatbots or digital assistants, which mimic human interaction to provide information and advice, operate on a type of AI called *natural language processing*.<sup>6</sup> This category enables AI systems to understand and interact with human language.<sup>7</sup> This includes systems that recognise speech and generate speech. *Agentic artificial intelligence* refers to systems that have a degree of autonomy and which can make decisions and undertake specific tasks with limited supervision.<sup>8</sup> It is built on machine learning models that emulate human decision-making. An example would be a virtual travel assistant which could make bookings when provided with information about a preferred destination.<sup>9</sup>

### *What are the principal use-cases for AI?*

AI has numerous and varied use-cases in modern society, both by state and non-state actors. A full analysis of all these use-cases is outside the scope of this contribution, but I highlight some contemporary examples here to illustrate the human rights and societal impacts, which are discussed in a later section.

In the defence sector, AI has a range of uses, from support to decision-making to weapons technology.<sup>10</sup> Cyber-defence and cyber-operations are key aspects

<sup>3</sup>Luciano Floridi, 'On the Brussels-Washington consensus about the legal definition of artificial intelligence', *Philosophy & Technology* 36 (4) (2023), 87.

<sup>4</sup>Chris Stokel-Walker and Richard Van Noorden, 'The promise and peril of generative AI', *Nature* 614 (1) (2023), 214–16.

<sup>5</sup>International Standards Organisation, ISO/IEC 23053:2022- Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML). Edition 1, 2022.

<sup>6</sup>Salvatore Claudio Fanni, Maria Febi, Gayane Aghakhanyan and Emanuele Neri, 'Natural language processing', in *Introduction to artificial intelligence* (Cham, 2023), 87–99.

<sup>7</sup>International Standards Organisation, 'Unravelling the secrets of natural language processing', available at: <https://www.iso.org/artificial-intelligence/natural-language-processing> (9 August 2025).

<sup>8</sup>San Murugesan, 'The rise of agentic AI: Implications, concerns, and the path forward', *IEEE Intelligent Systems* 40 (2) (2025), 8–14.

<sup>9</sup>Edward CS Ku, 'Anthropomorphic chatbots as a catalyst for marketing brand experience: Evidence from online travel agencies', *Current Issues in Tourism* 27 (23) (2024): 4165–184.

<sup>10</sup>Jean-Marc Rickli and Federico Mantellassi, 'Artificial intelligence in warfare: Military uses of AI and their international security implications', in Michael Raska and Richard A. Bitzinger (eds), *The AI wave in defence innovation: Assessing military artificial intelligence strategies, capabilities, and trajectories* (Abington, 2023), 12–36.

of modern defence capabilities. At the most impactful end of AI in defence, AI can be used in decision-making about whether defence capabilities are used in autonomous or semi-autonomous weapons.<sup>11</sup> There is debate in human rights frameworks as to whether new constraints are needed on this type of capability.<sup>12</sup> In cyber-security (which is a significant threat to national security as well as individual and corporate interests), AI can be used both as a shield against hacking, and increasingly by criminal actors to conduct cyber-crime such as fraud and hacking.<sup>13</sup> In law enforcement, AI is increasingly important to a range of policing functions, from back-office support and administration to surveillance to predictive policing systems.<sup>14</sup> AI underpins potentially intrusive surveillance technologies such as remote biometric surveillance systems, and automated number plate recognition systems, which allow tracking of individuals, groups and vehicles. AI powers predictive policing systems, which aggregate and analyse data to direct policing resources towards individuals, communities or geographical locations based on risk prediction.<sup>15</sup> AI can be used to automate or speed up processing of large datasets in complex investigations.<sup>16</sup>

The private sector is increasingly turning to technological surveillance to reduce retail crime, implementing automatic number plate recognition (ANPR) and facial recognition systems in retail premises including supermarkets and fuel stations.<sup>17</sup> AI is increasingly embedded in the planning and delivery of state services, such as forecasting, planning and risk assessment.<sup>18</sup> AI systems can be used for risk prediction in social welfare, immigration and child protection systems.<sup>19</sup> AI systems have also been used for detection of fraud in social welfare

<sup>11</sup>Vincent Boulanin, Neil Davison, Netta Goussac, Moa Peldán Carlsson/SIPRI, 2020, *Human Control in Autonomous Weapon Systems: Practical Elements and Limits*, 2020, Stockholm International Peace Research Institute. Sweden, available at: <https://coilink.org/20.500.12592/gfk9k9> COI: 20.500.12592/gfk9k9 (7 November 2025).

<sup>12</sup>Daragh Murray, 'Adapting a human rights-based framework to inform militaries' artificial intelligence decision-making processes', *Louis ULJ* 68 (2023), 293–326.

<sup>13</sup>Europol, *Steal, deal and repeat: How cybercriminals trade and exploit your data. Internet Organised Crime Threat Assessment*, Publications Office of the European Union, Luxembourg, 2025.

<sup>14</sup>Europol (2024), *AI and Policing the Benefits and Challenges of Artificial Intelligence for Law Enforcement: An Observatory Report from the Europol Innovation Lab*, doi: 10.2813/0321023 (7 November 2025).

<sup>15</sup>Andrew Ferguson, 'Policing predictive policing', *Washington University Law Review* 94 (2016), 1109.

<sup>16</sup>*The Policing Productivity Review*, 'Improving outcomes for the public', 2023, chrome-extension://efaidnbmninnbpcapjpcgclefindmkaj/[https://data.parliament.uk/DepositedPapers/Files/DEP2023-0895/Policing\\_Productivity\\_Review.pdf](https://data.parliament.uk/DepositedPapers/Files/DEP2023-0895/Policing_Productivity_Review.pdf) (7 November 2025).

<sup>17</sup>Zoe Chenier-Hinde, 'Work smarter, not harder: Why intelligence practitioners should embrace private sector partnerships', *Journal of the Australian Institute of Professional Intelligence Officers* 30 (2) (2022), 23–30.

<sup>18</sup>Government of Ireland, Department of Public Expenditure NDP Delivery and Reform, *Guidelines for the Responsible Use of Artificial Intelligence in the Public Service* (7 May 2025), available at: <https://www.gov.ie/en/department-of-public-expenditure-infrastructure-public-service-reform-and-digitalisation/publications/guidelines-for-the-responsible-use-of-ai-in-the-public-service/> (7 November 2025).

