Josuan Eguiluz Castañeira
Assessor legal, Adevinta

Carlos Fernández Hernández
Membre del consell assessor, Global LegalTech Hub

1. Introducció

Des que el 2018 la Unió Europea (UE) va començar a dissenyar el seu marc normatiu sobre la intel·ligència artificial (IA), va emfasitzar que aquesta tecnologia ha de ser «fiable». Es considera que una IA és fiable si respecta el marc normatiu aplicable i és ètica i robusta, tant des del punt de vista tècnic com social, ja que els sistemes d'IA, fins i tot si s'utilitzen amb bones intencions, poden provocar danys accidentals (Grup d'experts d'alt nivell sobre intel·ligència artificial, 2019).

En conseqüència, l'enfocament europeu en aquesta matèria encoratja el desenvolupament i l'adopció d'una IA ètica i fiable a tota l'economia de la UE, a partir del principi que aquesta tecnologia ha d'estar al servei de les persones i ser una força positiva per a la societat (Llibre blanc sobre la intel·ligència artificial, 2020: cap. 6).

Atès que disposar de dades és fonamental per entrenar els sistemes algorítmics, i que moltes d'aquestes dades són de caràcter personal, un component de la IA ètica és que ha d'incloure mecanismes de gestió de la privacitat i de les dades (Comissió Europea, revisió de 2021 del Pla coordinat sobre la IA). Aquesta exigència ha estat plenament inclosa en el Reglament europeu en matèria d'intel·ligència artificial (RIA), aprovat el juny de 2024, que fixa com a objectiu promoure l'adopció d'una IA fiable i centrada en la persona (art. 1), respectant alhora el marc normatiu vigent en matèria de protecció de dades, constituït –principalment, però no només– pel Reglament general de protecció de dades (RGPD) de 2016.

Com han assenyalat alguns autors (Almonacid Lamelas, 2024), el RIA representa un repte important per als governs locals, ja que han d'adaptar els seus processos, les seves polítiques i les seves estratègies per complir les noves exigències. Tanmateix, el RIA també suposa una oportunitat per millorar el funcionament dels ajuntaments, així com la qualitat i la confiança dels serveis basats en IA oferts als ciutadans (*ibíd.*). Això explica la proliferació de sistemes d'«intel·ligència artificial urbana», un concepte que fa referència a «la recopilació, la interpretació i l'anàlisi

de dades urbanes per tal de donar suport a la presa de decisions relacionades amb les polítiques, així com el desenvolupament de solucions que s'utilitzen, o podrien utilitzar-se, en un context urbà« (Galcerán-Vercher, 2023).

Els sistemes d'IA han de garantir la protecció de les dades al llarg de tot el seu cicle de vida. Això inclou tant la informació inicialment facilitada per l'usuari com la que es genera sobre ell en el context de la seva interacció amb el sistema.

Amb tot, el tractament de dades personals en l'àmbit públic de l'urbanisme pot plantejar problemes específics, des de la legitimitat del tractament per a una finalitat per a la qual originalment no es va consentir, fins a la necessitat de fer avaluacions de l'impacte que té sobre els drets fonamentals de les persones. Aquests factors, inequívocament, els han de tenir en compte els organismes públics.

D'acord amb el nou marc legislatiu, l'objecte d'aquest article és (i) presentar el marc jurídic i ètic que regula el tractament de dades personals en l'àmbit urbanístic per mitjà de sistemes d'IA, especialment a Europa (RIA); (ii) identificar els principals mecanismes per implementar el principi de privacitat, i (iii) analitzar els reptes que planteja aquest tipus de tractament de dades i oferir un conjunt de recomanacions i bones pràctiques per minimitzar-los o eliminar-los.

