**Josuan Eguiluz Castañeira**
*Legal Counsel, Adevinta*

**Carlos Fernández Hernández**
*Advisory Board Member, Global LegalTech Hub*

## 1. Introduction

When the European Union (EU) began to devise its regulatory framework for artificial intelligence (AI) in 2018, from the outset it placed particular emphasis on this technology being "trustworthy". An AI system is deemed trustworthy if it complies with all applicable legislation and it is ethical and robust, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm (High-Level Expert Group on AI, 2019).

Consequently, the European approach on this matter incentivises the development and uptake of ethical and trustworthy AI across the EU economy, based on the principle that the technology should work for people and be a force for good in society (White Paper on Artificial Intelligence, 2020, § 6).

Given that the availability of data is essential to train algorithmic systems and that much of that data is personal, a component of ethical AI is that it must include privacy and data governance mechanisms (European Commission, Coordinated Plan on Artificial Intelligence 2021 Review). This requirement is fully incorporated into the European regulation on artificial intelligence (AI Act) of June 2024. It states that one of its purposes is to promote the uptake of human-centric and trustworthy AI (Article 1), while complying with the existing legal framework on data protection, which comprises – principally  though not exclusively – the General Data Protection Regulation of 2016 (GDPR).

As several authors have noted (Almonacid Lamelas, 2024), the AI Act presents no small challenge to local governments, as they must adapt their processes, policies and strategies to meet the new requirements. But it is also an opportunity to improve their functioning, as well as the quality and trustworthiness of the AI-based services offered to citizens (ibid.). This explains the proliferation of "urban AI" systems, a concept that denotes "the collection, interpretation and analysis of urban data in order to support policy related decision-making and the development of solutions that are used, or could be used, in an urban context" (Galceran-Vercher, 2023).

Still, processing personal data in the public-urban sphere can raise specific problems, from the legitimacy of processing the data for a purpose that was not originally agreed to the need to carry out assessments of the impact on people's fundamental rights. These must clearly be taken into account by public bodies.

AI systems must also guarantee data protection throughout a system's entire life cycle. This includes the information initially provided by the user, as well the information generated about them over the course of their interaction with the system.

In light of the new legislative framework, the aim of this article is to (i) set out the legal and ethical framework that regulates personal data processing by AI systems in the urban sphere, particularly at the European level (AI Act); (ii) identify the main mechanisms for implementing the principle of privacy; and (iii) analyse the challenges that this type of data processing presents and offer a series of recommendations and good practices to minimise or rise to them.

## 2. AI ethics and privacy

Trustworthy AI must be ethical, and to do so it must, among other requirements, respect people's privacy. The AI Act sets the specific goal to "promote the uptake of human-centric and trustworthy AI". With that in mind, the common rules it lays down for high-risk AI systems must be consistent with the Charter of Fundamental Rights of the European Union (2000) and take into account both the European Declaration on Digital Rights and Principles for the Digital Decade (2022) and the ethics guidelines of the independent High-Level Expert Group on Artificial Intelligence (2019). According to these guidelines, in a context of rapid technological change,

"Trustworthiness is a prerequisite for people and societies to develop, deploy and use AI systems. Without AI systems – and the human beings behind them – being demonstrably worthy of trust, unwanted consequences may ensue and their uptake may be hindered, preventing the realisation of the potentially vast social and economic benefits that they can bring." (Introduction)

The trustworthiness of AI rests on three components, which must be present throughout the entire life cycle of the AI system:

1. It should be lawful, complying with all applicable laws and regulations;

2. It should be ethical, ensuring adherence to ethical principles and values; and

3. It should be robust, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm.

Ethics should therefore be a core pillar to ensure and scale trustworthy AI. This means that it is necessary to ensure alignment with some basic ethical norms, as well as with the measures laid down in the AI Act for the protection of fundamental rights.

Data protection is a fundamental right that is particularly affected by AI systems, and which is closely related to the principle of prevention of harm. That principle of prevention begins with adequate data

governance that covers the quality and integrity of the data used, its relevance in light of the domain in which the AI systems will be deployed, its access protocols and the capability to process data in a manner that protects privacy.

Those measures include AI systems having a privacy and data governance mechanism that takes in respect for privacy, quality and integrity of data, and access to data.

The AI Act gathers the general principle that the act fully complies with the EU's regulatory framework on data protection laid down in the GDPR.