<sup>19</sup>Emily Keddell, 'The devil in the detail: Algorithmic risk prediction tools and their implications for ethics, justice and decision-making', *The Sage Handbook of Decision Making, Assessment and Risk in Social Work* (2023), 405–20; Roxana Akhmetova and Erin Harris, 'Politics of technology: The use of artificial intelligence by US and Canadian immigration agencies and their impacts on human rights', in *Digital Identity, Virtual Borders and Social Media* (Cheltenham, 2021), 52–72.

systems and financial systems more generally.<sup>20</sup> In the education sector, the use of generative AI is becoming more prevalent, causing significant challenges for assessment and assurance of learning, and concerns about the impact on the creativity and depth of education.<sup>21</sup> Nonetheless, assistive and adaptive technology that utilises AI can provide support to learning for second-language learners or disabled learners.<sup>22</sup> In urban centres and in private homes, ‘smart technology’ is increasingly embedded. In a private residence, this could include automation of heating and cooling systems, and intelligent home security systems.<sup>23</sup> In ‘smart cities’, AI systems can monitor environmental impacts and streamline and automate local government services.<sup>24</sup>

The professional services field is changing with the availability of AI systems that can automate and speed up some tasks. For example, in legal practice, AI can provide support in drafting contracts and completing discovery.<sup>25</sup> In accounting, AI can analyse large amounts of numerical financial data quickly and automate aspects of financial reporting. Our consumption of media, both in terms of social media, video content and news content, is increasingly governed by algorithms, which order the priority in which content is delivered, and suggest new content, and consequently have a significant influence on the type and prevalence of information delivered to us.<sup>26</sup> Last, we are seeing the development of AI chatbots that purport to provide therapy and companionship.<sup>27</sup>

## THE IMPACT OF AI ON HUMAN RIGHTS

The preceding section has demonstrated how AI is increasingly embedded in modern society, in the domestic, state and private sectors. We can see from the diverse sample of use-cases that AI can have a significant impact on society and people. Again, this is a broad and constantly evolving issue, but this section draws attention to the most prevalent risks to human rights. It is important to also recognise that in some cases AI could potentially be used as a tool to uphold and protect human rights.

<sup>20</sup>Mike Zajko, ‘Automated government benefits and welfare surveillance’, *Surveillance & Society* 21 (3) (2023), 246–58.

<sup>21</sup>Sabrina Habib, Thomas Vogel, Xiao Anli, and Evelyn Thorne, ‘How does generative artificial intelligence impact student creativity?’ *Journal of Creativity* 34 (1) (2024), 100072.

<sup>22</sup>Katerina Zdravkova, ‘The potential of artificial intelligence for assistive technology in education’, in *Handbook on intelligent techniques in the educational process: Vol 1 recent advances and case studies* (Cham, 2022), 61–85.

<sup>23</sup>Xiao Guo, Zhenjiang Shen, Yajing Zhang and Teng Wu, ‘Review on the application of artificial intelligence in smart homes’, *Smart Cities* 2 (3) (2019), 402–20.

<sup>24</sup>Zaheer Allam and Zaynah A. Dhunny, ‘On big data, artificial intelligence and smart cities’, *Cities* 89 (2019), 80–91.

<sup>25</sup>Silvia Martinelli, ‘AI as a tool to manage contracts consequences and challenges in applying legal tech to contracts management’, *European Review of Private Law* 31 (2/3) (2023).

<sup>26</sup>Florian Saurwein and Charlotte Spencer-Smith, ‘Automated trouble: The role of algorithmic selection in harms on social media platforms’, *Media and Communication* 9 (4) (2021), 222–33.

<sup>27</sup>John Torous and Charlotte Bleas, ‘Generative artificial intelligence in mental health care: Potential benefits and current challenges’, *World Psychiatry* 23 (1) (2024), 1.

The taxonomy of human rights is a complex subject, and there are competing conceptualisations of the categories and status of individual and collective rights. For this contribution, I take a largely chronological approach based on Karel Vašák's generations of rights concept.<sup>28</sup> Nonetheless, I acknowledge the significant criticisms of this approach,<sup>29</sup> particularly around the interdependence of rights, and the evolution of different and more diverse conceptions of categorisations of human rights.<sup>30</sup>

I will first consider civil and political rights. These rights are centred on the protection of personal freedoms and restrictions on the power of the state,<sup>31</sup> and include non-derogable human rights such as the right to life and the right to be free from torture or inhuman and degrading treatment.<sup>32</sup> This category includes what are commonly known as 'due process' or criminal procedural rights. This includes the presumption of innocence, the right to a fair trial, and the right not to be arbitrarily detained.<sup>33</sup> It also includes electoral and political rights, the right of lawful protest, and freedom of expression.<sup>34</sup> These are also known as 'first generation' human rights.

To give examples of the impact of AI in this sphere, the right to privacy is a key concern given the collection, aggregation and analysis of data, which are intrinsic to AI. The right to private and family life is protected under Article 8 of the European Convention on Human Rights as well as other international instruments.<sup>35</sup> AI systems can impact individual privacy, in terms of information relating to individual human beings. Collective privacy is also a concern, and leads to people in society modifying their behaviour, either consciously or unconsciously because they know they are surveilled. This is also known as the 'chilling effect',<sup>36</sup> and can impact on the individual and collective rights of peaceful protest.<sup>37</sup> Where AI-powered biometric surveillance systems such as facial recognition, and powerful open-source intelligence systems are deployed by law

<sup>28</sup>Karel Vašák, 'Human rights: A thirty-year struggle: the sustained efforts to give force of law to the Universal Declaration of Human Rights', *UNESCO Courier* 30 11 (1977), 29–32.

<sup>29</sup>Philip Alston, 'A third generation of solidarity rights: Progressive development or obfuscation of international human rights law?', *Netherlands International Law Review* 29 (3) (1982), 307–22.

<sup>30</sup>Spasimir Domaradzki, Margaryta Khvostova and David Pupovac, 'Karel Vasak's generations of rights and the contemporary human rights discourse', *Human Rights Review* 20 (4) (2019), 423–43.