2. IA ètica i privacitat

Una IA fiable ha de ser ètica i per ser-ho ha de respectar la privacitat de les persones, entre altres requisits. El RIA estableix com a objectiu específic promoure l'adopció d'una IA fiable i centrada en l'ésser humà. Per això, les normes comunes que estableix per als sistemes d'IA d'alt risc han de ser coherents amb la Carta dels Drets Fonamentals de la Unió Europea (2000) i han de tenir en compte tant la Declaració Europea sobre els Drets i els Principis Digitals per a la Dècada Digital (2022) com les Directrius ètiques per a una IA fiable del Grup d'experts d'alt nivell sobre intel·ligència artificial (2019). Segons aquestes directrius, en un context de canvi tecnològic ràpid, «la fiabilitat és un prerequisit perquè les persones i les societats desenvolupin, despleguin i utilitzin sistemes d'IA. Si aquests sistemes –i les persones que es troben al darrere– no demostren ser mereixedors de confiança, hi pot haver conseqüències no desitjades que n'obstaculitzin l'adopció, cosa que impediria l'assoliment dels enormes beneficis econòmics i socials que poden comportar els sistemes d'IA». (Introducció, punt 13)

La fiabilitat de la IA es basa en tres components, que s'han de tenir en compte al llarg de tot el cicle de vida del sistema d'IA:

1. Ha de ser lícita, de manera que es garanteixi el respecte de tot el marc jurídic i normatiu aplicable.
2. Ha de ser ètica, és a dir, ha d'assegurar el compliment dels principis i els valors ètics.
3. Ha de ser robusta, tant des del punt de vista tècnic com social, ja que els sistemes d'IA, fins i tot si s'utilitzen amb bones intencions, poden provocar danys accidentals.

Per tant, cal establir l'ètica com a pilar fonamental per garantir i expandir una IA fiable. Això implica garantir que es compleixin unes normes ètiques bàsiques, així com les mesures que estableix el RIA per a la protecció dels drets fonamentals.

En aquest sentit, la protecció de dades és un dret fonamental que es veu especialment afectat pels sistemes d'IA i que té una relació estreta amb el principi de prevenció del dany. Aquest principi comença per una gestió adequada d'aquestes dades, que abasti la qualitat i la integritat de les que s'utilitzen, la seva pertinència en contrast amb l'àmbit en què es desplegaran els sistemes d'IA, els seus protocols d'accés i la capacitat per processar dades sense vulnerar la privacitat.

Entre aquestes mesures s'inclou el fet que els sistemes d'IA disposin d'un mecanisme de gestió de la privacitat i de les dades que inclogui tant el respecte de la privacitat com la qualitat i la integritat de les dades i l'accés a aquestes dades.

A més, els sistemes d'IA han de garantir la protecció de les dades al llarg de tot el seu cicle de vida. Això inclou tant la informació inicialment facilitada per l'usuari com la que es genera sobre ell en el context de la seva interacció amb el sistema (per exemple, els productes que genera el sistema d'IA per a determinats usuaris o la resposta d'aquests usuaris a certes recomanacions). Els registres digitals del comportament humà poden fer possible que els sistemes d'IA no només infereixin les preferències de les persones, sinó també l'orientació sexual, l'edat, el sexe o les opinions polítiques i religioses. Perquè els individus confiïn en el procés de recopilació de dades, cal garantir que la informació recollida sobre ells no s'utilitzarà per discriminar-los de manera injusta o il·legal.

Del compliment d'aquests requisits se n'han d'encarregar els operadors, en particular, els desenvolupadors dels sistemes d'IA i els responsables del desplegament (que cal que s'assegurin que els sistemes que utilitzen i els productes i els serveis que ofereixen compleixen els requisits establerts). D'altra banda, les persones que es vegin afectades pel funcionament d'un sistema d'IA tenen dret a estar informades d'aquesta afectació i, si escau, presentar una reclamació per infracció del RIA (arts. 85 i 86).

El article 2.7 del RIA recull el principi general que el propi RIA respecta íntegrament el marc regulador de la UE en matèria de protecció de dades que estableix l'RGPD.

2.1. La privacitat en el RIA

L'article 2.7 del RIA recull el principi general que el propi RIA respecta íntegrament el marc regulador de la UE en matèria de protecció de dades que estableix l'RGPD.

En primer lloc, les normes harmonitzades que s'estableixen en el RIA s'han d'aplicar a tots els sectors i s'han d'entendre sens perjudici del dret vigent de la UE. És important destacar, doncs, que el RIA no pretén afectar l'aplicació del dret de la UE que regula el tractament de dades personals, incloses les funcions i les competències de les autoritats de supervisió independents que vigilen el compliment d'aquests instruments. De la mateixa manera, tampoc no afecta les obligacions prèvies dels proveïdors i els encarregats del desplegament de sistemes d'IA com a responsables del tractament de dades personals. En particular, el RIA no ha d'afectar les pràctiques actualment prohibides pel dret de la UE, incloent-hi els drets en matèria de protecció de dades.

