

186. RETHINKING DIGITAL JUSTICE

ELS DE BUSSER

Institute for Information Law, University of Amsterdam

Digital technology redefines the way that justice is delivered and received¹. This observation led to a number of insights on how to describe this still developing field of what is often referred to as digital justice. But what exactly is digital justice? What is included and what is not? Academic literature and policy documents have dealt with digital justice in both civil and criminal justice by roughly using two approaches: a more restrictive approach using technology and the focal point and a wider approach using technology as the starting point for a further analysis of its impact on human rights. Both approaches have their merits. Yet, since the topic of digitalisation and justice is an ever-evolving theme, it is necessary to study what both approaches consist of and whether they stand the test of time.

For that reason, this paper first unpacks how academia and policy have defined digital justice thus far and second, how digital justice could be defined. The goal is to conclude in a comprehensive definition of digital justice.

I. THE STATUS QUO: HOW WE HAVE DEFINED DIGITAL JUSTICE

1. Restrictive approach: technology as the focal point

On 20 November 2025 the European Commission presented the so-called Digital Justice @2030 Strategy². Already in the first lines of the document

¹ KARIKKANDATHIL, S.: *How Digital Justice is Transforming the Justice System*, Microsoft, 2016: <https://news.microsoft.com/en-xm/2016/10/30/how-digital-justice-is-transforming-the-justice-system/>

² European Commission, DigitalJustice@2030, COM(2025) 802 final.

it is clear that the word justice in the title is meant to refer to the justice apparatus or the judges, courts, prosecution, law enforcement and the systems they use to do their jobs rather than to the substantive content of justice, i.e. human rights and the rule of law. The Commission's strategy sets out efforts of digitalisation and the deployment of digital technologies in the justice sector with the aim to «increase the efficiency of public services by making them digital by default, stimulating productivity»³.

Such approach to the concept of digital justice has been embraced by academia and policy documents before. It is an approach that zooms in on the more procedural and practical side of digitalisation, covering applications, infrastructure and ways in which digital technology can make existing processes in the justice apparatus more efficient or more accessible, or both. The effect on human rights is left out or at best sporadically mentioned and in the latter case that mention is limited to those rights that are immediately affected such as access to justice, the right to data protection and privacy and non-discrimination.

I will refer to this more restrictive and narrow approach as the formal or institutional part of digital justice due to the focus on the technology itself and how the institution applies it. As virtuous and necessary as this narrow view is, it leaves out the depth and width of the impact of digital technologies on human rights and the rule of law. The European Commission's strategy only refers to the effect of digitalisation on human rights briefly as it is clearly not its main focus. Obviously, the reason for such limited view on the part of the European Commission is also related to the nature of the document and the division in policy areas within the EU institutions. Nevertheless, when including other policy documents –such as from the Council of Europe– as well as academic articles, we see similar views surface. They mostly zoom in on using digital technology in several processes related to the justice system –recognizing the undeniable effect of the covid-19 pandemic– and acknowledge the effects on access to justice.

The above-mentioned Digital Justice @2030 Strategy had predecessors in the shape of the 2030 Digital Compass⁴ setting out a vision for digitalisation in different policy areas, but also a Eurojust initiative called the Digital Criminal Justice Programme. Considering the tasks of Eurojust in facilitating cross-border cooperation in criminal matters, the Digital Criminal Justice Pro-

³ *Ibid.*, p. 1 and COM(2021)118 final - 2030 Digital Compass: the European way for the Digital Decade, p. 10.

