Revista Catalana d'Administració Pública
[Societat Catalana d'Estudis Jurídics], núm. 2 (desembre 2024), p. 83-118
ISSN: 2938-5733 / DOI: 10.2436/20.3004.04.21
https://revistes.iec.cat/index.php/RCAP
Data de lliurament: 12 de novembre de 2024
Data de l'avaluació cega: 15 de novembre de 2024 i 25 de novembre de 2024
Data d'acceptació: 25 de novembre de 2024

ELS RISCOS PER A LA PRIVACITAT EN UN ENTORN TECNOLÒGIC GENERATIU. UN CAS D'ÚS: LES CIUTATS INTEL·LIGENTS (*SMART CITIES*)[1]

Xavier Urios Aparisi
Cap de l'Assessoria Jurídica
Autoritat Catalana de Protecció de Dades

Resum

En aquests moments ens trobem en l'anomenada *revolució industrial 5.0*, caracteritzada per la relació simbiòtica entre humans i màquines per a augmentar les capacitats de les persones i millorar-ne les condicions de vida, incloent-hi les condicions de treball.

Ja no es tracta de l'internet de les coses o de l'ús de les dades per a millorar els processos de fabricació i decisió, sinó que estem anant molt més enllà, perquè la implantació de sistemes d'intel·ligència artificial i la compartició de dades estan canviant de manera significativa els processos de decisió humana i, alhora, els riscos per a la privacitat s'han incrementat substancialment.

En aquest article analitzarem el concepte de *dada personal* des del punt de vista de la normativa de protecció de dades, que el configura d'una manera àmplia amb la voluntat de protegir la persona dels riscos d'identificabilitat que afectin la seva privacitat com a conseqüència de la implementació massiva de les tecnologies disruptives i, en particular, dels sistemes d'intel·ligència artificial.

En la part final d'aquest article analitzarem un cas d'ús: el paper de la protecció de dades en el context de les ciutats intel·ligents (*smart cities*). Avaluarem la complexitat que el tractament de dades implica en aquests entorns i els aspectes que cal considerar per a salvaguardar la privacitat de les persones.

Paraules clau: protecció de dades, intel·ligència artificial, ciutats intel·ligents, Administració.

LOS RIESGOS PARA LA PRIVACIDAD EN UN ENTORNO TECNOLÓGICO GENERATIVO. UN CASO DE USO: LAS CIUDADES INTELIGENTES (*SMART CITIES*)

Resumen

En estos momentos nos encontramos en la llamada *revolución industrial 5.0*, caracterizada por la relación simbiótica entre humanos y máquinas para aumentar las capacidades de las personas y mejorar sus condiciones de vida, incluyendo las condiciones de trabajo.

1. Citació recomanada: Urios Aparisi, Xavier (2024). «Els riscos a la privacitat en un entorn tecnològic generatiu. Un cas d'ús: les ciutats intel·ligents (*smart cities*)». *Revista Catalana d'Administració Pública*, núm. 2, p. 83-118.

Ya no se trata del internet de las cosas o del uso de los datos para mejorar los procesos de fabricación y decisión, sino que estamos yendo mucho más allá, puesto que la implantación de sistemas de inteligencia artificial y la compartición de datos están cambiando de manera significativa los procesos de decisión humana y, al mismo tiempo, los riesgos para la privacidad se han incrementado sustancialmente.

En este artículo analizaremos el concepto de *dato personal* desde el punto de vista de la normativa de protección de datos, que lo configura de una manera amplia con la voluntad de proteger a la persona de los riesgos de identificabilidad que afecten a su privacidad como consecuencia de la implementación masiva de las tecnologías disruptivas y, en particular, de los sistemas de inteligencia artificial.

En la parte final de este artículo analizaremos un caso de uso: el papel de la protección de datos en el contexto de las ciudades inteligentes (*smart cities*). Evaluaremos la complejidad que el tratamiento de datos implica en estos entornos y los extremos a considerar para salvaguardar la privacidad de las personas.

Palabras clave: protección de datos, inteligencia artificial, ciudades inteligentes, Administración.

PRIVACY RISKS IN DISRUPTIVE TECHNOLOGIES ENVIRONMENT. A USE CASE: SMART CITIES

Abstract

At the moment, we are in the so-called *industrial revolution 5.0*, characterized by the symbiotic relationship between humans and machines to increase people's capacities and improve people's living conditions, including working conditions.

It is no longer about the Internet of Things, or the use of data to improve manufacturing and decision-making processes, but we are going much further, as the implementation of artificial intelligence systems and data sharing are significantly changing human decision-making processes and, in the same way, Privacy risks have increased substantially.

In this article we will analyse the concept of *personal data* from the point of view of data protection regulations, which configure it in a broad way, with the aim of protecting the individual from the risks of identifiability that affect their privacy, as a result of the massive implementation of disruptive technologies and, in particular, artificial intelligence systems.

In the final part of this article we will analyse a use case: the role of data protection in the context of smart cities, assessing the complexity that data processing involves in these environments, and the extremes to be considered, to safeguard people's privacy.

Keywords: data protection, artificial intelligence, smart cities, Administration.

1. INTRODUCCIÓ

L'objectiu d'aquest treball és analitzar els riscos per a la privacitat de les persones, que avui, arran de la irrupció de les tecnologies disruptives, s'han incrementat substancialment.

El concepte de *noves tecnologies*, relacionat tradicionalment amb les innovacions tecnològiques, ha estat superat pel concepte de *tecnologies disruptives*. Com indica Piñar Mañas[2] (la traducció és nostra):

> El disruptiu és el que produeix disrupció, que, segons el diccionari de la RAE, és «trencament o interrupció brusca» (com recorda el mateix diccionari, deriva de l'anglès *disruption*, i aquest, del llatí *disrupti*, -ōnis, variació de *dirupti*, -ōnis, «trencament, fractura»). La innovació tecnològica (ja no té sentit parlar de «noves tecnologies», ja que van deixar de ser noves fa temps) suposa avenços inqüestionables per a la societat, però alhora pot tancar grans reptes, si no riscos o veritables amenaces, per al dret en general i certs drets fonamentals en particular. Va ser Clayton M. Christensen (1997) qui primer va utilitzar l'expressió *disruptive* el 1997 pel que fa a tecnologies que exigien un canvi radical respecte al passat per a començar una nova etapa gairebé des de zero. Es tractava de tecnologies d'evolució no gradual, sinó «rupturista», a les quals el dret ha de fer front, ja que formen part de la realitat vital de l'ésser humà avui. I ho faran en el futur, que és, senzillament, impredictible.

La intel·ligència artificial (IA), màxim exponent de les tecnologies disruptives, fonamenta els seus processos de decisió en l'aprenentatge i el tractament de dades. Per aquesta

2. José Luis Piñar Mañas, «Derecho, ética e innovación tecnológica», *Revista Española de Derecho Administrativo*, núm. 195 (2018), secció «Estudios».

raó, les tecnologies disruptives més conegudes, com la IA i el big data, tenen per objecte millorar les capacitats de les persones i les seves condicions de vida i de treball. Els seus processos de decisió se centren en les dades que tracten i, per aquesta raó, si són dades personals, el compliment de la normativa de protecció de dades és un paràmetre que s'ha de considerar.