<sup>31</sup>Charles R. Beitz, *The idea of human rights* (Oxford University Press, 2011). The primary source for these rights is the International Covenant on Civil and Political Rights (ICCPR). United Nations (General Assembly), 1966, 'International Covenant on Civil and Political Rights', *Treaty Series* 999 (December), 171, and these rights are also set out in the European Convention on Human Rights and its Protocols.

<sup>32</sup>For example Articles 6 and 7, ICCPR; Articles 2 and 3, ECHR.

<sup>33</sup>Articles 9, 10, 14, ICCPR.

<sup>34</sup>Article 19, ICCPR.

<sup>35</sup>Notably Article 12 of the Universal Declaration of Human Rights 1966, Article 17 of the International Covenant of Civil and Political Rights (1966) and Article 16 of the United Nations Convention on the Rights of the Child (1989).

<sup>36</sup>Ivan Manokha, 'Surveillance, panopticism, and self-discipline in the digital age', *Surveillance and Society* 16 (2) (2018).

<sup>37</sup>Articles 19 and 21, ICCPR. See also Human Rights Committee, General comment No. 37 (2020) on the right of peaceful assembly (Article 21). CCPR/C/GC/37.

enforcement and security agencies, individuals and groups may be less likely to exercise their rights to freedom of expression and of peaceful assembly, both in the online and the physical public space.<sup>38</sup> This is particularly observable in repressive regimes.<sup>39</sup>

The right to be free from discrimination is protected by numerous human rights instruments.<sup>40</sup> AI systems pose a significant risk in terms of bias.<sup>41</sup> There are a number of different types of bias associated with AI systems, including training bias (where the data that the system is trained on contains bias—for instance, a law enforcement database is likely to have overrepresentation by certain groups due to policing practice), algorithmic bias (where the design of the system itself is flawed), or cognitive bias (where the system absorbs or reflects the bias of the humans that designed it).<sup>42</sup> An example would be a system used by the Dutch government ('SyRI') to detect alleged welfare fraud. The bias baked into the system meant that immigration status, socio-economic status and neighbourhood profile labelled a person as being riskier, attracting disproportionate state interventions.<sup>43</sup>

Turning now to social, economic and cultural rights, these rights are based on the idea of a right to live a dignified life with access to the basic necessities of life.<sup>44</sup> These include the right to work and to education and to health. These are known as 'second generation' rights as these began to be recognised later in the twentieth century. However, while it is sometimes contended that this category of rights have lesser status in the human rights framework,<sup>45</sup> and are often expressed as being aspirational rather than mandatory, there is the same imposition of legal obligation on states as in relation to civil and political rights.<sup>46</sup> AI may have significant risks in the future of work in terms of privacy (for instance, relating to worker performance monitoring), and the effect of increased

<sup>38</sup>European Union Agency for Fundamental Rights. *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*, Publications Office of the European Union, 21 November 2019.

<sup>39</sup>Hamid Akin Ünver, *Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights*, Report for Directorate-General for External Policies, European Parliament, available at: [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO\\_IDA\(2024\)754450\\_EN.pdf](chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf) (2024).

<sup>40</sup>International Convention on the Elimination of All Forms of Racial Discrimination (1966), 660 UNTS 195.

<sup>41</sup>Bert Heinrichs, 'Discrimination in the age of artificial intelligence', *AI & Society* 37 (1) (2022), 143–54.

<sup>42</sup>Robert Challen, Joshua Denny, Martin Pitt, Luke Gompels, Tom Edwards and Krasimira Tsaneva-Atanasova, 'Artificial intelligence, bias and clinical safety', *BMJ Quality & Safety* 28 (3) (2019), 231–37.

<sup>43</sup>Marvin SL van Bekkum and Frederik Zuiderveen Borgesius, 'Digital welfare fraud detection and the Dutch SyRI judgment', *European Journal of Social Security* 23 (4) (2021), 323–40.

<sup>44</sup>These rights are set out in the Universal Declaration of Human Rights and given legal force in the core human rights instrument International Covenant on Economic, Social and Cultural Rights (1966).

<sup>45</sup>Matthew C.R. Craven, *The International Covenant on Economic, Social and Cultural Rights: A Perspective on its Development* (Oxford, 1995), 106–52.

<sup>46</sup>International Commission of Jurists, *Courts and the Legal Enforcement of Economic, Social and Cultural Rights: Comparative Experiences of Justiciability* (Geneva, 2008); Alicia Ely Yamin, 'The future in the mirror: Incorporating strategies for the defense and promotion of economic, social, and cultural rights into the mainstream human rights agenda', *Human Rights Quarterly* 27 (4) (2005), 1200–44.

automation for some roles and professions.<sup>47</sup> Cultural rights involve the preservation of indigenous, religious and ethnic communities' ways of life and languages, and include intellectual property rights. Concern has been expressed about the impact of generative AI on artists and creatives.<sup>48</sup> The training of AI on datasets derived from authors' and artists' work without permission or recompense impacts creators' ability to make a living from their work.<sup>49</sup> This leads to wider conversations about the effect of increased use of AI on human values, including educational and creative values.<sup>50</sup>

In environmental terms, our collective 'third generation' human rights such as the right to a healthy environment<sup>51</sup> may be impacted by the infrastructure required by AI systems. In many jurisdictions, including Ireland, concern has been expressed over the environmental impact caused by the power-hungry data centres required by AI systems.<sup>52</sup> Finally, the human rights framework protects the rights of societal groups, such as children,<sup>53</sup> women,<sup>54</sup> ethnic and racial minorities,<sup>55</sup> indigenous people<sup>56</sup> and disabled people.<sup>57</sup> Children are used in one of two case studies below to illustrate the challenges in constraining risks to vulnerable societal groupings. Though the above discussion zeros in on risks to human rights, it is important to recognise that AI could, like other technologies, be used as a tool to uphold and protect human rights. AI systems can be used to uphold positive human rights duties. An example would be where law enforcement authorities use AI, such as retrospective facial recognition technology, to detect and investigate the production and trading of child abuse imagery, thus upholding the state's positive duties under Article 19 of

<sup>47</sup>John Howard, 'Artificial intelligence: Implications for the future of work', *American Journal Of Industrial Medicine* 62 (11) (2019), 917–26. Eva Selenko, Sarah Bankins, Mindy Shoss, Joel Warburton and Simon Lloyd D. Restubog, 'Artificial intelligence and the future of work: A functional-identity perspective', *Current Directions in Psychological Science* 31 (3) (2022), 272–79.