AI systems must also guarantee data protection throughout a system's entire life cycle. This includes the information initially provided by the user, as well the information generated about them over the course of their interaction with the system (for example, the outputs the AI system generates for specific users or how they respond to particular recommendations). Digital records of human behaviour may allow AI systems to infer not only individuals' preferences, but also their sexual orientation, age, gender or religious and political views. To allow individuals to trust the data gathering process, it must be ensured that data gathered about them will not be used to discriminate against them unlawfully or unfairly.

Compliance with these requirements falls to the operators, particularly AI systems developers and those responsible for deploying the systems (who should ensure that the systems they use and the products and services they offer meet the requirements). Meanwhile, the people affected by the operation of an AI system shall have the right to be informed of that impact and, when applicable, lodge a complaint for breach of the AI Act (Articles 85 and 86).

### 2.1. Privacy and the European AI Act

Article 2(7) of the AI Act gathers the general principle that the act fully complies with the EU's regulatory framework on data protection laid down in the GDPR.

First, the harmonised rules laid down in the AI Act should apply across all sectors and should be without prejudice to existing EU law. It is important to point out, then, that the AI Act does not seek to affect the application of EU law governing the processing of personal data, including the tasks and powers of the independent oversight authorities that monitor compliance with those instruments. Similarly, nor does it affect the prior obligations of providers and deployers of AI systems in their role as data processors. In particular, the AI Act should not affect practices currently prohibited by EU law, including data protection law.

At the same time, the fact that an AI system is classified as high-risk should not be interpreted as indicating that its use is lawful under other acts of EU law or national law, for example on the protection of personal data. Any such use should continue to take place solely in accordance with the applicable requirements resulting from the Charter of Fundamental Rights, from EU secondary law and from national law.

Moreover, the AI Act does not provide for the legal ground for processing of personal data, including special categories of such data,

unless it is specifically otherwise provided for. Therefore, after the AI Act's entry into force, data subjects continue to enjoy all the rights and guarantees awarded to them by EU law, including those related to solely automated individual decision-making, such as profiling. The harmonised rules established under the AI Act should enable the exercise of the data subjects' rights and other remedies guaranteed under EU law on the protection of personal data and of other fundamental rights.

Finally, in order to facilitate compliance with EU data protection law, in specified conditions the AI Act provides the legal basis for the providers (and prospective providers) in the regulatory sandbox to use personal data collected for other purposes to develop certain AI systems in the public interest.

For cities, ensuring their AI systems comply with regulations such as the GDPR or the AI Act throughout the system's entire life cycle is crucial to safeguard citizens' rights and maintain public trust.

## 3. Policy mechanisms for implementing the principle of privacy in the urban environment

Privacy and data protection in the implementation of urban AI requires the adoption of specific policy mechanisms. These mechanisms allow cities to comply with existing regulations and ensure that AI is deployed ethically and responsibly, respecting citizens' rights. Below, we spotlight and explain the main policy mechanisms for implementing this ethical principle.

### a) Ensuring legal compliance

Compliance with regulation is an essential ethical requirement of privacy and data protection in public authority implementation of AI systems in urban environments. For cities, ensuring their AI systems comply with regulations such as the GDPR or the AI Act throughout the system's entire life cycle is crucial to safeguard citizens' rights and maintain public trust. This includes adherence to key requirements such as the quality and integrity of the data used, its relevance in light of the domain in which the AI systems will be deployed, its access protocols and the capability to process data in a manner that protects privacy (High-Level Group of Experts on AI, 2018).

Indeed, these requirements are present as specific obligations in the AI Act itself, purposely designed for high-risk cases such as AI systems for remote biometric identification – e.g. the ABIS program (Pascual, 2024) – or those used to assess a natural person's eligibility for essential public assistance services and benefits – e.g. the Syri case (Digital Future Society, 2022).

### b) Risk management and data governance systems

The AI Act includes specific obligations (Articles 9 and 10) closely linked to the principle of privacy and data protection. Article 9 focuses on the creation of a risk management system capable of identifying, documenting and mitigating the risks associated with the use of AI in cities. These risk management systems should establish continuous

iterative processes planned and run throughout the entire life cycle of AI technologies which, of course, will require regular systemic review and updating. In fact, not only does it mean assessing possible risks before the introduction into the market or the entry into service of these AI systems, but also setting up and/or supervising the functioning of a post-market monitoring system to manage emerging risks (Articles 17(1) h, 26(5) and 72 of the AI Act).