⁴ European Commission, 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final, 9.3.2021.

gramme⁵ is focused on making several of these processes digital such as the exchange of information from the Counter-Terrorism Register and Eurojust's own Case Management System. Logically the implementation of such innovative mechanisms required appropriate amendments to the Eurojust Regulation followed by the establishment of secure IT infrastructure⁶. It is not surprising that the mentioned documents, even though the focus is largely on the technology itself, often make a reference to the right to access to justice. The Council of the EU set the tone for this with its 2020 conclusions on «access to justice – seizing the opportunities of digitalisation»⁷. As one of the key aspects of the rule of law and the prerequisite for exercising other human rights, it is also access to justice that is impacted first and foremost by the introduction of digital tools. Online information sources, cross-border exchange of data over a secured IT system or videoconferencing in trials allowing for the testimony of a witness or victim abroad, allow for a better access to the justice system.

Similarly, in their 2016 Guidelines on how to drive change towards Cyberjustice⁸, the Council of Europe's Commission for the Efficiency of Justice (CEPEJ) does not analyse in depth the effect of digital tools on human rights and the rule of law. Nevertheless, the elaborate overview starts with access to justice and further also touches upon several aspects of the fair trial rights. In that sense –also considering the fact that 2016 was a relatively early point in time to introduce such guidelines– technology may have been a focal point, it was recognized as opening the door for more people to find their way to justice. In 2021, the CEPEJ followed up with an Action Plan that clearly has an underlining goal of improving fair trial rights but stops at the level of general orientations rather than a thorough study of what digitalisation means for human rights⁹.

In 2020, Scott Fraley published a critical opinion on digital justice and defines it as «the use of digital technologies to implement the practice of law and the work of the police, lawyers, and the courts»¹⁰. There is no doubt that his rather negative account of digital justice –even leaning into the argument that it may be a threat to the rule of law– is firmly placed in the more restricti-

⁵ European Commission, Digitalisation of justice in the European Union, COM(2020) 710 final, 2.12.2020.

⁶ Regulation (EU) 2023/2131 amending Regulation (EU) 2018/1727 of the European Parliament and of the Council and Council Decision 2005/671/JHA, as regards digital information exchange in terrorism cases, O. J. L 2131, 11.10.2023.

⁷ Council Conclusions Access to justice – seizing the opportunities of digitalisation, C 342 I, 14.10.2020.

⁸ CEPEJ, Guidelines on how to drive change towards Cyberjustice, CEPEJ (2016)13.

⁹ CEPEJ, 2022-2025 Action Plan Digitalisation for a Better Justice, CEPEJ (2021)12Final.

¹⁰ FRALEY, S.: «Digital Justice: Shining Future or Illusory Chimera?», Polemos 2020, p. 47.

ve approach. Even if we would make abstraction of his strong criticism on the use of digital technology in the justice system, he only briefly touches upon human rights like the right to a fair trial or cross examination. He does not mention any human rights that may be offered more protection by digital justice. Jane Donoghue wrote in 2017 how public participation and access to justice can be enhanced by means of courtroom technology¹¹. The paper is clearly concentrated on the infrastructural or institutional part of digital justice, covering videoconferencing for defendants and witnesses and other digital services such as making information accessible to the public. She makes a clear case for how digital justice can bring access to justice forward but also recognizes that policy frameworks need to be working in correspondence to ensure appropriate access to legal aid. Donoghue therefore builds the bridge to a wider view on digital justice –broader than merely introducing IT tools– but does not unpack what that should look like.

2. Wider approach: technology as the starting point

Where the European Commission in its aforementioned Digital Justice @2030 Strategy limited digital justice to the applications of digital technology by the justice sector, the 2025 report from the EU's Fundamental Rights Agency (FRA): Digitalising Justice – A Fundamental Rights Based Approach takes a much wider perspective¹². The report walks us through an in-depth fundamental rights analysis of 31 digital tools and systems applied in Austria, Estonia, France, Italy, Latvia, Poland and Portugal. The analysis includes elaborate use cases and is based on a combination of desk research and interviews with 208 professionals working in the justice field¹³. In this way, the technologies are not the focal point but the starting point of an examination into their effects on fundamental rights such as the right to privacy and data protection, the right to non-discrimination, defence rights, the right to a fair trial and the right to an effective remedy.