<sup>48</sup>Hye-Kyung Lee, 'Rethinking creativity: Creative industries, AI and everyday creativity', *Media, Culture & Society* 44 (3) (2022), 601–12.

<sup>49</sup>Jenny Quang, 'Does training AI violate copyright law?' *Berkeley Technology Law Journal* 36 (2021), 1407.

<sup>50</sup>Chris Stokel-Walker & Richard Van Noorden 'The promise and peril of generative AI' *Nature* 614 (1) (2023), 214–16.

<sup>51</sup>Richard P. Hiskes, *The human right to a green future: Environmental rights and intergenerational justice* (Cambridge, 2009).

<sup>52</sup>Hannah Daly, *Data Centres in the Context of Ireland's Carbon Budgets: Report commissioned by Friends of the Earth*, December 2024, available at: [chrome-extension://efaidnbmninnnigbpcajpcglclefindmkaj/https://www.friendsoftheearth.ie/assets/files/pdf/data\\_centres\\_and\\_the\\_carbon\\_budgets\\_-\\_prof\\_hannah\\_daly\\_dec\\_2024.pdf](chrome-extension://efaidnbmninnnigbpcajpcglclefindmkaj/https://www.friendsoftheearth.ie/assets/files/pdf/data_centres_and_the_carbon_budgets_-_prof_hannah_daly_dec_2024.pdf) (2 November 2025).

<sup>53</sup>Convention on the Rights of the Child, 20 November 1989

1577 U.N.T.S. 3; 28 I.L.M. 1456 (1989).

<sup>54</sup>Convention on the Elimination of All Forms of Discrimination against Women, 18 December 1979

1249 U.N.T.S. 13; 19 I.L.M. 33 (1980).

<sup>55</sup>International Convention on the Elimination of All Forms of Racial Discrimination, 21 December 1965 S. Exec. Doc. C, 95–2 (1978); S. Treaty Doc. 95–18; 660 U.N.T.S. 195, 212.

<sup>56</sup>United Nations (General Assembly), 2007, *Declaration on the Rights of Indigenous People*. G.A. Res. 61/295.

<sup>57</sup>Convention on the Rights of Persons with Disabilities, 3 May 2008, UN Doc. A/RES/61/106 A/RES/61/106, Annex I.

the United Nations Convention on the Rights of the Child.<sup>58</sup> Further, AI tools have been reported to be used by human rights defenders in investigating human rights abuses.<sup>59</sup>

## REGULATORY THEMES

Moving now to examine the contemporary global position on the regulation of AI, recently that there have been developments in concretising regulation, mostly in the European Union context. To date, development and use of AI has largely been steered by private sector interests, rather than anchored in deliberative legislative and policy decisions, with the input of citizens and consumers. This section discusses the distinct stages or waves of regulation of AI, and the extent to which these forms of regulation protect people and societies from the risks of AI.

As with any technology, the first stage of implementation involves improvement in the operation of the systems. For instance, in improving the training data sets to improve accuracy or reduce bias. The next question often becomes an ethical enquiry—should we be using this technology at all? In response to ethical concerns, a first distinct category of response was, and is, the development of ethical and principle-based guidance. Across the past ten years, as AI became increasingly embedded in everyday life, both state and private sector entities responded to concerns by developing guidelines and frameworks designed to promote trustworthy and ethical AI. These include those guidelines and frameworks formulated by international organisations,<sup>60</sup> by state sector agencies<sup>61</sup> and by the private sector.<sup>62</sup> This type of response centres around principles such as transparency, the safeguarding of ‘human in the loop’, ethics and fairness. These principles can be useful statements of values but are not enforceable and can easily be changed.<sup>63</sup>

In the second category of regulatory approach, there are numerous examples of contemporary global moves to regulate AI through legislation. The International Association of Privacy Professionals (IAPP)’ legislative tracker is

<sup>58</sup>Michael Pizzi, Mila Romanoff and Tim Engelhardt, ‘AI for humanitarian action: Human rights and ethics’, *International Review of the Red Cross* 102 (913) (2020), 145–80.

<sup>59</sup>Anne Dulka, ‘The use of artificial intelligence in international human rights law’, *Stanford Technology Law Review* 26 (2022), 316.

<sup>60</sup>E.g. UNESCO, ‘Recommendation on the ethics of artificial intelligence’, 2021, OECD. *Recommendation of the Council on Artificial Intelligence*. OECD/LEGAL/0449, adopted on: 22 May 2019, amended on: 3 May 2024.

<sup>61</sup>E.g. New Zealand Government, ‘Algorithm Charter for Aotearoa New Zealand’, 2020. [https://data.govt.nz/assets/data-ethics/algorithm/Algorithm-Charter-2020\\_Final-English-1.pdf](https://data.govt.nz/assets/data-ethics/algorithm/Algorithm-Charter-2020_Final-English-1.pdf).

<sup>62</sup>Google, ‘AI principles progress update’, 2023, <https://ai.google/static/documents/ai-principles-2023-progress-update.pdf>.

<sup>63</sup>Brent Mittelstadt, ‘Principles alone cannot guarantee ethical AI’, *Nature Machine Intelligence* 1 (11) (2019), 501–7.

a useful indicator of the significant levels of global legislative activity.<sup>64</sup> To use the most prevalent example, we will look at how the European Union (EU) has led the world in the enactment of comprehensive legislation to regulate AI. In doing so, the EU builds on a record of significant regulatory activity aimed at protecting individual and collective privacy and protecting consumers' fundamental rights by constraining 'big tech'. This has its foundation in the regulatory system for the protection of personal data, namely through the world-leading General Data Protection Regulation (GDPR), which came into force in 2018. The EU's actions are important because it is a global standard setter, and a very large world market. The halo effect of EU regulation (where jurisdictions not strictly subject to its rules align standards to the regulation—also known as the 'Brussels Effect')<sup>65</sup> increases its influence. The Digital Services Act and the Digital Markets Act, both commenced in 2022, also aim to protect citizens' fundamental rights and constrain cybercrime, the trade and exchange of illegal goods and services, misinformation, and the harmful effects of the monopoly of large digital platforms in citizens' lives.<sup>66</sup>