Data governance regulated in Article 10, meanwhile, requires the training, validation and testing data sets used in high-risk AI systems to be subject to data governance and management practices appropriate for its intended purpose. The practices to be implemented by cities to ensure effective and lawful data governance should focus on matters such as data collection processes and the origin of data; the purpose of the data processing; an assessment of the availability, quantity and suitability of the data sets needed; examination of possible biases that might affect the health, safety or fundamental rights of persons, and so on.

**c) Impact assessments**

Article 35 of the GDPR requires controllers (e.g. local authorities) to carry out a data protection impact assessment (DPIA). This assessment shall be carried out when a type of processing, given its nature, scope, context or purposes (in particular using new technologies), is likely to result in a high risk to the rights and freedoms of natural persons (AEPD, 2018; Article 29 Working Party, 2017; Friedwald et al., 2022). This preventive approach is vital in urban environments to anticipate possible data protection vulnerabilities and take the necessary steps to remedy them in a timely manner.

Likewise, for high-risk AI systems, Article 27 of the AI Act introduces the obligation to carry out a fundamental rights impact assessment (FRIA) (Government of the Netherlands, 2022; Danish Institute for Human Rights, 2020) to complement the DPIA. This assessment aims to identify the specific risks to the rights of individuals likely to be affected and establish measures to be taken in the event of a materialisation of those risks (Recital 96 AI Act). It is worth noting that the impact assessments (Manzoni et al., 2022) should focus not only on return on investment, but also on the sustainability and ethical impact of technology, addressing financial, human and environmental aspects (OECD, 2024).

**d) Auditing**

Having said this, it will be necessary to demonstrate to authorities, stakeholders and citizens that there is compliance with the law and all its specific implementation requirements. Accordingly, internal and external audits shall be carried out and certification shall be obtained to verify that systems operate within the established legal frameworks. To that end, European cities, for example, should carry out conformity assessments (Article 43 AI Act) in order to ensure and demonstrate compliance with the requirements associated with high-risk systems,

in line with the harmonised standards published in the *Official Journal of the European Union* (Article 41 AI Act). They should also follow the common specifications established by the European Commission, thus ensuring standardised and safe implementation of AI systems (e.g. ISO certifications).

AI audits are considered a fundamental governance mechanism to ensure that the deployment and operation of AI systems comply with established legal regulations and ethical and technical standards (Fernández and Eguiluz, 2024). Generally speaking, these audits should be carried out by independent and competent bodies. The auditing process includes methodologies that incorporate ethical impact assessments (UNESCO, 2024; CEN-CENELEC, 2017), ensuring that AI systems behave responsibly and that their impacts on society and on individuals are properly monitored and mitigated. It is, however, recommendable to consider AI audits from a multidisciplinary (legal, technical and ethical) perspective (Mökander, 2023). Thus, proposals such as "algo-scores" have arisen to classify and assess in an accessible manner an algorithmic system's level of conformity on matters such as ethical compliance, AI governance, the equity of the model and its subsequent monitoring, taking a similar approach to energy efficiency labelling (Galdon Clavell, 2024).

**e) Algorithm repositories and AI systems registers**

Lastly, it is important to remember the importance of public algorithm repositories and AI systems registries (Article 49 AI Act) that promote transparency in automated decision-making in the public sector and play a crucial role in protecting privacy and personal data. By making details of how these systems are designed, deployed and operated accessible, repositories and registries enable citizens and organisations to understand how and for what purposes their personal data is used in these processes. These repositories also include information about the data sources used and oversight mechanisms, which is essential to assess the impact on individual privacy and ensure that data protection measures are effective (Gutiérrez and Muñoz-Cadena, 2024).

## 4. Challenges and recommendations

Inadequate data management is one of the chief limitations when it comes to deploying AI in the public sector. As is lack of access to sufficient volumes of high-quality data. This problem is exacerbated by unsatisfactory sharing of data across organisations owing to the absence of unified standards and underdeveloped data governance. In addition, distrust of AI systems compounds these challenges. Scattered laws and insufficient knowledge of the impacts of AI also form significant barriers (Manzoni et al., 2023). Likewise, increasing cyberattacks have led to the NIS 2 Directive (2022) boosting the level of security and legal responsibility for administrators. In 2023, the public administration was one of the most affected sectors, registering 19% of reported incidents, with a marked rise in ransomware and DDoS attacks (ENISA, 2023).