2. CONCEPTE DE *DADA PERSONAL* I IDENTIFICABILITAT DE LA PERSONA

Això ens obliga a parlar prèviament del concepte de *dada personal*, ja que moltes vegades els ciutadans no som conscients que es tracta d'un concepte molt ampli i, al mateix temps, no ens adonem dels riscos per a la nostra privacitat que es deriven de la possibilitat de ser identificats partint de dades que, aparentment, no ho haurien de permetre.

Avui en dia, el *big data*[3] i la IA[4] han canviat les regles del joc. Es tracta de tecnologies diferents però que són interdependents, ja que la combinació de les dues fa que la segona desplegui la seva potencialitat al màxim, no tan sols quant als resultats de sortida, sinó també quant a la possibilitat d'identificar i perfilar les persones.

Com indica Valero Torrijo, ens trobem davant del següent estat evolutiu de la innovació tecnològica:[5]

> Doncs bé, certament, aprofitant les possibilitats del *big data*, però, a més, la capacitat d'aprenentatge autònom que permet la tecnologia actual, ens trobem davant d'un canvi qualitatiu molt destacat, ja que permet en molts casos fer el salt des de la simple anàlisi a la potencial decisió sense intervenció directa d'una persona humana, i fins i tot a la formulació de previsions (Tinholt *et al*., 2017), amb la capacitat addicional de reconfiguració dels criteris si es detectés algun tipus d'error o desviació. No es tracta, doncs, de noves solucions als problemes actuals, sinó, per contra, de noves metodologies (Verhulst i Young, 2017) que permeten afrontar la presa de decisions des de paràmetres més refinats i, almenys potencialment, també més precisos, però també més invasius.

Tornant al concepte de *dada personal*, l'article 4.1 del Reglament (UE) 2016/679 del Parlament i del Consell, del 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de les dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (en endavant, RGPD), defineix les dades personals com:

3. El big data és un concepte que descriu un gran volum de dades que creix de manera exponencial amb el pas del temps. En poques paraules, és un conjunt de dades tan gran i complex que cap de les eines tradicionals de dades és capaç d'emmagatzemar-les o processar-les de manera eficient.

4. Sistema d'IA (article 3, apartat 1, del RIA): sistema basat en una màquina que està dissenyat per a funcionar amb diferents nivells d'autonomia i que pot mostrar capacitat d'adaptació després del desplegament, i que, per a objectius explícits o implícits, infereix de la informació d'entrada que rep la manera de generar resultats de sortida, com prediccions, continguts, recomanacions o decisions, que poden influir en entorns físics o virtuals.

5. Julián Valero Torrijo, «Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración», *Revista Catalana de Dret Públic*, núm. 58 (2019); la traducció és nostra.

> [...] qualsevol informació sobre una persona física identificada o identificable (l'interessat). S'ha de considerar persona física identificable qualsevol persona la identitat de la qual es pot determinar, directament o indirectament, en particular mitjançant un identificador, com, per exemple, un nom, un número d'identificació, dades de localització, un identificador en línia o un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social [...].[6]

Hem de tenir en compte que l'element determinant és la «identificabilitat» d'una persona i que, des del moment en què en un context determinat puguem vincular qualsevol informació a una persona, estarem tractant dades.

Aquesta identificabilitat va ser tractada pel Grup de protecció de les persones pel que fa al tractament de les dades personals, creat per l'article 29 de la Directiva 95/46/CE, que en el Dictamen 4/2007, sobre el concepte de *dades personals*, adoptat el 20 de juny (document WP 136), ja va recordar que és possible parlar de l'existència de dades personals fins i tot en supòsits en què no es té una identificació singularitzada de l'interessat, i va indicar:

> [...] convé assenyalar que si bé la identificació a través del nom i els cognoms és a la pràctica la més habitual, aquesta informació pot no ser necessària en tots els casos per a identificar una persona. Així pot succeir quan s'utilitzen altres «identificadors» per a singularitzar algú. Efectivament, els fitxers informatitzats de dades personals solen assignar un identificador únic a les persones registrades per a evitar tota confusió entre dues persones incloses en el fitxer. També a internet, les eines de control del trànsit permeten identificar amb facilitat el comportament d'una màquina i, per tant, el de l'usuari que es troba al darrere. Així doncs, s'uneixen les diferents peces que componen la personalitat de l'individu per tal d'atribuir-li determinades decisions. Sense ni tan sols sol·licitar el nom i la direcció de la persona, és possible incloure-la en una categoria sobre la base de criteris socioeconòmics, psicològics, filosòfics o d'un altre tipus, i atribuir-li determinades decisions, ja que el punt de contacte de l'individu (un ordinador) fa innecessari conèixer la seva identitat en sentit estricte. En altres paraules, la possibilitat d'identificar una persona ja no equival necessàriament a la capacitat de poder arribar a conèixer-ne el nom i els cognoms. La definició de *dades personals* reflecteix aquest fet. [...] Les autoritats nacionals de protecció de dades s'han enfrontat a casos en què el responsable del tractament sostenia que només s'havien tractat informacions disperses, sense referències a noms o altres identificadors directes, i advocava perquè les dades no es consideressin com a personals i no estiguessin subjectes a les normes de protecció de les dades. I, tanmateix, el tractament d'aquesta informació només cobrava sentit si permetia la identificació d'individus concrets i el seu tractament d'una manera determinada. En aquests casos, en què la finalitat del tractament implica la identificació de persones, es pot assumir que el responsable del tractament o qualsevol altra persona implicada té o pot tenir mitjans que «puguin ser raonablement utilitzats» per a identificar l'interessat. De fet, sostenir que les persones físiques no són identificables, quan la finalitat del tractament és precisament identificar-les, seria una contradicció flagrant. Per tant, cal considerar que la informació es refereix a persones físiques identificables i el tractament ha d'estar subjecte a les normes de protecció de dades.

6. Totes les traduccions de normativa comunitària són nostres.

Aquest dictamen analitza la possibilitat d'identificar la persona des del punt de vista dels mitjans que raonablement es puguin utilitzar, fet que s'ha de connectar amb la tecnologia aplicable o disponible i que s'ha de configurar com una prova dinàmica, per la qual cosa s'ha de tenir en compte el grau d'avenç tecnològic en el moment del tractament i el seu possible desenvolupament en el període durant el qual es conservaran les dades. Pot ser que la identificació no sigui factible amb el conjunt dels mitjans que puguin ser utilitzats raonablement en el moment en què es fa el tractament i, en aquest sentit, si es preveu que les dades es conservin durant un mes, és raonable que en aquest període no sigui factible arribar a la identificació durant el «cicle de vida» de la dada i, conseqüentment, la dada no pugui ser considerada dada personal. Ara bé, si el període de conservació previst és molt més gran —per exemple, deu anys—, és possible que el transcurs del temps i l'evolució de la tecnologia facin possible aquesta identificació. Aquest aspecte ha de ser valorat pel responsable del tractament i, doncs, els sistemes de tractament han de ser capaços d'adaptar-se als progressos tecnològics a mesura que es produeixin i que s'introdueixin les mesures tècniques i organitzatives apropiades quan sigui l'hora, per a evitar aquesta identificació.