I will refer to this wider approach as the substantial or contextual part of digital justice as it leans on the content of justice, meaning human rights and the rule of law, and it considers the socio-technical context as well by looking

¹¹ DONOGHUE, J.: «The Rise of Digital Justice: Courtroom Technology, Public Participation and Access to Justice», *Modern Law Review*, 2017, pp. 996-1025.

¹² EU Agency for Fundamental Rights, Digitalising Justice – A Fundamental Rights-based Approach, Report, November 2025.

¹³ *Ibid.*, p. 3.

at the impact of digital technologies on citizens and their rights. The FRA report is quite unique in taking this contextual point of view on how digital technologies affect human rights and how this concerns more human rights than are commonly included in academic literature and policy documents.

In academia, Corien Prins¹⁴ and Natali Helberger¹⁵ expand their view on digital justice to also include the effect of technology on human rights and the rule of law. Where Prins' key argument is that «the conditions for the functioning of the constitutional state contain an inherent obligation for all state powers to make use of digitisation»¹⁶, she recognizes the negative as well as the positive effect that the use of digital technology could have in courts. Highlighting a number of beneficial uses of technology, such as more efficient case law management and thus shortening the duration of cases or data analysis into similarities between cases, she advocates for a responsible and balanced introduction of technology. Even if Helberger's article carries the title «The rise of technology courts, or: How technology companies re-invent adjudication for a digital world», it is not solely focused on the formal and institutional part of digital justice. On the contrary, the article first zooms in on the different values that are introduced into the courtroom with the advent of digital technology developed and delivered by companies. Those company values, such as efficiency and scalability, become bridges for moving the lens to human rights when Helberger expands the meaning of digital justice to include the court-like power and the set-up of oversight boards with platform providers like Meta, openly questioning how they interpret human rights and adjudicate, but also openly questioning whether our traditional views of the justice system are still equipped for protecting human rights in today's digital world?¹⁷

Using digital technology as a focal –and only– point as opposed to a starting point to discuss digital justice, changes the direction of the debate. The first will stop at studying the use of digital technology, the second will expand into a range of human rights that are potentially impacted by that use. In this paper I advocate for joining both views on digital justice. This means that digital justice should be described as a goal that can be reached by studying digital technology applications, processes and infrastructure within the (civil and criminal) justice system as well as their impact on human rights and the rule of law. The rationale behind this broader definition of digital justice is the

¹⁴ PRINS, C.: «Digital Justice», *Computer Law and Security Review*, 2018, pp. 920-923.

¹⁵ HELBERGER, N.: «The rise of technology courts, or: How technology companies re-invent adjudication for a digital world», *Computer Law and Security Review*, 2025, p. 106118.

¹⁶ PRINS, C.: «Digital Justice», p. 922.

¹⁷ HELBERGER, N.: «The rise of technology courts», p. 9.

deep and wide impact that digital technologies can have on individuals' lives. By only studying the processes and infrastructure used in and by the justice system, we miss a substantial opportunity to protect human rights and the rule of law as it is only by assessing the potential impact of a technology *before* using it that harm to human rights and the rule of law can be prevented. Waiting until harm manifests, makes it often technically difficult to go back and fix the technology in question. In addition, the financial cost of repairing the technology can go hand in hand with a human cost¹⁸. Ideally, this attention to human rights and the rule of law is moved to the earliest point in time, i.e. before the design and development of a technology, also known as «by-design thinking»¹⁹. The latter requires close cooperation with the developers, different perspectives on the matter and follow-up throughout the process of developing and deploying technology. This means that at the start of this process a thorough assessment should be made of the potential impact of digital technology on humans, on society and on the justice system.

II. A NORMATIVE ANALYSIS ON HOW DIGITAL JUSTICE SHOULD BE DEFINED

Which human rights should we take into account when embracing the wider definition of digital justice? In the existing literature and policy documents we often see the same rights surfacing in combination with digital technology, the so-called usual suspects of human rights. These will be the subject of subsection 1. In subsection 2 I will widen the view and touch upon those human rights that are not always front and centre but should be included to achieve a full picture.