The project to regulate AI within the European Union commenced with work done by the High-Level Expert Group on AI.<sup>67</sup> The final version—the AI Act (enacted in mid-2024, and to be gradually implemented until 2027) is a significant development in regulating this fast-developing technology. The EU AI Act, though it is centred on the protection of fundamental rights, is built on a product safety framework. Importantly, it stretches past principles and guidance into a legislative regime that sets rules and imposes penalties for non-compliance. It categorises AI systems into levels of risk.<sup>68</sup> The level of risk then governs the legal obligations on designers and deployers of AI systems (such as accuracy, data governance and cybersecurity). Some types of systems are classed as 'prohibited' and cannot be sold on the EU market. These include emotion recognition systems, social scoring systems and AI systems that are used to manipulate vulnerable people.<sup>69</sup> As will be discussed in more detail below, the original premise was that remote biometric identification systems would be banned, but this has been significantly weakened in the final version.<sup>70</sup> High risk systems include AI systems in medical devices, in the operation of

<sup>64</sup>IAPP, Global AI Law and Policy Directory (updated to May 2025). Available at: <https://iapp.org/resources/article/global-ai-legislation-tracker/> (7 November 2025).

<sup>65</sup>Anu Bradford, *The Brussels effect: How the European Union rules the world* (Oxford University Press, USA, 2020).

<sup>66</sup>European Commission, The Digital Services Act package, available at: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> (7 November 2025).

<sup>67</sup>European Commission, *White Paper on Artificial Intelligence: A European approach to excellence and trust* (2020), available at: [https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust\\_en](https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en) (7 November 2025).

<sup>68</sup>Jonas Schuett, 'Risk management in the Artificial Intelligence Act', *European Journal of Risk Regulation* 15 (2) (2024), 367–85.

<sup>69</sup>EU AI Act, Article 5(1).

<sup>70</sup>EU AI Act, Article 5(1)(h).

critical infrastructure, in education and in hiring systems in employment.<sup>71</sup> The EU AI Act does not apply to national security systems, nor to some border related uses, these systems being considered within the responsibility of the member state.<sup>72</sup> The delineations between law enforcement, border security and national security may not be completely clear, particularly in transnational crime.<sup>73</sup>

The third framework for considering the constraint of AI is through a human rights lens.<sup>74</sup> In a preceding discussion, we identified some of the most prevalent risks AI systems pose to human rights. The key discourse in the human rights systems is around whether existing human rights frameworks are sufficient to respond to these challenges and risks or whether new instruments, or indeed the recognition of new human rights might be required. In the last decade, human rights bodies, such as the United Nations Committee on the Rights of the Child,<sup>75</sup> have cautioned on the challenges of AI and other emerging technologies for individual and collective human rights such as privacy and freedom of expression. Other significant risks are the use of AI in armed conflict and to promote hate speech.<sup>76</sup> To respond to the challenges, activity on specific legal instruments may be observed. In 2024, the Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law was enacted, which is a specific treaty related to ensuring that activities in the life cycle of AI systems are consistent with human rights, democracy and the rule of law.<sup>77</sup> It is also increasingly apparent that new human rights may have to be recognised in the age of AI, particularly rights relating to neuro-privacy and cognitive freedom.<sup>78</sup>

## CASE STUDY 1: BIOMETRIC SURVEILLANCE SYSTEMS

The past decade has seen considerable evolution in technology-enabled surveillance. This term covers a significant range of technologies, from remote biometric surveillance such as facial recognition technology, to artificial intelligence powered open-source analytics used to analyse social media posts, to automatic

<sup>71</sup>EU AI Act, Article 6 and Annex I and III.

<sup>72</sup>EU AI Act, Recital, at para (24).

<sup>73</sup>Nessa Lynch, 'Facial recognition technology in policing and security: case studies in regulation', *Laws* 13 (3) (2024), 35.

<sup>74</sup>Mathias Risse, 'Human rights and artificial intelligence: An urgently needed agenda', *Human Rights Quarterly* 41 (1) (2019), 1–16.

<sup>75</sup>United Nations Committee on the Rights of the Child. General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, 2 March 2021.

<sup>76</sup>United Nations held an International Day for Countering Hate Speech on 18 June 2025, with the theme of 'Hate speech and artificial intelligence', available at: <https://www.un.org/en/observances/countering-hate-speech> (7 November 2021)

<sup>77</sup>CETS 225 – Artificial Intelligence, 5.IX.2024.

<sup>78</sup>Daniel Susser and Laura Y. Cabrera, 'Brain data in context: Are new rights the way to mental and brain privacy?' *AJOB Neuroscience* 15 (2) (2024), 122–33.

number plate recognition technology. There is a significant body of literature on the impact of technology-enabled surveillance on human rights. This includes intrusions into collective and individual privacy rights, the potential ‘chilling effect’ on citizens’ rights in moving around public spaces and in protest settings, and the risks of embedded bias in technology resulting in discriminatory outcomes.<sup>79</sup>

To illustrate the challenges of regulating an intrusive form of AI system, we will look at remote biometric identification (a common example of which is facial recognition technology). This type of technology can identify individuals through automated processing of their biometric data against a stored template. This operation can be performed in real time (e.g. where a CCTV camera is fitted with biometric identification capability), or retrospectively (e.g. in a cold case investigation).<sup>80</sup> Identification can be done in real-time and without the subject’s knowledge, making this a powerful tool for law enforcement, anti-terrorism and national security purposes. I will discuss two of the regulatory categories set out above, and how these have been applied to attempt to constrain the risks of this technology for individual and collective rights.