Pel que fa a la raonabilitat quant als mitjans utilitzables per a la identificació, Romeo Casabona indica que es tracta d'una qüestió casuística que s'ha de determinar en relació amb els mitjans que s'han d'utilitzar i el temps i l'activitat que impliqui, i s'ha de marcar el límit del que és raonable quan comença la desproporció. Desproporció que planteja igualment problemes perquè ha d'estar vinculada a un factor que serveixi de comparació i que també s'ha de relacionar amb la finalitat perseguida per a identificar la persona.[7]

Aquest criteri d'identificabilitat ha estat incorporat al considerant 26 de l'RGPD.[8]

En aquest sentit, com a primera reflexió, a ningú se li escapa que els avenços tecnològics i l'aplicació massiva de la IA fan avui en dia molt més factible que dades aparentment anònimes, degudament interrelacionades i contextualitzades, puguin acabar identificant una persona.[9]

7. Carlos María Romero Casabona, «Definiciones: persona identificada o identificable, el afectado o interesado y el procedimiento de disociación en la protección de datos de carácter personal», a *Comentarios a la Ley Orgánica de protección de datos de carácter personal*, Madrid, Civitas, 2010.

8. Els principis de la protecció de dades s'apliquen a tota la informació relativa a una persona física identificada o identificable. Les dades personals pseudonimitzades, q ue es podrien atribuir a una persona física utilitzant informació addicional, s'han de considerar informació sobre una persona física identificable. Per a determinar si una persona física és identificable, cal tenir en compte tots els mitjans que raonablement pot utilitzar el responsable del tractament o qualsevol altra persona per a identificar directament o indirectament la persona física, com, per exemple, la singularització. Per a determinar si hi ha una probabilitat raonable que s'utilitzin mitjans per a identificar una persona física, cal considerar-ne tots els factors objectius, com els costos i el temps necessaris per a la identificació, tenint en compte tant la tecnologia disponible en el moment del tractament com els avenços tecnològics. Per tant, els principis de protecció de dades no s'apliquen a la informació anònima, és a dir, a la informació que no té relació amb una persona física identificada o identificable, ni a les dades convertides en anònimes de manera que l'interessat no sigui identificable o deixi de ser-ho. En conseqüència, aquest reglament no afecta el tractament d'aquesta informació anònima, fins i tot amb finalitats estadístiques o de recerca.

9. És el cas, per exemple, de la recollida de l'iris de les persones a canvi de bitcoins, que va sortir recentment a la premsa, per part de l'empresa Worldcoin (Tools for Humanity), que pretenia justificar aquesta recollida en el fet que l'iris no configurava una dada personal com a tal, ja que es convertia en un codi alfa-

A més, cal tenir present si aquest tractament implica categories especials de dades, que es troben recollides en l'article 9 de l'RGPD, sota la regla general de prohibició del tractament, llevat que concorri algun dels supòsits habilitadors de l'apartat 2 d'aquest mateix article 9.

L'apartat 1 indica:

> Es prohibeix el tractament de dades personals que revelin l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques o l'afiliació sindical, i el tractament de dades genètiques, dades biomètriques destinades a identificar de manera unívoca una persona física, dades relatives a la salut o dades relatives a la vida sexual o l'orientació sexual d'una persona física.

En els casos en què es troben afectades categories especials de dades, els requeriments legals per al seu tractament, òbviament, són superiors.

3. LA DADA PERSONAL COM UN ACTIU AMB VALOR ECONÒMIC

A més, avui en dia les dades personals són una font d'informació molt valuosa no tan sols per a les administracions públiques,[10] sinó també per a les empreses, ja que permeten perfilar els consumidors i usuaris a l'efecte de poder oferir-los determinats productes i serveis en funció de les condicions socioeconòmiques, les preferències personals, la salut i, fins i tot, les opinions polítiques que es puguin derivar de l'anàlisi i el tractament de les dades personals.

Aquesta realitat és perceptible en àmbits com els mitjans de comunicació (accés a diaris digitals, per exemple), l'accés a determinades xarxes socials o el registre als webs d'empreses per a rebre ofertes comercials. En els dos primers casos, recentment s'ha implementat l'opció de pagar per a accedir als continguts o les xarxes i, en cas que no vulguis pagar, donar el teu consentiment per al tractament de les dades de caràcter personal (l'anomenat *consent or pay*).

Això ens permet fer una primera aproximació al consentiment com a base legitimadora del tractament de dades i, en aquests casos en concret, l'adequació o no a la normativa de protecció de dades de l'alternativa donada al consumidor per a accedir a determinats béns, serveis o aplicacions, de pagar per l'accés o consentir.

---

numèric que no permetia reidentificar la persona. Al marge d'altres consideracions sobre la certesa o no d'aquesta afirmació, com que l'iris és una dada de caràcter especial, com a dada biomètrica, de caràcter permanent, no es pot garantir que en el futur aquesta identificació no sigui tecnològicament possible. En aquests moments, sembla que l'empresa afectada ha decidit suspendre les seves activitats de tractament a tot Europa arran dels requeriments derivats de l'RGPD.

10. Un dels grans reptes que tenen actualment les administracions públiques és la prestació de serveis proactius, que es defineixen en l'article 31 del Decret 76/2020, del 4 d'agost:

> [...] s'entén per *servei proactiu i personalitzat* el servei digital que té per finalitat informar les persones, de manera predictiva i anticipada, sobre els serveis públics als quals poden accedir. Els serveis proactius i personalitzats es presten sobre la base de la informació obtinguda i elaborada pels subjectes relacionats a l'article 2 d'aquest decret, garantint la protecció de dades personals i el conjunt dels drets i les llibertats que els són propis, especialment pel que fa al principi de transparència i a la definició de les garanties adequada al disseny dels serveis.

Cal recordar que aquest consentiment, sovint donat de manera irreflexiva pel titular de les dades, sense analitzar les condicions generals del tractament que porta implícit, suposa la incorporació en el teu equip informàtic o dispositiu d'unes galetes o *cookies* analítiques que permeten extreure informació personal de les consultes i navegacions que fas a internet i que es troben vinculades a una determinada direcció IP (*internet protocol*) o a una direcció MAC com a identificador generalment fix i unívoc de tot dispositiu mòbil, usat en les comunicacions entre els diferents elements d'una xarxa. Aquests direccions són dades personals perquè permeten identificar el seu titular.[11]

El *consent or pay* s'ha imposat d'una manera massiva a partir de l'any 2023 arran de la Sentència del Tribunal Superior de Justícia de la Unió Europea del 4 de juliol de 2023, dictada en l'assumpte C-252/21 contra Meta Platforms Inc., anteriorment Facebook Inc.