En paral·lel, el fet que un sistema d'IA sigui classificat com d'alt risc no s'ha d'interpretar com un indicador que el seu ús sigui lícit d'acord amb altres actes del dret de la UE o del dret nacional, per exemple, en matèria

de protecció de dades personals. Tots els usos d'aquest tipus de sistemes d'IA s'han de continuar fent exclusivament d'acord amb els requisits oportuns derivats de la Carta, el dret derivat de la UE i el dret nacional.

A més, el RIA no constitueix un fonament jurídic per al tractament de dades personals, incloses les categories especials de les dades esmentades, llevat que es disposi específicament una altra cosa. Per això, arran de l'entrada en vigor del RIA les persones interessades continuen gaudint de tots els drets i les garanties que els confereix el dret de la UE, inclosos els que estan relacionats amb les decisions individuals totalment automatitzades, com ara l'elaboració de perfils. Així doncs, les normes harmonitzades que estableix el RIA han de permetre l'exercici dels drets i d'altres vies de recurs dels interessats garantits pel dret de la UE en matèria de protecció de dades personals i altres drets fonamentals.

Per a les ciutats, garantir que els seus sistemes d'IA compleixen regulacions com l'RGPD o el RIA al llarg de tot el cicle de vida de la IA és fonamental per salvaguardar els drets dels ciutadans i mantenir la confiança pública

Finalment, per tal de facilitar el compliment del dret de la UE en matèria de protecció de dades, en determinades condicions, el RIA proporciona la base jurídica perquè, en un entorn controlat de proves, els proveïdors (també els potencials) utilitzin dades personals recollides per a altres finalitats per desenvolupar determinats sistemes d'IA en favor de l'interès públic.

3. Mecanismes polítics per implementar el principi de privacitat en l'àmbit urbanístic

La protecció de la privacitat i de les dades a l'hora d'implementar la IA urbana requereix l'adopció de mecanismes polítics específics, els quals permeten a les ciutats complir les normatives vigents i assegurar que la IA es desplega de manera ètica i responsable, respectant els drets dels ciutadans. Tot seguit, s'identifiquen i expliquen els principals mecanismes polítics per implementar aquest principi ètic.

a) Garantia de la conformitat legal

El compliment de la regulació és un requisit ètic essencial en la protecció de la privacitat i les dades a l'hora d'implementar sistemes d'IA en entorns urbans per part de les autoritats públiques. Per a les ciutats, garantir que els seus sistemes d'IA compleixen regulacions com l'RGPD o el RIA al llarg de tot el cicle de vida de la IA és fonamental per salvaguardar els drets dels ciutadans i mantenir la confiança pública. Això inclou l'adhesió a requeriments clau com la qualitat i la integritat de les dades utilitzades, la seva pertinència en contrast amb l'àmbit en què es desplegaran els sistemes d'IA, els seus protocols d'accés i la capacitat per processar dades sense vulnerar la privacitat (Grup d'experts d'alt nivell sobre intel·ligència artificial, 2019).

Precisament, aquests requeriments es materialitzen en obligacions concretes al mateix RIA, específicament dissenyades per a casos d'alt risc, com ara els sistemes d'IA d'identificació biomètrica remota —per exemple, el programa ABIS (Pascual, 2024)— o els que s'utilitzen per avaluar si les persones físiques compleixen els requisits per beneficiar-se de serveis i prestacions essencials d'assistència pública —per exemple, el cas Syri (Digital Future Society, 2022).

b) Sistemes de gestió de risc i governança de dades

El RIA inclou obligacions específiques (arts. 9 i 10) estretament vinculades al principi de privacitat i protecció de dades. D'una banda, l'article 9 se centra en la creació d'un sistema de gestió de riscos que sigui capaç d'identificar, documentar i mitigar els riscos associats a l'ús d'IA a les ciutats. Aquests sistemes de gestió de riscos han d'establir processos iteratius continus, planificats i executats al llarg de tot el cicle de vida de les tecnologies d'IA, que, per descomptat, requeriran revisions i actualitzacions sistemàtiques periòdiques. De fet, no es tracta només d'avaluar els possibles riscos abans de la introducció al mercat o posada en servei d'aquests sistemes d'IA, sinó també establir i/o supervisar el funcionament d'un sistema de vigilància postcomercialització per gestionar riscos emergents –arts. 17.1 h), 26.5 i 72 RIA–.