The complex regulatory landscape also presents a significant challenge. Interaction between urban regulations at European, national and local level creates a web of rules that hampers effective AI deployment in cities. Urban legislation and specific regulations in each municipality should align with European laws such as the Interoperable Europe Act (2022), which seeks to improve the interoperability of digital public services (Tangi et al., 2023).

Another major limitation is the lack of experience and technical knowledge in local administrations, which hinders proper implementation of AI. The general shortage of professionals in the field, coupled with growing competition for talent, present a significant barrier for cities that are trying to develop and deploy these systems effectively (OECD, 2024).

Additionally, the mass collection of personal data, which is required to train these systems, may infringe a citizen's right to control their data as it may be sensitive or managed inappropriately. Meanwhile, AI applications like those used in policing can intensify mass surveillance and compromise individual privacy still further (Véliz, 2020; Agarwal, 2018; Dwivedi et al., 2019).

In order to overcome these barriers, it is essential to promote innovation mechanisms such as regulatory sandboxes (Madiega, 2022) that allow cities to experiment with AI in a controlled environment while guaranteeing regulatory compliance (Tangi et al., 2023). Likewise, coordination between national authorities (in Spain's case, the Spanish Artificial Intelligence Oversight Agency, AESIA) and European bodies (the European AI Office) is crucial to ensure that AI systems comply with existing regulations and are deployed safely and responsibly.

It is essential to promote innovation mechanisms such as regulatory sandboxes that allow cities to experiment with AI in a controlled environment while guaranteeing regulatory compliance.

Interoperability and collaboration are equally crucial. Initiatives such as the SALER – a rapid alert system used in the autonomous community of Valencia to prevent corruption in the administration – show how AI can be used effectively to improve governance processes (Digital Future Society, 2023). Likewise, it is essential that public funding is conditional on the various administrations making specific outputs available (e.g. generating public data sets) (European Commission, 2022). To this end, the European Commission published in its Implementing Regulation (EU) 2023/138 a list of specific high-value data sets that should be available for free re-use, highlighting the potential of public data to benefit society, the environment and the economy (European Commission, 2022). In addition, access to multilingual data to train local AI models that reflect the specific characteristics of each region (OECD, 2024) and the collection of AI use cases in the public sector at European level (European Commission, 2021) will improve AI systems' effectiveness and equity while providing a valuable source of information on how these technologies are being implemented in different contexts.

## 5. Conclusions

The general data protection framework in the EU now rests on a set of principles that the EU's administrative and judicial bodies are aware of and solidly interpret. AI, however, poses specific problems

of a technological and legal nature that are at a nascent moment of knowledge and treatment.

Numerous studies, experiences and clarifications shall be still necessary, then, to provide them with a legal framework that ensures the proclaimed purpose that AI should be human centred, a tool for people and have the ultimate goal of improving their well-being.

The introduction of specific policy mechanisms is essential to ensure that cities use AI systems in a manner that is ethical and respects citizens' rights. Compliance with regulations such as the GDPR and the AI Act is crucial to safeguard privacy and personal data in urban environments. Similarly, it is paramount that cities establish risk management systems that iteratively address contingencies associated with the AI's entire life cycle, including regular reviews and external audits to ensure regulatory compliance.

Data governance, too, must be at the heart of urban AI strategies. Cities must implement sound data governance and management practices, focusing on the quality, relevance and protection of the data sets used in AI systems. This includes conducting impact assessments both for the protection of personal data and for fundamental rights, ensuring that the technology deployed does not breach citizens' privacy or security.

Ultimately, achieving human centred AI will require a joint effort among those responsible for developing public policies, academic institutions and the private sector, who must work together to ensure that AI systems implemented by cities align with fundamental values and ethical principles.

As stated, the future of smart cities will be marked by the synthesis of multiple technologies aimed at satisfying the intricate mosaic of human needs. This convergence will require precise optimisation of the technologies applied to ensure that the digitalisation of urban spaces conforms to sustainable and equitable practices, as well as attentiveness to the ethical dimensions involved in these innovations. It is therefore imperative that the integration of AI into the heart of smart cities abides by principles that protect privacy, security and inclusion. As Zhenjun et al. (2023) say: "Ensuring that the benefits of smart city developments are equitably shared will be essential in avoiding societal fractures and fostering an environment where technology serves as a bridge to a more enlightened, harmonious urban life."