Aquesta sentència va tractar diferents qüestions prejudicials plantejades i, en termes globals, va declarar il·legal el tractament de dades que feia aquesta empresa. No obstant això, en una de les qüestions es van plantejar les condicions d'accés al contingut que oferia aquesta plataforma i la Sentència es va pronunciar en els termes següents:

> (150) Así pues, en el marco del proceso contractual, esos usuarios deben disponer de la libertad de negarse individualmente a prestar su consentimiento a operaciones particulares de tratamiento de datos que no sean necesarias para la ejecución del contrato, sin verse por ello obligados a renunciar íntegramente a la utilización del servicio ofrecido por el operador de la red social en línea, lo que implica que se ofrezca a dichos usuarios, en su caso a cambio de una remuneración adecuada, una alternativa equivalente no acompañada de tales operaciones de tratamiento de datos.

Fixem-nos que el plantejament de l'opció es feia des de la protecció dels usuaris, però la davallada d'ingressos que va patir Meta la va portar a introduir la regla del *consent or pay*. Regla que, com ja hem dit, ha estat massivament implantada per altres plataformes i prestadors de serveis digitals.

Aquesta actuació abusiva ha justificat que el Comitè Europeu de Protecció de Dades (integrat per les autoritats nacionals de protecció de dades de la Unió Europea i que ha substituït l'anomenat Grup de Treball de l'Article 29) aprovés el 17 d'abril de 2024 el Dictamen 08/2024, sobre el consentiment vàlid en el context dels models de consentiment o pagament implementats per les grans plataformes en línia.

Aquest dictamen indica que l'oferta de (només) una alternativa de pagament en el servei que inclogui el tractament de dades amb finalitats de publicitat basada en el comportament, no hauria de ser la via predeterminada per als controladors. A l'hora de desenvolupar l'alternativa a la versió del servei amb publicitat basada en el comportament, considera que

11. És el cas de les tecnologies de seguiment wifi, en relació amb les quals l'Autoritat Catalana de Protecció de Dades, l'Autoritat Basca de Protecció de Dades, el Consell de Transparència i Protecció de Dades d'Andalusia i l'Agència Espanyola de Protecció de Dades han elaborat orientacions específiques per als responsables del tractament a l'hora d'abordar els tractaments de dades amb tecnologia de seguiment wifi o *wifi tracking*. El document analitza les implicacions d'aquesta tecnologia, identifica els principals riscos i ofereix una sèrie de recomanacions per a un ús responsable i compatible amb la normativa de protecció de dades.

les grans plataformes en línia haurien de valorar oferir als interessats una «alternativa equivalent» que no impliqui el pagament d'una taxa. Si els responsables opten per cobrar una tarifa per a accedir a l'«alternativa equivalent», haurien de considerar oferir també una altra alternativa, gratuïta, sense publicitat basada en el comportament, per exemple amb una forma de publicitat que impliqui el tractament de menys dades personals (o cap). Aquest és un factor especialment important en l'avaluació de certs criteris per al consentiment vàlid segons l'RGPD. En la majoria dels casos, el fet que el responsable ofereixi una altra alternativa sense publicitat basada en el comportament, de manera gratuïta, tindrà un impacte substancial en l'avaluació de la validesa del consentiment, en particular pel que fa a l'aspecte perjudicial.

El Comitè Europeu de Protecció de Dades recorda els requisits de l'RGPD per a poder considerar que el consentiment és vàlid. En primer lloc, quant al fet que el consentiment ha de ser «donat lliurement», indica que per tal d'evitar perjudicis que excloguin el consentiment lliure, no pot ser que el preu o la taxa imposada inhibeixi efectivament l'interessat de fer una elecció lliure. A més, es pot produir un perjudici quan el fet de no pagar el pugui portar a l'exclusió del servei, especialment en els casos en què el servei té un paper destacat o és decisiu per a la participació de la persona en la vida social o l'accés a xarxes professionals.

Un altre element que es tracta és el relatiu a l'existència o no d'un desequilibri de poder entre l'interessat i el responsable. Entre els factors que s'han d'avaluar hi ha la posició de la gran plataforma en línia en el mercat, l'existència d'efectes de bloqueig o xarxa, la mesura en què l'interessat confia en el servei i l'audiència principal del servei.

Un criteri que igualment s'ha d'avaluar quant a considerar si el consentiment és «lliure» és si, davant la negativa a pagar o consentir, es dona una alternativa equivalent. En aquest punt, una «alternativa equivalent» es refereix a una versió alternativa del servei que ofereix el mateix responsable del tractament que no implica el consentiment per al tractament de dades personals amb finalitats de publicitat conductual.

A més, el Dictamen recorda que les dades personals no es poden considerar com una mercaderia negociable i que els responsables del tractament han de tenir en compte la necessitat d'evitar que el dret fonamental a la protecció de dades es transformi en una característica que els interessats han de pagar per a gaudir-ne. Per aquesta raó, considera que els responsables han d'avaluar, cas per cas, tant si una tarifa és adequada com quina quantitat és adequada en les circumstàncies donades, tenint en compte les possibles alternatives a la publicitat basada en comportaments que impliquen el tractament de menys dades personals, així com la posició dels interessats.

Una altra condició del consentiment és la granularitat, que implica que quan es presenta a l'interessat un model de «consentiment o pagament», hauria de ser lliure d'escollir quina finalitat del tractament accepta, en lloc d'enfrontar-se a una sol·licitud de consentiment que agrupa diverses finalitats.

El consentiment vàlid també ha de ser «específic», és a dir, donat per a una o més finalitats específiques, i ha d'equivaler a una indicació inequívoca de desitjos: en els models de «consentiment o pagament» és especialment important que els responsables del tractament dissenyin atentament com es demana als interessats que donin el seu consentiment, per tal que els usuaris no hagin d'estar subjectes a patrons de disseny enganyosos.

A més, perquè el consentiment sigui «informat», el procés d'informació construït pels responsables del tractament ha de permetre als interessats tenir una comprensió completa i clara del valor, l'abast i les conseqüències de les seves possibles eleccions, tenint en compte la complexitat de les activitats de tractament relacionades amb la publicitat basada en comportaments.

D'igual manera, el Dictamen també proporciona aclariments sobre la retirada del consentiment i aconsella als responsables que avaluïn acuradament la freqüència amb què s'ha de «renovar» el consentiment.

Aquest Dictamen 8/2024 permet apreciar com les autoritats de control en matèria de protecció de dades reaccionen davant de situacions que es poden considerar abusives, com ara posar en perill la llibertat d'elecció efectiva de la persona a l'hora de donar el consentiment, que, com a regla general, és la que serveix en l'àmbit privat per a fonamentar el tractament de dades.

En aquest sentit, una segona conclusió a la qual podríem arribar és que el consentiment, com a base jurídica habilitadora per al tractament de dades, no és un supòsit que permeti tractar les dades sense cap tipus de condicionant, sinó que ha de ser un consentiment vàlid en els termes de l'RGPD.[12]

4. L'EXCLUSIÓ DEL CONSENTIMENT COM A BASE LEGITIMADORA EN L'ÀMBIT DE LES ADMINISTRACIONS PÚBLIQUES

Ja hem indicat que el consentiment és la base habilitadora usual en l'àmbit de les relacions privades, però aquest no és el cas del funcionament de les administracions públiques.