This technology has been regularly criticised by human rights groups based on privacy, freedom of expression and assembly, and the right to be free from discrimination.<sup>81</sup> There is a spectrum of intrusiveness, with the live biometric identification use case being at one end, while at the other end, retrospective use is considered less impactful, due to the potential intervention by law enforcement being more measured in how it is carried out.<sup>82</sup> However, it is important to assess the context and usage of retrospective analysis, particularly where the time lag is short.<sup>83</sup>

The EU’s stance on restricting intrusive and risky forms of AI is increasingly important as a counterbalance to developments elsewhere in the global legal order. Civil society groups across Europe advocated strongly for the EU AI Act to ban law enforcement use of this technology entirely. An earlier iteration of

<sup>79</sup>See e.g. Mathias Klang and Andrew Murray (eds), *Human rights in the digital age* (Routledge-Cavendish 2005); Daragh Murray, ‘Facial recognition and the end of human rights as we know them?’ *Netherlands Quarterly of Human Rights* 42 (2) (2024), 145–52; Nessa Lynch, ‘Facial recognition technology in policing and security: Case studies in regulation’, *Laws* 13 (35) (2024). Joe Purshouse and Liz Campbell, ‘Privacy, crime control and police use of automated facial recognition technology’, *Criminal Law Review* 3 (2019) available at: <https://research.monash.edu/en/publications/privacy-crime-control-and-police-use-of-automated-facial-recognit/> (7 November 2025).

<sup>80</sup>E. Jakubowska, *Remote biometric identification: A technical & legal guide* European Digital Rights, 2023, available at: <https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/> (7 November 2025).

<sup>81</sup>Michael O’Flaherty, ‘Facial recognition technology and fundamental rights’, *European Data Protection Law Review* 6 (2020).

<sup>82</sup>Nessa Lynch and Andrew Chen, *Facial Recognition Technology: Considerations for use in Policing: Report Commissioned by the New Zealand Police* (2021).

<sup>83</sup>Daragh Murray, ‘Police use of retrospective facial recognition technology: A step change in surveillance capability necessitating an evolution of the human rights law framework’, *The Modern Law Review* 87 (4) (2024), 833–63.

the regulation would have done so.<sup>84</sup> However, the final text (due in part to disagreement between Member States' prioritisation of security concerns, particularly at major events),<sup>85</sup> allows the use of the technology in specified circumstances such as the targeted search of specific victims of crimes like abduction, human trafficking and missing persons (presumably justified because of the importance of protecting vulnerable victims).<sup>86</sup> The second permitted objective is the prevention of a 'substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack'.<sup>87</sup> The third permitted objective is the localisation or identification of suspects in relation to specified serious offending. For Member States who decide to use RBI for law enforcement purposes in public spaces after 2 February 2025, the state must 'expressly provide for the possibility to authorise such use in its detailed rules of national law'.<sup>88</sup>

Elsewhere, I have argued that the significant exceptions in the EU AI Act will probably result in more usage of this technology, as it may be regarded as being 'EU approved' if the conditions are met.<sup>89</sup> For example, Ireland is currently considering draft legislation arising from commitments in the Programme for Government to empower facial recognition technology for use by law enforcement.<sup>90</sup> This appears to be modelled from the limits in the EU AI Act, indicating the use of the provisions as a policy 'floor' rather than a 'ceiling'. Ireland's situation is complex, as under Protocol 21, the jurisdiction appears to have an exclusion from the law enforcement parts of the EU AI Act, including remote biometric, predictive policing, and biometric categorisation for law enforcement purposes.<sup>91</sup> Nonetheless, the government has made public statements that it

<sup>84</sup>Irish Council for Civil Liberties, ICCL welcomes AI Act vote in European Parliament, 14 June 2023, available at: <https://www.iccl.ie/2023/iccl-welcomes-ai-act-vote-in-european-parliament/> (7 November 2025).

<sup>85</sup>E.g. Maria Maggioro, Leila Miñano, Harald Schumann (22 January 2025), 'France spearheads member state campaign to dilute European AI regulation. Investigate Europe', available at: <https://www.investigate-europe.eu/posts/france-spearheads-member-state-campaign-dilute-european-artificial-intelligence-regulation> (5 November 2025).

<sup>86</sup>EU AI Act, Article 5(1)(h)(i).

<sup>87</sup>EU AI Act, Article 5(1)(h)(ii).

<sup>88</sup>EU AI Act, Recital at para. 37.

<sup>89</sup>Nessa Lynch, 'An exploration of the exceptions allowing remote biometric identification for law enforcement purposes in the European Union (accepted for publication in a forthcoming book [*AI and Power*] to be published by the University of London Press).

<sup>90</sup>Harry McGee, 'Facial recognition: Work on law to introduce technology "well advanced", says Minister', *Irish Times*, Friday 25 April 2025.

<sup>91</sup>Protocol (No 21) on the Position of the United Kingdom and Ireland in Respect of the Area of Freedom, Security and Justice [2016] OJ C202/295 (Protocol 21). Recital (40) of the EU AI Act says 'In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, Ireland is not bound by the rules laid down in Article 5(1), first subparagraph, point (g), to the extent it applies to the use of biometric categorisation systems for activities in the field of police cooperation and judicial cooperation in criminal matters, Article 5(1), first subparagraph, point (d), to the extent it applies to the use of AI systems covered by that provision, Article 5(1), first subparagraph, point (h), Article 5(2) to (6) and Article 26(10) of this Regulation adopted on the basis of Article 16 TFEU which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU, where Ireland is not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 TFEU'.

considers itself to be bound, as in its view ‘Protocol 21 only applies in instances where the legal basis for a new legislative measure is drawn from Title V of Part 3 of the Treaty on the Functioning of the European Union. This is not the legal basis for the EU AI Act.’<sup>92</sup>

In terms of the international human rights system, there is as yet no clear statement that the use of remote biometric identification systems is considered to be completely contrary to human rights. There are two important cases considering the application of the European Convention on Human Rights to facial recognition systems. *R. (Bridges) v Chief Constable of South Wales Police*<sup>93</sup> was a decision of the High Court of England and Wales in 2019, which was appealed to the Court of Appeal. It was found that the police’s use of this technology was in breach of the right to private and family life, and that police did not comply with data protection and other administrative requirements. However, police services across England and Wales continue to use this technology, as with the correct policies and procedures in place, it complies with the law. In 2023, the European Court of Human Rights (ECtHR), in the case of *Glukhin v Russia*,<sup>94</sup> considered the case of a Russian citizen who alleged breach of rights to private and family life under Article 8 of the Convention, and to freedom of expression under Article 10 of the Convention. This was in relation to the Moscow law enforcement authorities’ use of both retrospective and live facial recognition, which led to Glukhin’s conviction for an administrative offence related to a protest.