1. The usual suspects of human rights

The human rights that are typically included in academic articles and policy documents covering digital technologies and civil or criminal justice are those that we perceive as immediately affected by such technologies, even though several other human rights can be touched in a more indirect or even insidious way.

¹⁸ See for example the Dutch Child Benefits scandal explained in section I.3. See also Amnesty International, *Xenophobic Machines: Discrimination Through Unregulated Use of Algorithms in the Dutch Childcare Benefits Scandal*, AI Index EUR 35/4686/2021, Report 2021.

¹⁹ DE BUSSE, E.: «Human Rights in Technology -- A Need for a New Norm», *Case W. Res. J. Int'l L.* 2025, pp. 133-134.

First, above I distinguished a restrictive approach to digital justice from a wider approach and in spite of the restriction of the formal or institutional definition of the concept, one part of the rule of law that was not overlooked was access to justice. This can be explained by the immediate effect of good-working digital infrastructure on how citizens find their way to the administration of justice, for example by finding information on laws and case law, by physically or virtually accessing their files or a courtroom, etc. Access to justice is a fundamental part of the rule of law as without it, exercising any other human rights becomes nearly impossible²⁰.

Second, the right to privacy and data protection are quickly mentioned whenever digital technologies and their impact are explained. We can distinguish two main reasons for this observation. On the one hand, data –whether personal data or non-personal data– are mostly collected, processed and stored by using digital technologies. This does not mean that non-digital ways of collecting, processing and storing data –for example a paper catalogue or file containing evidence– do not touch upon these rights. It means that digital technologies make it easier, more efficient and more cost-effective to do that. Even when the identification of an individual –the prerequisite to speak of personal data– is not possible, the use of digital technologies such as facial recognition or listening devices can still infringe the right to privacy when individuals are filmed or recorded in a private setting. On the other hand, databases of digital data can be combined²¹ leading to a number of data points on one individual such as a risk profile on whether someone is likely to commit a criminal act in the future. By combining a certain amount of non-personal data from such databases, it is also possible to conclude on the identification of an individual, making the combination effectively personal data and activating the right to data protection. The latter is a relevant method for police and prosecution authorities to find and identify a suspect²².

Due to the increase in the use of AI driven technologies and research revealing that a non-representative set of training data can lead to a discriminatory outcome²³, the right to non-discrimination and the related equality principle can also be considered among the usual suspects of human rights affected

²⁰ World Justice Project (n.d.), What is the rule of law? <https://worldjusticeproject.org/about-us/overview/what-rule-law>

²¹ See for an overview of interoperability in criminal matters: European Commission, Report on the evaluation of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), COM(2026) 32 final, 26.1.2026.

²² Regulation 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration, O. J. L 135, 22.5.2019.

²³ See inter alia BUOLAMWINI, J./GEBRU, T.: Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research 81, 2018, pp. 1-15 and Autoriteit Persoonsgegevens, Belastingdienst/Toeslagen De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag (z2018-22445), Report 2020.

by digital technologies. In the field of border control and surveillance, where facial recognition technologies are often used, the adverse effects and biases around ethnicity and race are particularly alarming²⁴. However, discriminatory outcomes can also be the result of skewed data collection or even algorithms that were structured in a way that they do not measure what they were intended to measure. The latter can happen when poorly selected quantifiable factors are used or numerical proxies are used for relevant but not-quantifiable factors²⁵.

A more foundational aspect of digital technologies and their discriminatory effect is their use, excluding those individuals or groups of individuals who are unable –for any reason imaginable– to work with them. Forcing citizens to use particular apps or websites without offering help or an analogue alternative, leaves out those who live in areas where the necessary digital infrastructure is lacking and those who have the infrastructure but not the means or the intellectual capabilities to use digital solutions. This techno-solutionism²⁶ or techno-fixes²⁷ as a way to solve or mitigate societal problems by using technology, was criticized from several angles²⁸. Even though inequality and discrimination are mentioned among the issues to solve, the argument that over-indexing on technological solutions could in itself create more inequality and discrimination could receive more attention, especially in practice.