Existeixen àmbits, com el de les relacions laborals o el de les relacions juridicoadministratives, en què la posició de desigualtat entre les parts exclou que el consentiment pugui ser considerat com a lliure, fet que determina que no sigui vàlid.

El considerant 43 de l'RGPD ho exposa d'una manera molt clara:

> Per a garantir que el consentiment s'ha donat lliurement, aquest no ha de constituir un fonament jurídic vàlid per al tractament de dades de caràcter personal en un cas concret en què hi ha un desequilibri clar entre l'interessat i el responsable del tractament, en particular si el responsable esmentat és una autoritat pública i, per tant, és improbable que el consentiment s'hagi donat lliurement en totes les circumstàncies d'aquesta situació particular. Es presumeix que el consentiment no s'ha donat lliurement quan no permet autoritzar per separat les diferents operacions de tractament de dades personals, tot i ser adequat en el cas concret, o quan el compliment d'un contracte, inclosa la prestació d'un servei, depèn del consentiment, fins i tot si no és necessari per a dit compliment.

12. Article 4.11 de l'RGPD. «"Consentiment de l'interessat": qualsevol manifestació de voluntat lliure, específica, informada i inequívoca per la qual l'interessat accepta, mitjançant una declaració o una acció afirmativa clara, el tractament de dades personals que l'afecten».

Igualment, el consentiment s'ha rebutjat com a base legitimadora de la utilització de les dades biomètriques per al control horari en l'àmbit laboral, atenent a la situació de desigualtat que es produeix entre l'empresari i el treballador.

5. EL DRET FONAMENTAL A LA PROTECCIÓ DE DADES NO ÉS UN DRET ABSOLUT. RELACIÓ AMB EL REGLAMENT D'INTEL·LIGÈNCIA ARTIFICIAL

Una tercera consideració seria que, si bé el dret a la protecció de dades és un dret fonamental, com indica el considerant 4 de l'RGPD, no és un dret absolut, sinó que s'ha de conciliar amb altres drets fonamentals i s'ha de mantenir-ne l'equilibri, d'acord amb el principi de proporcionalitat.[13]

I aquest és probablement el major repte davant el qual ens trobem actualment, ja que no és fàcil conciliar la protecció de dades amb l'increïble desenvolupament tecnològic present avui en dia, com a conseqüència de l'auge i l'ús cada vegada més freqüent dels sistemes d'IA. I, com més dades, més tractament d'aquestes, i més riscos per a la privacitat.

El passat 12 de juliol de 2024 es va publicar el Reglament 2024/1689, en matèria d'intel·ligència artificial (d'ara endavant, RIA), que es planteja com una norma que pretén establir un marc legislatiu que preservi els valors essencials de la Unió Europea (d'ara endavant, UE) sense restringir la competitivitat europea, conciliant la llibertat empresarial i el progrés tecnològic amb el respecte als drets fonamentals i la seguretat dels sistemes d'IA.

El RIA és una norma que, a diferència de l'RGPD, no pretén establir drets dels ciutadans ni està dirigit als usuaris finals dels sistemes d'IA. El RIA regula les condicions d'entrada dels sistemes d'IA al mercat econòmic de la UE. Per això, els proveïdors, els distribuïdors i els responsables del desplegament de tercers països han de complir unes obligacions per a poder introduir-se a la UE. Aquest enfocament integral i preventiu del RIA aspira a produir el conegut com a «efecte Brussel·les», ja aconseguit en matèria de protecció de dades, tot instaurant estàndards mundials. Per tant, tot i que és una normativa de l'àmbit de la UE, produeix, inevitablement, efectes extramurs d'aquest territori. Fins ara la majoria de països de fora de la UE o bé han apostat per seguir el model de les regulacions sectorials o autoregulacions del sector privat, o bé han adoptat una posició que podríem catalogar de *laissez-faire*.

En aquest sentit, el RIA té com a objectiu, d'acord amb el seu article 1.1:

> [...] millorar el funcionament del mercat interior i promoure l'adopció d'una intel·ligència artificial (IA) centrada en l'ésser humà i fiable, garantint al mateix temps un elevat nivell de protecció de la salut, la seguretat i els drets fonamentals consagrats en la Carta, inclosos la democràcia, l'estat de dret i la protecció del medi ambient, enfront dels efectes perjudicials dels sistemes d'IA (en endavant, «sistemes d'IA») a la Unió, així com donar suport a la innovació.

13. El tractament de dades personals ha d'estar concebut per a servir la humanitat. El dret a la protecció de les dades personals no és un dret absolut, sinó que s'ha de considerar en relació amb la seva funció en la societat i ha de mantenir l'equilibri amb altres drets fonamentals, d'acord amb el principi de proporcionalitat. Aquest reglament respecta tots els drets fonamentals i observa les llibertats i els principis reconeguts en la Carta tal com es consagren en els tractats.

En aquest punt, és important destacar que el RIA no desplaça l'RGPD, sinó que es produeix una situació d'intersecció. Tal com indica el considerant 10 del RIA:

> El dret fonamental a la protecció de les dades personals està garantit, en particular, pels reglaments (UE) 2016/679 i (UE) 2018/1725 del Parlament Europeu i del Consell i per la Directiva (UE) 2016/680 del Parlament Europeu i del Consell. A més, la Directiva 2002/58/CE del Parlament Europeu i del Consell protegeix la vida privada i la confidencialitat de les comunicacions, també establint condicions per a qualsevol emmagatzematge de dades personals i no personals en els equips terminals, i l'accés des d'aquests. Aquests actes legislatius de la Unió constitueixen la base per a un tractament de dades sostenible i responsable, també quan els conjunts de dades continguin una combinació de dades personals i no personals. El present reglament no pretén afectar l'aplicació del dret de la Unió vigent que regula el tractament de dades personals, incloses les funcions i competències de les autoritats de supervisió independents competents per a vigilar el compliment d'aquests instruments. Tampoc no afecta les obligacions dels proveïdors i els responsables del desplegament de sistemes d'IA en el seu paper de responsables o encarregats del tractament de dades derivades del dret de la Unió o nacional en matèria de protecció de dades personals en la mesura que el disseny, el desenvolupament o l'ús de sistemes d'IA impliquin el tractament de dades personals. També convé aclarir que els interessats continuen gaudint de tots els drets i les garanties que els confereix aquest dret de la Unió, inclosos els drets relacionats amb les decisions individuals totalment automatitzades, com l'elaboració de perfils. Unes normes harmonitzades per a la introducció en el mercat, la posada en servei i la utilització de sistemes d'IA establertes en virtut del present reglament han de facilitar l'aplicació efectiva i permetre l'exercici dels drets i altres vies de recurs dels interessats garantits pel dret de la Unió en matèria de protecció de dades personals, així com d'altres drets fonamentals.

Si bé la traducció és nostra, hem reproduït literalment aquest considerant perquè és important destacar que la normativa d'IA no desplaça en cap cas la normativa de protecció de dades i, com veurem, atribueix un paper rellevant als sistemes d'IA d'alt risc.

6. EL TRACTAMENT DE DADES AL CENTRE DEL CONTROL I LA PROTECCIÓ DE LA PRIVACITAT

Abans ens hem referit a les dades de caràcter personal, però també ens hem de referir al tractament de dades com l'eix vertebrador del sistema de protecció de la privacitat de les persones.