In this case, the ECtHR undertook a complete examination of the ambit of Article 8 (the right to private and family life), underscoring that the right to respect for private life extends into the public sphere, as it encompasses the notion of a ‘private social life.’ This interpretation includes ‘a zone of interaction of a person with others, even in a public context’, which may nonetheless fall within the scope of ‘private life’.<sup>95</sup> The ECtHR considered that the mere retention of personal data is an infringement of this right. It said that an individual’s ‘reasonable expectations of privacy’ were significant in assessing the proportionality of the data retention.<sup>96</sup> Additionally, the ECtHR reiterated previous cases, where it had found violations arising from the ‘collection and storing of data by the authorities on particular individuals’, even where such data pertained exclusively to public conduct, as well as from the ‘collection of data in

<sup>92</sup>Minister for Justice, Written Answer in response to Question no. 205 from Deputy Sinéad Gibney, Wednesday 12 February 2025. Available at: <https://www.oireachtas.ie/en/debates/question/2025-02-12/205/> (7 November 2025).

<sup>93</sup>*R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341; *R (Bridges) v Chief Constable of South Wales Police & Ors* [2020] EWCA Civ 1058.

<sup>94</sup>App. No. 11519/20. Judgment. At <https://hudoc.echr.coe.int/?i=001-225655>. European Court of Human Rights (Third Section), July 4, 2023.

<sup>95</sup>[para. 64].

<sup>96</sup>[para. 66].

a public place.<sup>97</sup> While the ECtHR in *Glukhin* does not say that the technology should be completely prohibited, it considers the technology to be ‘particularly intrusive’ and requires a ‘high level’ of justification, with the ‘highest level’ required for the use of live FRT. The ECtHR does not go so far as to say what this ‘highest level’ of justification may involve. It is likely that this centres around situations where there is a significant risk to public safety.

Thus, although biometric identification systems are considered by human rights bodies and human rights scholars to pose a very high risk to individual and collective human rights, even the EU AI Act’s provisions are a weak response. In a White Paper published last year, I and others have called for specific human rights frameworks and protections to respond to these particularly intrusive systems.<sup>98</sup>

## CASE STUDY 2: CHILDREN’S HUMAN RIGHTS AND AI

Children (those aged less than 18 years) have specific protections under international human rights law, under the UN Convention on the Rights of the Child. Children provide an excellent case study of the inadequacy of global moves to regulate AI, both in terms of the gaps in the regulatory framework or moves to overregulate and ban some types of AI.<sup>99</sup> Again, this is a broad and fast evolving issue, but I will concentrate on an aspect that is prevalent in public discourse, and highly relevant to Ireland as so many large technology companies are headquartered within this jurisdiction.

As was discussed in an earlier section, AI systems operate a significant influence on the media and content we consume. Algorithms order social media feeds, suggest content and are capable of being programmed by advertisers or political parties to amplify content for particular groups. The harmful aspects of social media are amplified for children, given their vulnerability and need for protection, in line with the principle of evolving capacities. To give some examples of the harm that can be caused by AI-related systems, we will look at three examples, as well as the regulatory challenges these use-cases pose.

The first aspect is the risk of synthetic content produced by AI. This can include misleading content such as deepfakes or images generated by AI, which as UNICEF warn ‘can potentially be personalized to individual users and, as a result, be harder to combat by automated and human moderators’.<sup>100</sup> Emerging

<sup>97</sup>[para. 67].

<sup>98</sup>Alexander Kriebitz *et al.*, *White Paper. Promoting and Advancing Human Rights in Global AI Ecosystems: The Need for A Comprehensive Framework under International Law* (February 2025). Available at: <https://repository.globethics.net/handle/20.500.12424/4321222> (7 November 2025).

<sup>99</sup>See Nessa Lynch, ‘Children and artificial intelligence’, forthcoming in *International Journal of Children’s Rights* (2026).

<sup>100</sup>UNICEF, ‘Generative AI: Risks and opportunities for children. How can we empower and protect children in the face of artificial intelligence?’ Available at: <https://www.unicef.org/innocenti/generative-ai-risks-and-opportunities-children> (7 November 2025).

technologies such as AI have created new risks and amplified existing risks in relation to sexual harm and offending against children. Particularly relevant (and novel) is the issue of non-consensual image sharing, and the creation of sexualised deepfake images.<sup>101</sup> Regulation, both domestically and internationally, has lagged behind the creation of sexualised deepfake imagery, such as apps that ‘undress’ people in images. The creation and circulation of such imagery is increasingly common in spaces where children and young people congregate, such as school environments. This aspect involves image sharing between peers, but this type of technology may also be used by paedophiles to create sexualised imagery of children.<sup>102</sup>

Second, concern has been growing about the increasing impacts of recommender algorithms in social media systems, which can have a significant impact on children whose brains are developing. Concern has been expressed in relation to male children around the spread of misogynistic material and views, and in radicalisation by the far right.<sup>103</sup> In relation to female children, content amplified includes that relating to disordered eating and suicidal ideation. While algorithmic ordering and amplification of harmful content can impact any user, children are particularly susceptible. In an editorial, Ursula Kilkelly discusses a report by the Five Eyes intelligence alliance, which highlights the risks of young people becoming involved in violent extremism.<sup>104</sup> In Ireland, the teenage boy convicted and sentenced to detention for the attempted murder of an army chaplain outside an army barracks in Galway, was reported to have been radicalised online, and committed the violent attack because of misinformation about the role of the Irish defence forces in Mali.<sup>105</sup> Also in Ireland, an RTÉ Prime Time investigation in 2024 demonstrated how an account set to the age of a 13 year old was shown harmful content related to self-harm and suicidal thoughts within twenty minutes.<sup>106</sup>

The European Union has taken the initiative under the Digital Services Act and the Digital Markets Act to move to regulate harmful content generated by

<sup>101</sup>Elena Martellozzo and Paula Bradbury, ‘The Intersection of AI and CSAM: A reflection on the UK’s online safety act’, *Media@LSE*, 6 March 2025, available at: <https://blogs.lse.ac.uk/media/2025/03/06/the-intersection-of-ai-and-csam-a-reflection-on-the-uks-online-safety-act/> (7 November 2025).

<sup>102</sup>Asher Flynn, Anastasia Powell, Adrian J. Scott and Elena Cama, ‘Deepfakes and digitally altered imagery abuse: A cross-country exploration of an emerging form of image-based sexual abuse’, *The British Journal of Criminology* 62 (6) (2022), 1341–358.