2. The unusual suspects of human rights

Besides the aforementioned human rights that are typically referred to when the impact of digital technology is studied, three other rights tend to be overlooked because how they are affected is less direct and less visible: the right to asylum and migration, the right to a fair trial and freedom of peaceful

²⁴ See inter alia ACHIUME, E. T.: *Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance: Racial and Xenophobic discrimination and the use of digital technologies in border and immigration enforcement*, A/HRC/48/76, 2021, p. 5.

²⁵ OBERMEYER, Z./POWERS, C./VOGELI, C./MULLAINATHAN, S.: «Dissecting racial bias in an algorithm used to manage the health of populations», *Science*, 2019, pp. 447-453.

²⁶ MOROZOV, E.: «To save everything, click here: The folly of technological solutionism», Public Affairs, 2013 and SÆTRA H. S./SELINGER, E.: «Technological Remedies for Social Problems: Defining and Demarcating Techno-Fixes and Techno-Solutionism», *Sci Eng Ethics* 30, 2024, p. 60.

²⁷ WEINBERG, A.: «Can technology replace social engineering?», *Bulletin of the Atomic Scientists*, 22(10) 1966, pp. 4–8.

²⁸ For an overview, see SÆTRA, H. S./SELINGER, E.: «Technological Remedies for Social Problems», p. 60; ALLEN, H. J.: *Fintech and Techno-Solutionism*, 98 *Southern California Law Review*, 2025, p. 761 and PERKINS, H.: «Beyond techno-solutionism: Towards critical perspectives in environmental education and digital technology. A critical-hermeneutic review», *International Journal of Child-Computer Interaction*, 2024, p. 100705.

assembly and association. I zoom in on these three rights due to their link to criminal justice.

Closely related to the use of digital technologies for the purpose of border control and surveillance, is their effect on asylum and migration. A concept called «digital borders» coined by Dennis Broeders, explains this well as it also taps into the power of combining the content of databases, often containing biometric data, with each other²⁹. The practice of interoperability of databases and their use for the purpose of proactive risk profiling –not just in the context of asylum and migration but for traveling in general– will effectively grow in the near future with the operationalization of new systems such as the European Travel Information and Authorization System (ETIAS) and the Entry and Exit System (EES).³⁰ By the end of 2026, both should be fully operational.

Yet the concept of digital borders could also describe a similar situation but at an earlier moment in time. Where Broeders refers mostly to the gathering and combining of data on irregular migrants who have already entered an EU member state, UN Special Rapporteur E. T. Achume is effectively widening the scope of the question of digitalisation in the context of migration to the gathering of data before and at the point of entry into a country³¹. She offers examples from countries where data carriers of undocumented asylum seekers are confiscated at the border or drones are used to surveille border areas and seas. Data are used for the purpose of identification, risk profiling or border control management. The link with criminal justice lies in how the aforementioned practices –often using military-grade technologies and equipment– show a growing trend towards a criminalisation of migration³².

The right to a fair trial as laid down in article 6 of the European Convention on Human Rights (further: ECHR) and articles 47 to 50 of the Charter of

²⁹ BROEDERS, B.: «The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants», *International Sociology*, 22 /1, pp. 71-92.

³⁰ See Meijers Committee, Comments on the proposal for a Regulation of the European Parliament and of the Council and establishing a European Travel Information and Authorisation System (ETIAS), COM(2016) 731 final, Opinion CM1708, 2017; Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011 (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, O. J. L 236, 19.9.2018, p. 1 and Regulation, (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, O. J. L 327, 9.12.2017, p. 20.

³¹ ACHUME, E. T., 2021, pp. 4-5.