L'RGPD defineix el tractament de dades com:

> […] qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunts de dades personals, ja sigui per procediments automatitzats o no, com la recollida, el registre, l'organització, l'estructuració, la conservació, l'adaptació o la modificació, l'extracció, la consulta, la utilització, la comunicació per transmissió, difusió o qualsevol altra forma d'habilitació d'accés, acarament o interconnexió, limitació, supressió o destrucció.

Aquest tractament i la manera en què es duu a terme són essencials a l'hora d'analitzar si es compleix la normativa de protecció de dades.

A tall d'exemple, el tractament de la imatge i la veu de les persones físiques ha generat un debat molt intens. La veu, per exemple, és una dada molt valuosa perquè permet derivar l'estat d'ànim de la persona i altres dades com ara el nivell social. En qualsevol cas, la imatge i la veu de les persones físiques, en principi, d'acord amb l'RGPD no han de considerar-se categories especials de dades. En aquest sentit, l'article 4.14 de l'RGPD estableix què són dades biomètriques:

> […] dades personals obtingudes a partir d'un tractament tècnic específic, relatives a les característiques físiques, fisiològiques o conductuals d'una persona física, que permeten o confirmen la identificació única d'aquesta persona, com ara imatges facials o dades dactiloscòpiques.

Però el considerant 51 especifica:

> El tractament de fotografies no s'ha de considerar sistemàticament tractament de categories especials de dades personals, ja que únicament s'inclouen en la definició de dades biomètriques si, quan es tracten amb mitjans tècnics específics, permeten la identificació o l'autenticació unívoques d'una persona física.

Per tant, es considera que la imatge i la veu únicament són dades biomètriques quan s'apliquin mitjans tècnics que permetin la identificació o l'autenticació unívoca d'una persona física.

En aquest sentit, escau tenir en consideració els punts 10 i 12 de les Directrius 05/2022 sobre l'ús de la tecnologia de reconeixement facial en l'àmbit de l'aplicació de la llei, del Comitè Europeu de Protecció de Dades, aprovades el 26 d'abril de 2023, que posen de manifest la diferència entre la identificació (destinada a verificar que una persona és qui diu ser) i l'autenticació (destinada a trobar una persona entre un grup d'individus dins d'una àrea concreta, una imatge o una base de dades) per a concloure que:

> Tot i que ambdues funcions —autenticació i identificació— són diferents, totes dues es relacionen amb el tractament de dades biomètriques relacionades amb una persona física identificada o identificable i, per tant, constitueixen un tractament de dades personals i, més concretament, un tractament de categories especials de dades personals.

El tractament de les imatges de les persones ha generat una àmplia controvèrsia, sobretot si es tracta de dades biomètriques. En aquest punt, hi ha iniciatives que han permès contrastar la possibilitat d'identificar una persona partint de la seva imatge captada a la via pública, més el tractament d'altres dades públiques.

Es pot destacar la feina feta per l'Autoritat de Control de França, la Commission Nationale de l'Informatique et des Llibertés (CNIL), que el 2022 va publicar la seva posició respecte a la utilització de les denominades *càmeres intel·ligents* o *càmeres augmentades* en espais públics.

Les *càmeres intel·ligents* o *augmentades* són càmeres que duen acoblat un programari de tractament d'imatges automatitzat, que analitza les persones per tal de deduir-ne informació i dades personals (a més de filmar-les). Permeten, per exemple, comptar automàticament el nombre de persones que hi ha en un lloc, analitzar algunes de les seves característiques (vestimenta, ús de mascareta, etc.) i fins i tot identificar determinats comportaments (abandonament d'equipatge, violació, etc.),

En el seu comunicat, la CNIL demana fer una reflexió general sobre l'ús d'aquestes eines en espais públics, independentment de la base de legitimació esgrimida.

Pel que fa al seu ús per autoritats públiques per a la detecció i persecució de delictes, destaca que, avui, no hi ha cap normativa que autoritzi les autoritats franceses a recórrer a aquest tipus de dispositius.

No obstant això, indica que certs usos d'aquestes podrien arribar a ser legítims. És el pas, per exemple, del comptatge de vianants, cotxes o ciclistes a la via pública, l'adaptació de les capacitats del transport públic en funció del seu ús, la seva utilització per a analitzar el consum energètic d'un edifici, etc.

A més, destaca que amb aquests dispositius generalment no és possible que les persones exerceixin els drets que els atorga l'RGPD, com ara el dret a oposar-se a ser analitzades per la càmera. Per això, indica que aquests usos «només seran lícits quan hagin estat autoritzats per les autoritats públiques», les quals prèviament «han d'adoptar un text (reglamentari o legislatiu) per a deixar sense efecte el dret d'oposició».

D'altra banda, la CNIL confirma que quan aquestes eines siguin utilitzades únicament per a produir estadístiques (compostes per dades anònimes), el seu ús està permès sense autorització prèvia. Aquest seria el cas, per exemple, d'un dispositiu que permetés calcular les aglomeracions al metro i així mostrar als viatgers els trens que circulen amb menys passatgers.

Com a resum, hem de tenir present que, des del punt de vista de la normativa de protecció de dades, la imatge és un dels actius més rellevants, no tan sols perquè ens ubica com a individus dins d'una societat, sinó també perquè les condicions de captació de la imatge (p. ex., la localització) i l'anàlisi de la imatge en si mateixa traslladen informació sobre la nostra persona, i avui en dia aquesta imatge, amb l'associació d'altres dades personals, pot portar a una identificació perfecta de la nostra persona.

7. ELS RISCOS DERIVATS DE LA UTILITZACIÓ DE SISTEMES D'INTEL·LIGÈNCIA ARTIFICIAL

7.1. Diferenciació entre els sistemes d'intel·ligència artificial i l'actuació automatitzada

Prèviament hem avançat que, quan parlem d'IA, els riscos per a la nostra privacitat s'incrementen exponencialment. Però abans d'enumerar aquests riscos hem de diferenciar els sistemes d'IA del que és l'actuació automatitzada.

No sempre s'utilitza IA (en els termes de la definició del RIA) quan en la descripció d'un producte o servei s'incorpora el concepte d'IA. I això respon al fet que a vegades es fa

simplement com a estratègia de màrqueting. Tanmateix, amb el RIA en vigor, l'aplicació de les obligacions establertes en aquesta norma ens podria portar a confusió.

Per tant, hem de ser rigorosos en totes les anàlisis i un dels primers passos ha de ser determinar si realment estem davant d'un sistema d'IA o només davant d'una mera automatització d'un procés. González Cabanes i Díaz Díaz defineixen la IA com la disciplina que intenta replicar i desenvolupar la intel·ligència natural, d'humans i éssers vius, mitjançant ordinadors o màquines.[14] En aquest sentit, la IA no és humana però està dissenyada per humans, amb els riscos que es poden derivar de la programació o el disseny que es dugui a terme.

Un altre punt important que les entitats han de tenir en compte és com s'han d'integrar (com encaixen) els rols de l'RGPD (responsable i encarregat del tractament) amb els definits en el RIA (proveïdor i responsable del desplegament).