D'altra banda, la governança de dades regulada a l'article 10 exigeix que els conjunts de dades d'entrenament, validació i prova utilitzats en sistemes d'IA d'alt risc se sotmetin a pràctiques de governança i gestió de dades adequades per a la finalitat prevista. Les pràctiques que han d'implementar les ciutats per assegurar una governança de dades efectiva i legal s'han de centrar en qüestions com ara els processos de recollida i origen de les dades, la finalitat del tractament, l'avaluació de la disponibilitat, la quantitat i l'adequació dels conjunts de dades necessàries, l'examen de possibles biaixos que puguin afectar la salut, la seguretat o els drets fonamentals de les persones, etc.

c) Avaluacions d'impacte

L'article 35 de l'RGPD imposa als responsables del tractament (per exemple, ajuntaments) l'obligació de fer una avaluació d'impacte relativa a la protecció de dades (AIPD). Aquesta avaluació s'ha de fer quan sigui probable que un tipus de tractament, per la seva naturalesa, abast, context o finalitat (en particular si utilitza noves tecnologies), comporti un alt risc per als drets i les llibertats de les persones físiques (AEPD, 2018; Grup de Treball de l'Art. 29, 2017; Friedewald *et al*., 2022). Aquest enfocament preventiu és fonamental als entorns urbans per anticipar possibles vulnerabilitats en la protecció de dades i prendre les mesures necessàries per corregir-les a temps.

Així mateix, per als sistemes d'IA d'alt risc, l'article 27 del RIA introdueix l'obligació de fer una avaluació d'impacte relativa als drets fonamentals (FRAI) (Govern dels Països Baixos, 2022; Institut Danès de Drets Humans, 2020), que complementi l'AIPD. Aquesta avaluació té com a objectiu determinar els riscos específics per als drets de les persones que probablement se'n vegin afectades i definir les mesures que s'han d'adoptar en cas que es materialitzin aquests riscos (considerant 96 RIA). Cal destacar que les avaluacions d'impacte (Manzoni *et al*., 2022) s'han de centrar no només en el retorn de la inversió, sinó també en la sostenibilitat i l'impacte ètic de la tecnologia, abordant aspectes financers, humans i mediambientals (OECD, 2024).

d) Auditories

A continuació, cal poder demostrar davant les autoritats, les parts interessades i els ciutadans que es compleix la legislació i tots els seus requisits específics d'implementació. En aquest sentit, cal dur a terme

auditories internes i externes i obtenir certificacions que verifiquin que els sistemes operen dins els marcs legals establerts. Per això, les ciutats europees, per exemple, han de fer avaluacions de conformitat (art. 43 RIA) per tal de garantir i demostrar que han complert els requisits associats a sistemes d'alt risc, de conformitat amb les normes harmonitzades publicades en el *Diari Oficial de la Unió Europea* (art. 41 RIA). També han de seguir les especificacions comunes establertes per la Comissió Europea, assegurant així una implementació estandarditzada i segura dels sistemes d'IA (per exemple, certificacions ISO).

Les auditories d'IA es consideren un mecanisme de governança fonamental per assegurar que la implementació i l'operació dels sistemes d'IA compleixen les normatives legals i els estàndards ètics i tècnics establerts (Fernández i Eguíluz, 2024). Amb caràcter general, aquestes auditories les han de dur a terme entitats independents i competents. El procés d'auditoria inclou metodologies que incorporen avaluacions d'impacte ètic (UNESCO, 2024; CEN-CENELEC, 2017), que asseguren que els sistemes d'IA es comporten de manera responsable i que els seus efectes en la societat i els individus són degudament monitorats i mitigats. No obstant això, és recomanable plantejar les auditories d'IA des d'un punt de vista multidisciplinari –legal, tècnic i ètic– (Mökander, 2023). En aquest sentit, sorgeixen propostes com la d'Algo Score per classificar i avaluar de manera accessible el nivell de conformitat dels sistemes algorítmics en matèries com el compliment ètic, la governança de la IA, l'equitat del model i la seva vigilància posterior, seguint un enfocament similar al de les etiquetes d'eficiència energètica (Galdon, 2024).