## References

Agencia Española de Protección de Datos (AEPD). "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales". Madrid, 2018 [accessed: 2 September 2024]

Agencia Española de Protección de Datos. "Guía sobre protección de datos y administración local". Updated 2023 [accessed: 2 September 2024]

AI Ethics Impact Group. "From Principles to Practice: An interdisciplinary framework to operationalise AI ethics". 1 April 2020 [accessed: 2 September 2024]

Alan Turing Institute. "Urban analytics" [accessed: 2 September 2024]

Alan Turing Institute. "Why the public sector needs to know about AI ethics (and how we're helping)". 2 November 2023 [accessed: 2 September 2024]

Almonacid Lamelas, V. "Reglamento (europeo) de Inteligencia Artificial: impactos y obligaciones que genera en los Ayuntamientos". El Consultor de los Ayuntamientos, LA LEY, 15 July 2024 [accessed: 2 September 2024]

Article 29 Working Party. "Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", Brussels, 2017 [accessed: 2 September 2024]

Burbano, L. (1). "Privacy protection in smart cities: How are they taking care of citizens' most precious information?" *Tomorrow.city*, 23 January 2024 [accessed: 2 September 2024]

Burbano, L. (2). "AI urbanism: risks and benefits of a seemingly unstoppable movement". *Tomorrow.city*, 22 February 2024 [accessed: 2 September 2024]

Canda, J. "AI in Urban Planning and Smart City Development". *Medium*, 7 April 2024 [accessed: 2 September 2024]

CEN-CENELEC. "Ethics assessment for research and innovation - Part 2: Ethical impact assessment framework". CWA 17145-2, June 2017 [accessed: 2 September 2024]

Centro Latinoamericano de Administración para el Desarrollo (CLAD). "Carta Iberoamericana de Inteligencia Artificial en la Administración Pública". 20 November 2023 [accessed: 2 September 2024]

Danish Institute for Human Rights. "Guidance on Human Rights Impact Assessment of Digital Activities". Copenhagen, 2020 [accessed: 2 September 2024]

Digital Future Society (1). "Algorithmic discrimination in Spain: limits and potential of the legal framework", August 2022 [accessed: 2 September 2024]

Digital Future Society (2). "El acceso digital en las ciudades, entendido como algo más que un derecho fundamental", June 2023 [accessed: 2 September 2024]

Digital Future Society (3). "El uso de algoritmos en el sector público en España: cuatro estudios de caso sobre ADMS", February 2023 [accessed: 2 September 2024]

European Commission (1). "Selected AI cases in the public sector (JRC129301)". Joint Research Centre (JRC), 2021 [accessed: 2 September 2024]

European Commission (2). "Revisión de 2021 del plan coordinado sobre la inteligencia artificial", Anexos de la Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Fomentar un planteamiento europeo en materia de inteligencia artificial, COM(2021) 205 final, 2021 [accessed: 2 September 2024]

European Commission (3). "Opportunities and challenges of artificial intelligence technologies for the cultural and creative sectors". Publications Office of the EU, Luxembourg, 2022 [accessed: 2 September 2024]

European Commission (4). "Second Report on the application of the General Data Protection Regulation", COM(2024) 357 final, Brussels, 25 July 2024 [accessed: 2 September 2024]

European Data Protection Board (EDPB). "Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework", 16 July 2024 [accessed: 2 September 2024]

European Union Agency for Cybersecurity (ENISA). "Threat Landscape 2023", October 2023 [accessed: 2 September 2024]

Fernández, C. and Eguiluz, J. A. "Diez puntos críticos del Reglamento europeo de Inteligencia Artificial". *Diario LA LEY*, No. 85, Sección Ciberderecho, 28 June 2024 [accessed: 2 September 2024]

Friedewald, M *et al*. "Data Protection Impact Assessments in Practice: Experiences from Case Studies". *Computer Security, ESORICS 2021 International Workshops*, February 2022, pp. 424-443 [accessed: 2 September 2024]

Galceran-Vercher, M. "Trustworthy Cities: Ethical Urban Artificial Intelligence". The GovLab, Course "AI Ethics, Global perspectives", December 2023 [accessed: 2 September 2024]