Només així es podran definir les obligacions que corresponen a cadascun i com s'han d'integrar en complir-les. Pensem, per exemple, en la protecció de dades des del disseny o el principi de responsabilitat proactiva.

De la mateixa manera, quan ens trobem en l'àmbit del dret administratiu, l'actuació automatitzada és l'actuació administrativa automatitzada a què fa referència l'article 41 de la Llei 40/2015, del 3 d'octubre, de règim jurídic del sector públic.[15]

En versions prèvies a l'aprovació del RIA s'incloïa en el seu àmbit d'aplicació l'automatització de processos, però en la versió aprovada definitivament s'ha deixat fora de la seva regulació, tal com indica el considerant 12.[16]

14. F. González Cabanes i N. Díaz Díaz, «¿Qué es la inteligencia artificial?», a F. L. Pérez Guerrero (coord.), *Inteligencia artificial y sector público: Retos, límites y medios*, València, Tirant Lo Blanch, 2023.

15. **Article 41**

1. S'entén per actuació administrativa automatitzada qualsevol acte o actuació realitzada íntegrament a través de mitjans electrònics per una administració pública en el marc d'un procediment administratiu i en la qual no hagi intervingut de manera directa un empleat públic.

2. En cas d'actuació administrativa automatitzada, s'haurà d'establir prèviament l'òrgan o els òrgans competents, segons els casos, per a la definició de les especificacions, la programació, el manteniment, la supervisió i el control de qualitat i, si escau, l'auditoria del sistema d'informació i del seu codi font. Així mateix, s'haurà d'indicar l'òrgan que ha de ser considerat responsable a l'efecte de la impugnació.

16.

S'ha de definir amb claredat el concepte de *sistema d'IA* en el present reglament i harmonitzar-lo estretament amb els treballs de les organitzacions internacionals que s'ocupen de la IA, a fi de garantir la seguretat jurídica i facilitar la convergència a escala internacional i una àmplia acceptació, alhora que es preveu la flexibilitat necessària per a donar cabuda als ràpids avenços tecnològics en aquest àmbit. A més, la definició s'ha de basar en les principals característiques dels sistemes d'IA que els distingeixen, des dels sistemes de programari o els plantejaments de programació tradicionals i més senzills, i no ha d'incloure els sistemes basats en les normes definides únicament per persones físiques per a executar automàticament operacions. Una característica principal dels sistemes d'IA és la seva capacitat d'inferència. Aquesta capacitat d'inferència es refereix al procés d'obtenció de resultats de sortida, com prediccions, continguts, recomanacions o decisions, que pot influir en entorns físics i virtuals, i a la capacitat dels sistemes d'IA per a deduir models o algoritmes, o ambdós, a partir d'informació d'entrada o dades. Les tècniques que permeten la inferència en construir un sistema d'IA inclouen estratègies d'aprenentatge automàtic que aprenen de les dades, com assolir determinats objectius i estratègies basades en la lògica i el coneixement que infereixen a partir de coneixements codificats o

En resum, quan parlem de sistemes d'IA, hem de ser estrictes i, sens perjudici del control que es pot exercir en relació amb qualsevol decisió basada en una màquina o sistema, hem de diferenciar-los.

7.2. Riscos dels sistemes d'intel·ligència artificial

Com he dit abans, quan parlem d'IA, els riscos en relació amb la protecció de dades augmenten. Els riscos que es poden destacar són els que s'exposen a continuació.

7.2.1. *Opacitat en la presa de decisions (caixes negres)*

Abans ens hem referit a la necessària justificació que ha d'acompanyar una decisió administrativa. Quan aquesta prové d'un sistema d'IA, cal avaluar si la programació o el funcionament de l'algoritme és correcte. Aspecte tecnològic, en termes de prova tecnològica, planteja una gran complexitat.

Autors com Ponce Solé han analitzat la problemàtica del control de les decisions i l'opacitat de la IA.

7.2.2. *Discriminació algorítmica i estupidesa artificial*

S'indica igualment que els processos de configuració de l'algoritme, en funció del disseny i les condicions de recollida de les dades, plantegen biaixos que posteriorment, amb la posada en funcionament del sistema, poden generar discriminacions o resultats arbitraris, fins i tot absurds.

En aquest sentit, es poden produir resultats esbiaixats i sortides d'IA distorsionades que perjudiquin el destinatari de la decisió, derivades d'errors en el tractament de la informació, al marge que també es poden produir problemes ètics o de discriminació.

Fins i tot, els sistemes d'IA poden arribar a fabricar fortuïtament informació, que pot suposar problemes seriosos si no es fa una supervisió humana acurada (és la coneguda al·lucinació de la màquina), ja que pot produir informació de poca qualitat i derivar en una manca de confiança en els sistemes.

d'una representació simbòlica de la tasca que s'ha de resoldre. La capacitat d'inferència d'un sistema d'IA transcendeix el tractament bàsic de dades, en permetre l'aprenentatge, el raonament o la modelització. El terme *basat en una màquina* es refereix al fet que els sistemes d'IA s'executen en màquines. La referència a objectius explícits o implícits subratlla que els sistemes d'IA poden funcionar d'acord amb objectius definits explícits o a objectius implícits.

7.2.3. *Predictibilitat preventiva*

Un dels grans reptes o límits el trobem en la predictibilitat preventiva, la possibilitat dels sistemes d'IA d'interpretar o deduir conductes futures, que podria afectar de manera significativa la llibertat de l'individu.

El RIA es preocupa d'aquest punt i en l'article 5.1 prohibeix una sèrie de pràctiques d'IA. En concret, quant a la predictibilitat preventiva, la lletra *d* prohibeix la introducció de la IA en el mercat, la seva posada en servei per a aquest fi específic o l'ús d'un sistema d'IA per fer avaluacions de riscos de persones físiques a fi de valorar o predir el risc que una persona física cometi un delicte.[17]

7.2.4. *Precaució algorítmica*

Un dels principis bàsics a l'hora de prendre decisions, sobretot en l'àmbit del dret administratiu, és el principi de precaució, que determina que, davant de la possibilitat que una actuació pugui produir un dany, en relació igualment amb el principi de proporcionalitat, no s'ha d'adoptar una determinada mesura.

Aquest principi, plenament integrable en els processos de decisió humana i en la discrecionalitat de la decisió, no és fàcilment traslladable a l'entorn de la IA, que, en principi, no pensa.

Autors com Ponce Solé s'han pronunciat respecte a aquesta qüestió en els termes següents [18] (la traducció és nostra):

> En tot cas, en espera de poder avançar, potser, en un dilema que ha ocupat brillants ments durant segles i aplicant aquí, més que les metàfores de la física newtoniana, les pròpies de la física quàntica de la nostra època, la *incertesa* que envolta encara la possibilitat de replicar una consciència humana i una empatia emocional equivalent en la IA ens porta a proposar l'aplicació jurídica del *principi de precaució* per a prevenir els greus riscos amb què ens enfrontem (màquines adoptant decisions automatitzades discrecionals que han d'implicar drets d'humans).