e) Repositoris d'algoritmes i registres de sistemes d'IA

En darrer lloc, convé recordar la importància dels repositoris d'algoritmes públics i els registres de sistemes d'IA (art. 49 RIA), que promouen la transparència en la presa de decisions automatitzades en el sector públic i tenen un paper crucial en la protecció de la privacitat i les dades personals. En fer accessibles els detalls sobre com es dissenyen, implementen i operen aquests sistemes, els repositoris i els registres permeten als ciutadans i a les organitzacions entendre com s'utilitzen les dades personals en aquests processos i amb quines finalitats. Aquests repositoris inclouen també informació sobre les fonts de les dades utilitzades i els mecanismes de supervisió, cosa que és essencial per avaluar l'impacte dels sistemes en la privacitat dels individus i garantir que les mesures de protecció de dades siguin efectives (Gutiérrez i Muñoz-Cadena, 2024).

4. Reptes i recomanacions

La gestió inadequada de les dades és una de les principals limitacions per a la implementació d'IA en el sector públic. Igualment, també ho és la manca d'accés a volums suficients de dades d'alta qualitat. Aquest problema es veu agreujat per l'intercanvi insatisfactori de dades entre organitzacions per la manca d'estàndards unificats i una governança de dades poc desenvolupada. A més, la desconfiança en els sistemes d'IA agreuja aquests reptes. La dispersió de les lleis i el coneixement insuficient sobre els impactes de la IA també generen barreres significatives (Manzoni *et al*., 2023). Així mateix, l'augment de ciberatacs ha fet que

la Directiva NIS 2 (2022) reforci la seguretat i la responsabilitat legal per als administradors. L'any 2023, l'Administració pública va ser un dels sectors més afectats, amb el 19 % dels incidents reportats, entre els quals destaca l'augment del nombre d'atacs, com ara el programari de segrest (o *ransomware*) i l'atac DDoS (ENISA, 2023).

El complex panorama regulador també suposa un repte significatiu. La interacció entre les normatives urbanístiques europees, estatals i locals crea un entramat de regles que complica la implementació efectiva d'IA a les ciutats. La legislació urbanística i les regulacions específiques de cada municipi s'han d'adaptar a les normatives europees com el Reglament sobre l'Europa Interoperable (Interoperable Europe Act) (2022), que cerca millorar la interoperabilitat dels serveis públics digitals (Tangi *et al*., 2023).

Una altra limitació important és la manca d'experiència i de coneixement tècnic que hi ha al si de les administracions locals, cosa que dificulta la implementació de la IA de manera adequada. L'escassetat de professionals especialitzats en aquesta matèria arreu del món i la creixent competència pel talent representen una barrera significativa per a les ciutats que intenten desenvolupar i desplegar aquests sistemes de manera efectiva (OECD, 2024).

D'altra banda, la recollida massiva de dades personals, necessària per entrenar aquests sistemes, pot vulnerar el dret dels ciutadans a controlar les seves dades, ja que poden ser dades sensibles o gestionades de manera inapropiada. A més, les aplicacions d'IA, com les que es fan servir en el control policial, poden intensificar la vigilància massiva i comprometre encara més la privacitat dels individus (Véliz, 2020; Agarwal, 2018; Dwivedi *et al*., 2019).

Per superar aquestes barreres, és essencial promoure mecanismes d'innovació, com els *sandboxes* reguladors (Madiega, 2022), que permeten a les ciutats experimentar amb IA en un entorn controlat mentre es garanteix el compliment regulador (Tangi *et al*., 2023). Així mateix, la coordinació entre les autoritats estatals (en el cas espanyol, l'Agència Espanyola de Supervisió de la Intel·ligència Artificial - AESIA) i europees (l'Oficina Europea d'Intel·ligència Artificial) és crucial per garantir que els sistemes d'IA compleixin les normatives vigents i s'implementin de manera segura i responsable.

És essencial promoure mecanismes d'innovació, com els *sandboxes* reguladors, que permeten a les ciutats experimentar amb IA en un entorn controlat mentre es garanteix el compliment regulador.