³² *Ibid.*, pp. 6 and 11.

Fundamental Rights and Freedoms (further: the Charter), is known to have a civil and a criminal limb. Whereas the ECHR joins both in one article, article 47 of the Charter covers the fair trial rights in civil cases and articles 48 to 50 cover criminal trials. Referring back to the earlier mentioned practice of risk profiling and the algorithmic prediction that someone is likely to commit a crime, the presumption of innocence is at stake³³. When individuals' lives and those of the people around them, expressed in data points, are analysed in order to score the probability of them committing a criminal act, the subsequent treatment of these individuals can have a significantly adverse impact on their lives and that of their families. The use of algorithmic scoring combined with human selection by the Dutch tax authorities in an attempt to fight fraud with childcare benefits³⁴, resulted in a financial cost that is estimated at fourteen billion euros³⁵ and an immeasurable human cost that includes forced evictions, mental health problems, divorces, etc.³⁶

Besides the presumption of innocence, digital technology affects more rights included in the package of fair trial rights, such as the right to information and translation. The impact on these rights looks more like a facilitation by digital means than a genuine negative effect. Nevertheless, the negative effect may be indirect, it is not absent. The right to information refers to the right to know which criminal charge is made against you and to receive such information in a language you understand. Considering existing technological applications, especially the most recent AI and GenAI applications that allow for direct translation, it is not unthinkable to introduce such technologies in the courtroom for translation purposes. Several countries have already taken steps in that direction³⁷. Additional incentives can be the increasing workload of many court systems and strained budgets which could tip the scales in favour

³³ VAN BRAKEL, R./DE HERT, P.: «Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies», in De Pauw, E./Ponsaers, P./van der Vijver, K./Bruggeman, W./Deelman, P. (eds): *Technology-led Policing, Journal of Police Studies*, 2011-3, p. 179. See also ZEDNER, L./ASHWORTH, A.: «The Rise and Restraint of the Preventive State», *Ann. Rev. Crim.* 2019, p. 443 and FERZAN, K.: «Preventive justice and the presumption of innocence», *Crim. Law Philos.*, 2012, pp. 505-525.

³⁴ Autoriteit Persoonsgegevens, Belastingdienst/Toeslagen: De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag, Report, 2020, pp. 26–29.

³⁵ DE ROOY, M./JONKER, J.: Herstel toeslagenaffaire dreigt ongekende strop te worden: nog 5 miljard extra, NOS, 13.05.2024: <https://nos.nl/artikel/2520340-herstel-toeslagenaffaire-dreigt-ongekende-strop-te-worden-nog-5-miljard-extra>

³⁶ Amnesty International, Xenophobic Machines: Discrimination Through Unregulated Use of Algorithms in the Dutch Childcare Benefits Scandal, AI Index EUR 35/4686/2021, Report 2021, p. 13.

³⁷ For an overview, see PANEZI, A./O'SHEA, J.: «Artificially Translating the Law: Risks of Decentering the Human Expert», 1.10.2025. Available at SSRN: <http://dx.doi.org/10.2139/ssrn.5816664>

of using automated translation over human translation³⁸. Simultaneously, companies advertise AI tools the legal profession can outsource some of their work to³⁹. The unseen costs of these practices are considerable. First, the reliability of automated translations is doubtful due to the lack of context and nuance which can make a substantial difference in criminal investigations and prosecutions. Moreover, spoken dialects and accents can make it difficult for automated translations to work properly. From a broader perspective, any questions around the reliability of translations can cause a discouraging effect on citizens seeking justice. This means that indirectly, access to justice can also be negatively impacted by automated translations⁴⁰. Second, uploading legal briefs into an AI translation tool raises important questions around data protection, confidentiality and even copyright⁴¹. Third, just like AI and GenAI applications in general, translation tools can contain –gender, racial, etc.– bias and risk perpetuating such bias in the translated texts they produce⁴².