<sup>103</sup>European Union Terrorism Situation and Trend Report (EU TE-SAT).

<sup>104</sup>Ursula Kilkelly, ‘Editorial: Young people and violent extremism’ (2025), *Youth Justice: An International Journal*, 7–11, citing Five Eyes (2024), *Five Eyes Insights: Young People and Violent Extremism: A Call for Collective Action*, available at: <https://rcmp.ca/en/corporate-information/publications-and-manuals/five-eyes-insights-young-people-and-violent-extremism-call-collective-action> (7 November 2025).

<sup>105</sup>Alison O’Riordan, ‘Defence Forces chaplain repeatedly stabbed tells his attacker he forgives him’, *Breakingnews.ie*, 10 April 2025.

<sup>106</sup>RTÉ Prime Time experiment reveals disturbing content recommended to 13-year-old TikTok users in Ireland. Thursday 18 April 2024, available at: <https://about.rte.ie/2024/04/18/rte-prime-time-experiment-reveals-disturbing-content-recommended-to-13-year-old-tiktok-users-in-ireland/> (7 November 2025).

AI. In 2024, the European Commission issued formal proceedings against the social media company TikTok on whether it breached European regulations by failing to protect children and mitigating foreseeable risks around the use of algorithmic systems. The European Commission noted that the system operated by TikTok can produce behavioural addictions. Thierry Breton (the Commissioner for the Internal Market) noted that ‘we must spare no effort to protect our children’.<sup>107</sup> There has been criticism that the European Commission, and national authorities are not going far enough to constrain the use of algorithms that push harmful content. The Irish Council for Civil Liberties have specifically called on the President of the European Commission to put political pressure on Ireland (as the regulator of many big technology firms headquartered in Ireland) to switch off these algorithms.<sup>108</sup>

In some jurisdictions, children under the age of 16 have been banned from social media platforms to reduce harm.<sup>109</sup> Complete prohibitions or excessively restrictive measures on children’s use of artificial intelligence do not constitute a coherent or effective response to associated risks. Such strategies may unconsciously encourage children to circumvent safeguards by turning to unregulated environments.<sup>110</sup> Furthermore, they fail to adequately recognise and uphold the autonomy and participatory rights of children, particularly older adolescents. The UN Committee on the Rights of the Child’s General Comment on children’s rights in relation to the digital environment, places emphasis on the Member States’ parties’ duty:<sup>111</sup>

to consult with children on relevant legislative, administrative and other measures and to ensure that their views are considered seriously, and that children’s participation does not result in undue monitoring or data collection that violates their right to privacy, freedom of thought and opinion.

This case study demonstrates the challenges in regulating AI systems that are under the control of multi-national large technology companies, and in ensuring that there is not a disproportionate response to risks that result in further human rights impacts.

<sup>107</sup>European Commission, Press Release: Commission opens formal proceedings against TikTok under the Digital Services Act, 19 February 2024, available at: [https://ec.europa.eu/commission/presscorner/detail/en/%5E/ip\\_24\\_926](https://ec.europa.eu/commission/presscorner/detail/en/%5E/ip_24_926) (7 November 2025).

<sup>108</sup>Johnny Ryan, ‘Europe’s race to rearm is pointless if its adversaries are waging war online’ *Guardian*, 15 April 2025, available at: <https://www.theguardian.com/commentisfree/2025/apr/15/us-europe-military-spending-trump-ireland> (7 November 2025).

<sup>109</sup>Jasmine Fardouly, ‘Potential effects of the social media age ban in Australia for children younger than 16 years’, *The Lancet Digital Health* 7 (4) (2025), e235–e236.

<sup>110</sup>Kelsey L. McAlister, Clare C. Beatty, Jacqueline E. Smith-Caswell, Jacquelyn L. Yourell, and Jennifer L. Huberty, ‘Social media use in adolescents: Bans, benefits, and emotion regulation behaviors’, *JMIR Mental Health* 11 (2024), e64626.

<sup>111</sup>United Nations Committee on the Rights of the Child, General Comment No. 25 (2021) on Children’s Rights in Relation to the Digital Environment. 2 March 2021, at [para 18].

## IN CONCLUSION, WHAT ROLE CAN IRELAND PLAY?

This contribution has analysed the challenges and risks that AI poses for people and for society, with a focus on two case-studies. Concluding with a specific comment on Ireland, Ireland has for a number of reasons developed an outsize role in relation to AI regulation.

The presence of many international technology companies in Ireland, who come under the jurisdiction of the Irish regulatory authorities, such as the Data Protection Commission, Coimisiún na Meán (the media regulator), which includes the Online Safety Commissioner, means that Ireland's regulators have a significant part to play in the battle to regulate large technology companies and to constrain harmful uses of AI. Ireland's regulators must take a strong role in implementing the EU regulations and ensuring that these companies are not causing harm to vulnerable groups. In particular, social media companies have significant responsibilities in combatting misinformation and disinformation and reducing the availability of harmful content to children. This must be done in a manner that respects children's rights, particularly in relation to their evolving capacities. The actions of Ireland, with and on behalf of the EU, are particularly critical at a point of geopolitical tensions involving constraint of technology companies. The Trump administration has come out strongly in favour of the technology companies, describing EU regulations as constraining freedom of speech and describing these regulations as censorship.<sup>112</sup>

In the area of technology-based surveillance, Ireland, as the only common-law jurisdiction in the EU, has an important role to play in demonstrating a model for a common-law, human rights respecting approach to the use of intrusive surveillance technology. The shape of a proportionate approach, which upholds individual and collective rights to privacy, freedom of association and peaceful protest, and protects vulnerable groups, is yet to be modelled internationally. A principled approach does not preclude the use of such tools in genuine carefully defined emergency situations, or in a proportionate response in a situation where the system contributes to upholding human rights.

<sup>112</sup>Alexandre Piquard, 'Trump fires back at EU tech regulation', *Le Monde*, 9 March 2025, available at: [https://www.lemonde.fr/en/economy/article/2025/03/09/trump-fires-back-at-eu-tech-regulation\\_6738972\\_19.html](https://www.lemonde.fr/en/economy/article/2025/03/09/trump-fires-back-at-eu-tech-regulation_6738972_19.html) (7 November).