La interoperabilitat i la col·laboració són igualment clau. Iniciatives com el sistema SALER - Sistema d'Alertes Ràpides, utilitzat a la Comunitat Valenciana per prevenir la corrupció a l'Administració, demostren que la IA es pot utilitzar de manera efectiva per millorar els processos de governança (Digital Future Society, 2023). Igualment, és essencial que el finançament públic estigui condicionat a l'assoliment de certs resultats per part de les diferents administracions (per exemple, generar conjunts de dades públiques) (Comissió Europea, 2022). En aquest sentit, la Comissió Europea ha publicat, mitjançant el Reglament d'execució (UE) 2023/138, una llista de conjunts de dades específiques d'alt valor que han d'estar disponibles per a la reutilització gratuïta, cosa que destaca el potencial de les dades públiques en benefici de la societat, el medi ambient i l'economia (Comissió Europea, 2022). A més, l'accés a dades multilingües per entrenar models locals d'IA que reflecteixin les carac-

terístiques específiques de cada regió (OECD, 2024) i la recopilació de casos d'ús d'IA en el sector públic europeu (Comissió Europea, 2021) milloraran l'efectivitat i l'equitat dels sistemes d'IA i alhora seran una valuosa font d'informació sobre com es van implementant aquestes tecnologies en diversos contextos.

5. Conclusions

El marc general de protecció de dades a la UE ja està establert en uns principis coneguts i sòlidament interpretats pels organismes administratius i jurisdiccionals de la UE. Tot i això, la IA planteja problemes específics, de caràcter tecnològic i jurídic, el coneixement i el tractament dels quals encara són incipients.

Per això, encara calen nombrosos estudis, experiències i precisions per dotar-los d'un marc jurídic que garanteixi la finalitat proclamada que la IA ha d'estar centrada en l'ésser humà, ser una eina per a les persones i tenir com a objectiu últim millorar el seu benestar.

La implementació de mecanismes polítics específics és essencial per garantir que les ciutats utilitzin sistemes d'IA de manera ètica i respectuosa amb els drets de la ciutadania. El compliment de regulacions com l'RGPD i el RIA resulta indispensable per salvaguardar la privacitat i les dades personals en entorns urbans. De la mateixa manera, és fonamental que les ciutats estableixin sistemes de gestió de riscos que abordin de manera iterativa les contingències associades a tot el cicle de vida de la IA, incloent-hi revisions periòdiques i auditories externes que assegurin el compliment normatiu.

D'altra banda, la governança de dades ha de ser el centre de les estratègies urbanes d'IA. Les ciutats han d'implementar pràctiques de governança i gestió de dades sòlides, centrades en la qualitat, la pertinència i la protecció dels conjunts de dades emprats als sistemes d'IA. Això inclou dur a terme avaluacions d'impacte tant per a la protecció de dades personals com per als drets fonamentals per assegurar que les tecnologies implementades no vulnerin la privacitat ni la seguretat de la ciutadania.

En definitiva, aconseguir una IA centrada en l'ésser humà exigeix un esforç conjunt entre els responsables de desenvolupar polítiques públiques, les institucions acadèmiques i els sectors privats, que han de col·laborar per assegurar que els sistemes d'IA que implementin les ciutats concordin amb els valors i els principis ètics fonamentals.

Com hem assenyalat, el futur de les ciutats intel·ligents es caracteritzarà per la combinació de múltiples tecnologies orientades a satisfer l'intricat mosaic de necessitats humanes. Aquesta convergència requereix una optimització precisa de les tecnologies aplicades que asseguri que la digitalització dels espais urbans està en consonància amb pràctiques sostenibles i equitatives, així com l'atenció a les dimensions ètiques que aquestes innovacions comporten. Per això, és imperatiu que la integració de la IA al si de les ciutats intel·ligents es regeixi per principis que defensin la privacitat, la seguretat i la inclusió. En aquest sentit, i com apunten Zhenjun *et al*. (2023), "garantir que els beneficis del desenvolupament de

les ciutats intel·ligents es comparteixin equitativament és essencial per evitar fractures socials i fomentar un entorn en què la tecnologia serveixi de pont cap a una vida urbana més il·lustrada i harmoniosa".