Lastly, the fair trial rights also include the right to defence. Besides the earlier mentioned questions around the impact of digital technology, the use of GenAI for fabricating legal arguments and legal precedents should be included here. Worldwide, over 700 cases are known in which a decision was made by a court or a judge after a party was found to rely on content or citations hallucinated by a GenAI tool⁴³. 27 cases are known in which legal arguments were fabricated by GenAI⁴⁴. The majority of the cases where citations were fake originate from predominantly common law systems such as the US, UK, Australia and Canada. Using fake citations in jurisdictions that are based on the power of legal precedent signifies a larger –legal and societal– problem. Every fake citation that was not detected and sanctioned will live on in the legal archive, potentially becoming a precedent itself. This undermining of legal precedents is an academically underdeveloped concern, yet its consequences could be vast.

³⁸ WRIGHT, S.: «Artificial Intelligence and the Language of Law», *International Journal of Language and Law*, 14, 2025, p. 124.

³⁹ For example: Thomson Reuters, How to write a legal brief – better and faster with AI, 2025: <https://legal.thomsonreuters.com/blog/how-to-write-a-legal-brief-better-and-faster-with-ai/>

⁴⁰ PANEZI, A./O'SHEA, J.: «Artificially Translating the Law», pp. 22-25 and WRIGHT, S.: «Artificial Intelligence and the Language of Law», pp. 133-134.

⁴¹ PANEZI, A./O'SHEA, J.: «Artificially Translating the Law», pp. 19-21.

⁴² *Ibid.* and SAVOLDI, B./GAIDO, M./BENTIVOGLI, B./NEGRI, M./TURCHI, M.: «Gender Bias in Machine Translation», *Transactions of the Association for Computational Linguistics* 2021, pp. 845–874.

⁴³ Database AI Hallucinations Cases created by CHARLOTIN, D.: www.damiencharlotin.com/hallucinations/ (accessed 02.01.2026)

⁴⁴ Database AI Evidence Cases created by CHARLOTIN, D.: www.damiencharlotin.com/ai-evidence/ (accessed 02.01.2026)

Freedom of peaceful assembly and freedom of association are not frequently mentioned when discussing digital technologies. This changed significantly with the increased use of facial recognition technology, especially when combined with other means of data collection such as social media monitoring. In 2024 the UN special rapporteur on the rights to freedom of peaceful assembly and of association, Clément Voule, published the Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests.⁴⁵ Even if the protocol aims to facilitate peaceful protests in general, it contains a substantial part laying down principles and best practices around the use of digital technologies. Especially in countries where forms of dissent and protest are met with harsh consequences, the use of digital technologies intensifies the possibilities for authorities to identify, intimidate and potentially prosecute individuals. The use of surveillance tools in combination with AI and its effects on assembly and association rights, including the chilling effects of it, will be the subject of a future report by the current UN special rapporteur Gina Romero.

III. WIDENING THE APERTURE

Studying the use of digital technologies in the justice system from the perspective of technology as the focal point – and therefore, the only point – misses a substantial part of the picture, namely its effect on human rights. It is a different way of thinking to use technology as the starting point in order to study their effect on human rights and the rule of law. Widening the aperture and also moving our lens onto the consequences of the use of digital technology in the justice system, both positive and negative consequences, invites a different approach. An approach that allows for introducing and applying digital technology in a way that supports human rights and the rule of law, facilitates their exercise and protects them.

The use of digital technologies can lead to injustice. This realization is missed when we solely focus on the technology as such and not on what it causes. Especially in the justice system, where human rights and the rule of law should be safeguarded, it is essential that our concentration and our efforts are not consumed by a purely utilitarian view on technology since this could

⁴⁵ VOULE, C. N.: *Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, A/HRC/55/60, 31.01.2024.

cause harm. That harm could be caused to other human rights than those we typically have on our minds when discussing digital justice. The right to a fair trial, the right to asylum and migration and the freedom of peaceful assembly and association should enter the discussions on digital justice.