Galceran-Vercher, M. and Vidal, A. "Mapping urban artificial intelligence: first report of GOUAI's Atlas of Urban AI". Global Observatory of Urban Artificial Intelligence (GOUAI), 2024 [accessed: 2 September 2024]

Galdon, G. "AI Auditing. Proposal for Algo-scores". EDPB, 27 June 2024 [accessed: 2 September 2024]

Ghisleni, C. "Artificial Intelligence and Urban Planning: Technology as a Tool for City Design". *ArchDaily*, 8 February 2024 [Last accessed: 2 September 2024]

Government of the Netherlands. "Impact Assessment Fundamental Rights and Algorithms", 31 March 2022 [accessed: 2 September 2024]

Gutiérrez, J. D. and Muñoz-Cadena, S. "Algorithmic transparency in the public sector: A state-of-the-art report of algorithmic transparency instruments". *Global Partnership on Artificial Intelligence*, May 2024 [accessed: 2 September 2024]

Hadec, J., Di Leo, M. and Kotsev, A. "AI generated synthetic data in policy applications". *Science for Policy Brief*, European Commission, Joint Research Center, 2024 [accessed: 2 September 2024]

High-Level Expert Group on AI. "Directrices éticas para una IA fiable", April 2019 [accessed: 2 September 2024]

Imdat As, P.; Basu, P. and Talwar, P. *Artificial Intelligence in Urban Planning and Design. Technologies, Implementation, and Impacts*. Amsterdam: Elsevier, 2022.

Madiega, T. and Van De Pol, A. L. "Artificial intelligence act and regulatory sandboxes". European Parliamentary Research Service (EPRS), PE 733.544, June 2022 [accessed: 2 September 2024]

Manzoni, M. *et al.* AI Watch. Road to the adoption of Artificial Intelligence by the public sector. Publications Office of the EU. Luxembourg, 2022. JRC129100 [accessed: 2 September 2024]

Mökander, J. "Auditing of AI: Legal, Ethical and Technical Approaches" *Digital Society*, vol. 2, article no. 49, 2023 [accessed: 2 September 2024]

Organisation for Economic Co-operation and Development (OECD) (1). "Advancing Accountability in AI: governing and managing risks throughout the lifecycle for trustworthy AI", *OECD Artificial Intelligence Papers,* no. 349, 23 February 2023 [accessed: 2 September 2024]

Organisation for Economic Co-operation and Development (OECD) (2). "Governing with artificial intelligence: Are governments ready?", *OECD Artificial Intelligence Papers*, no. 20, June 2024 [accessed: 2 September 2024]

Pascual, M. G. "La Policía española ya usa en sus investigaciones un sistema automático de reconocimiento facial". *El País*, 28 May 2024 [accessed: 2 September 2024]

Pellegrin, J., Colnot, L. and Delponte, L. "Artificial Intelligence and Urban Development". Research for REGI Committee, European Parliament, Policy Department for Structural and Cohesion Policies, Brussels, 2021 [accessed: 2 September 2024]

Tangi, L. *et al.* "Artificial Intelligence for Interoperability in the European Public Sector: an exploratory study", Publications Office of the EU, Luxembourg, 2023 [accessed: 2 September 2024]

Tangi, L. *et al*. "AI Watch. European Landscape on the Use of Artificial Intelligence by the Public Sector", Publications Office of the EU, Luxembourg, 2022 [accessed: 2 September 2024]

Timan, T., Van Veenstra, A. F. and Bodea, G. "Artificial Intelligence and public services". Policy Department for Economic, Scientific and Quality of Life Policies, PE 662.936, July 2021 [accessed: 2 September 2024]

United Nations (UN). "Recommendation on the Ethics of Artificial Intelligence", 23 November 2021 [accessed: 2 September 2024]

Véliz, C. *Privacidad es poder: Datos, vigilancia y libertad en la era digital*. Madrid: Debate, 2021.

Verhulst, S. G. "Are we entering a Data Winter? On the urgent need to preserve data access for the public interest" [accessed: 2 September 2024]

Yan, Z. *et al*. "Intelligent urbanism with artificial intelligence in shaping tomorrow's smart cities: current developments, trends, and future directions". *Journal of Cloud Computing*, 18 December 2023 [accessed: 2 September 2024]