Referències bibliogràfiques

Agencia Española de Protección de Datos (AEPD). «Gestión del riesgo y evaluación de impacto en tratamientos de datos personales». Madrid, 2018 [Data de consulta: 02.09.2024]

Agencia Española de Protección de Datos. «Guía sobre protección de datos y administración local». Actualitzada el 2023 [Data de consulta: 02.09.2024]

AI Ethics Impact Group. «From Principles to Practice: An interdisciplinary framework to operationalise AI ethics». 1 d'abril de 2020 [Data de consulta: 02.09.2024]

Alan Turing Institute. «Urban analytics» [Data de consulta: 02.09.2024]

Alan Turing Institute. «Why the public sector needs to know about AI ethics (and how we're helping)». 2 de novembre de 2023 [Data de consulta: 02.09.2024]

Almonacid Lamelas, V. «Reglamento (europeo) de Inteligencia Artificial: impactos y obligaciones que genera en los Ayuntamientos». El Consultor de los Ayuntamientos, LA LEY, 15 de juliol de 2024 [Data de consulta: 02.09.2024]

Burbano, L. (1). «Privacy protection in smart cities: How are they taking care of citizens' most precious information?» Tomorrow.city, 23 de gener de 2024 [Data de consulta: 02.09.2024]

Burbano, L. (2). «AI urbanism: risks and benefits of a seemingly unstoppable movement». Tomorrow.city, 22 de febrer de 2024 [Data de consulta: 02.09.2024]

Canda, J. «AI in Urban Planning and Smart City Development». Medium, 7 d'abril de 2024 [Data de consulta: 02.09.2024]

CEN-CENELEC. «Ethics assessment for research and innovation - Part 2: Ethical impact assessment framework». CWA 17145-2, juny de 2017 [Data de consulta: 02.09.2024]

Centro Latinoamericano de Administración para el Desarrollo (CLAD). «Carta Iberoamericana de Inteligencia Artificial en la Administración Pública». 20 de novembre de 2023 [Data de consulta: 02.09.2024]

Comissió Europea (1). «Selected AI cases in the public sector (JRC129301)». Joint Research Centre (JRC), 2021 [Data de consulta: 02.09.2024]

Comissió Europea (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 [Data de consulta: 02.09.2024]

Comissió Europea (3). «Opportunities and challenges of artificial intelligence technologies for the cultural and creative sectors». Oficina de Publicaciones de la UE, Luxemburg, 2022 [Data de consulta: 02.09.2024]

Comissió Europea (4). «Second Report on the application of the General Data Protection Regulation», COM(2024) 357 final, Brussel·les, 25 de juliol de 2024 [Data de consulta: 02.09.2024]

Digital Future Society (1). «Algorithmic discrimination in Spain: limits and potential of the legal framework», agost de 2022 [Data de consulta: 02.09.2024]

Digital Future Society (2). «El acceso digital en las ciudades, entendido como algo más que un derecho fundamental», juny de 2023 [Data de consulta: 02.09.2024]

Digital Future Society (3). «El uso de algoritmos en el sector público en España: cuatro estudios de caso sobre ADMS», febrer de 2023 [Data de consulta: 02.09.2024]

European Data Protection Board (EDPB). «Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework», 16 de juliol de 2024 [Data de consulta: 02.09.2024]

European Union Agency for Cybersecurity (ENISA). «Threat Landscape 2023», octubre de 2023 [Data de consulta: 02.09.2024]

Fernández, C. i Eguiluz, J. A. «Diez puntos críticos del Reglamento europeo de Inteligencia Artificial». Diario LA LEY, núm. 85, Sección Ciberderecho, 28 de juny de 2024 [Data de consulta: 02.09.2024].

Friedewald, M. *et al*. «Data Protection Impact Assessments in Practice: Experiences from Case Studies». Computer Security, ESORICS 2021 International Workshops, febrer de 2022, p. 424-443 [Data de consulta: 02.09.2024]

Galceran-Vercher, M. «Trustworthy Cities: Ethical Urban Artificial Intelligence». The GovLab, Course «AI Ethics, Global perspectives», desembre de 2023 [Data de consulta: 02.09.2024]

Galceran-Vercher, M. i Vidal, A. «Mapping urban artificial intelligence: first report of GOUAI's Atlas of Urban AI». Global Observatory of Urban Artificial Intelligence (GOUAI), 2024 [Data de consulta: 02.09.2024]

Galdon, G. «AI Auditing. Proposal for Algo-scores». EDPB, 27 de juny de 2024 [Data de consulta: 02.09.2024]

Ghisleni, C. «Artificial Intelligence and Urban Planning: Technology as a Tool for City Design». ArchDaily, 8 de febrer de 2024 [Data de consulta: 02.09.2024]

Govern dels Països Baixos. «Impact Assessment Fundamental Rights and Algorithms», 31 de març de 2022 [Data de consulta: 02.09.2024].

Grup d'experts d'alt nivell sobre intel·ligència artificial. «Directrices éticas para una IA fiable», abril de 2019 [Data de consulta: 02.09.2024]

Grup de treball de l'Art. 29. «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», Brussel·les, 2017 [Data de consulta: 02.09.2024]

Gutiérrez, J. D. i Muñoz-Cadena, S. «Algorithmic transparency in the public sector: A state-of-the-art report of algorithmic transparency instruments». Global Partnership on Artificial Intelligence, maig de 2024 [Data de consulta: 02.09.2024]

Hadec, J., Di Leo, M. i Kotsev, A. «AI generated synthetic data in policy applications». *Science for Policy Brief*, European Commission, Joint Research Center, 2024 [Data de consulta: 02.09.2024]

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

Institut Danès de Drets Humans. «Guidance on Human Rights Impact Assessment of Digital Activities». Copenhaguen, 2020 [Data de consulta: 02.09.2024]

Madiega, T. i Van De Pol, A. L. «Artificial intelligence act and regulatory sandboxes». European Parliamentary Research Service (EPRS), PE 733.544, juny de 2022 [Data de consulta: 02.09.2024]

Manzoni, M. *et al.* «AI Watch. Road to the adoption of Artificial Intelligence by the public sector». Oficina de Publicaciones de la UE. Luxemburg, 2022. JRC129100 [Data de consulta: 02.09.2024]

Mökander, J. «Auditing of AI: Legal, Ethical and Technical Approaches». Digital Society, vol. 2, art. núm. 49, 2023 [Data de consulta: 02.09.2024]

Organización de Naciones Unidas (ONU). «Recommendation on the Ethics of Artificial Intelligence», 23 de novembre de 2021 [Data de consulta: 02.09.2024]

Organización para la Cooperación y el Desarrollo Económico (OCDE) (1). «Advancing Accountability in AI: governing and managing risks throughout the lifecycle for trustworthy AI», OECD Artificial Intelligence Papers, núm. 349, 23 de febrer de 2023 [Data de consulta: 02.09.2024]

Organización para la Cooperación y el Desarrollo Económico (OCDE) (2). «Governing with artificial intelligence: Are governments ready?», OECD Artificial Intelligence Papers, núm. 20, juny de 2024 [Data de consulta: 02.09.2024]

Pascual, M. G. «La Policía española ya usa en sus investigaciones un sistema automático de reconocimiento facial». El País, 28 de maig de 2024 [Data de consulta: 02.09.2024]

Pellegrin, J., Colnot, L. i Delponte, L. «Artificial Intelligence and Urban Development». Research for REGI Committee, European Parliament, Policy Department for Structural and Cohesion Policies, Brussel·les, 2021 [Data de consulta: 02.09.2024]

Tangi, L. *et al.* «Artificial Intelligence for Interoperability in the European Public Sector: an exploratory study», Oficina de Publicaciones de la UE, Luxemburg, 2023 [Data de consulta: 02.09.2024]

Tangi, L. *et al.* «AI Watch. European Landscape on the Use of Artificial Intelligence by the Public Sector», Oficina de Publicaciones de la UE, Luxemburg, 2022 [Data de consulta: 02.09.2024]

Timan, T., Van Veenstra, A. F. i Bodea, G. «Artificial Intelligence and public services». Policy Department for Economic, Scientific and Quality of Life Policies, PE 662.936, juliol de 2021 [Data de consulta: 02.09.2024]

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» [Data de consulta: 02.09.2024]

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 de desembre de 2023 [Data de consulta: 02.09.2024]