17. Altres sistemes d'IA que es prohibeixen en l'article 5 són els que tinguin per objecte alterar de manera substancial el comportament d'una persona o un col·lectiu; explotar vulnerabilitats de les persones o col·lectius derivades de la seva edat o discapacitat, situació social o econòmica específica; classificar les persones per raó del seu comportament social, característiques personals o personalitat, conegudes, inferides o predites; crear o ampliar les bases de dades de reconeixement facial mitjançant l'extracció no selectiva d'imatges facials d'internet o de circuits tancats de televisió; usar sistemes per a inferir les emocions d'una persona física en el lloc de treball o en centres educatius, o determinats sistemes d'identificació i categorització biomètrica.

18. Juli Ponce Solé, «Inteligencia artificial, derecho administrativo y reserva de humanidad: algoritmes y procedimiento administrativo debido tecnológico», *Revista General de Derecho Administrativo* (Iustel), núm. 50 (gener 2019).

7.2.5. *Reserva d'humanitat (ètica)*

En connexió amb això anterior, ha d'avaluar-se igualment la vessant ètica de la decisió, és a dir, fins a quin punt es poden introduir aquests aspectes en les decisions que s'han de prendre, com a mesura de protecció dels individus davant decisions adoptades per sistemes d'IA.

7.2.6. *Riscos de vulneració de la normativa de protecció de dades*

Els sistemes d'IA poden suposar riscos per a la privacitat, ja que processen i analitzen dades personals sense el consentiment i les salvaguardes suficients o, en general, sense l'existència de bases legitimadores que habiliten la recollida i el tractament. A més, els resultats de sortida dels sistemes d'IA generativa i els models d'IA poden arribar a identificar individus combinant múltiples fonts de dades.

7.2.7. *Riscos de seguretat*

Finalment, no es pot deixar de banda la seguretat, això és, la possibilitat que els sistemes d'IA siguin objecte d'atacs per a prendre el control dels sistemes informàtics, revelar informació sensible o provocar un mal funcionament. Pensem, per exemple, en la possibilitat que els ciberatacants manipulin conjunts de dades d'informació, explotant vulnerabilitats informàtiques, que determinin que els resultats de sortida dels sistemes d'IA no siguin veraços.

7.3. Posicionament de les autoritats i institucions públiques

Són moltes les autoritats i institucions públiques i privades que han manifestat la seva preocupació pels sistemes d'IA. En aquest punt, podem destacar tres posicionaments, que exposem a continuació.

7.3.1. *Informe de la relatora especial sobre el dret a la privacitat, del Comissionat de Drets Humans de les Nacions Unides, del 30 d'agost de 2023. Principis de transparència i explicabilitat en el processament de dades personals a través de la intel·ligència artificial*

En aquest informe, la relatora especial sobre el dret a la privacitat, Ana Brian Nougrères, accentua la importància dels principis de transparència i explicabilitat en el processament de dades personals a través d'IA.

L'omnipresència de la IA en totes les activitats i la presa de decisions sobre les persones a partir de l'ús d'aquesta, obliguen a analitzar aquest tema i a adoptar mesures perquè l'ús de la IA sigui ètic, responsable i respectuós amb els drets humans.

Això anterior és rellevant perquè la transparència i l'explicabilitat no només ajuden a generar confiança i fiabilitat en la IA, sinó que contribueixen a protegir els drets humans. Mitjançant aquests principis, d'una banda, s'informa a través les persones de manera oportuna, completa, senzilla i clara sobre aspectes bàsics respecte a l'ús de la seva informació personal en processos o projectes d'IA i les seves conseqüències; d'altra banda, s'exigeix que les persones afectades per la IA coneguin els motius concrets que van donar origen a aquesta afectació. Amb això, la persona podrà exercir els seus drets, com, per exemple, el dret al procés degut i el de defensa davant les decisions adoptades mitjançant eines o tecnologies d'IA.

7.3.2. *Resolució del Parlament Europeu del 14 de març de 2017, sobre les implicacions de les macrodades en els drets fonamentals: privacitat, protecció de dades, no-discriminació, seguretat i aplicació de la llei*

El Parlament Europeu també s'ha preocupat per la protecció dels drets fonamentals arran de les implicacions i els riscos que es deriven de la recollida, l'anàlisi i l'acumulació que es repeteix de grans quantitats de dades, incloent-hi dades personals, des d'una varietat de fonts, que són objecte de processament automàtic per algoritmes informàtics i impliquen tècniques de processament de dades que utilitzen dades tant les emmagatzemades com les fluides per a generar certes correlacions, tendències i patrons.

El Parlament Europeu és conscient que el progrés de tecnologies de la comunicació, l'ús de mecanismes electrònics amb sistemes de localització, els ginys (*gadgets*) de control, els mitjans de comunicació socials, les interaccions de webs i les xarxes, incloent-hi mecanismes que comuniquen informació sense interferència humana, han conduït al desenvolupament de sistemes de dades massius, sempre creixents, que, a través de tècniques de processament avançades i analítiques, proporcionen informació sense precedents del comportament humà i la vida privada de les persones.

Al mateix temps, s'és conscient que l'analítica de dades genera plusvàlues molt positives i oportunitats per als ciutadans en àrees com l'assistència sanitària, la batalla contra el canvi climàtic, la reducció del consum energètic, la millora de la seguretat en el transport, la possibilitat d'establir ciutats intel·ligents, per tal d'incrementar l'optimització i l'eficiència de les empreses i contribuir a millorar les condicions laborals i a detectar i lluitar contra el frau; i que les macrodades poden oferir un avantatge competitiu per als processos de presa de decisions de les empreses europees, alhora que el sector públic pot beneficiar-se d'una major eficàcia gràcies a un millor coneixement dels diferents nivells de desenvolupament socioeconòmic.

A partir d'aquesta aproximació, on s'ha de conciliar el potencial que el tractament massiu de les dades implica, s'és igualment conscient dels riscos que comporta i, dintre de les consideracions generals que fa, la primera indica:

> [...] els ciutadans, els sectors públic i privat, el món acadèmic i la comunitat científica només podran aprofitar plenament les perspectives i oportunitats que brinden les macrodades si la confiança pública en aquestes tecnologies es garanteix mitjançant l'estricta obser-

> vança dels drets fonamentals i el compliment de la legislació vigent de la Unió en matèria de protecció de dades, així com la seguretat jurídica en relació amb totes les parts interessades; posa en relleu que el tractament de les dades personals només pot fer-se de conformitat amb algun dels fonaments jurídics recollits a l'article 6 del Reglament (UE) 2016/679; considera fonamental que la transparència i la correcta informació al públic afectat són fonamentals per generar la confiança de l'opinió pública i la protecció dels drets individuals.

I afegeix en la consideració cinquena:

> [...] el Dret de la Unió sobre la protecció de la privacitat i les dades personals, el dret a la igualtat i a la no-discriminació, el dret de les persones a rebre informació sobre la lògica que subjau en relació amb la presa de decisions automatitzada i l'elaboració de perfils i el dret a interposar un recurs per via judicial, són aplicables al tractament de dades fins i tot quan aquest tractament estigui precedit de tècniques de pseudonimització o, en qualsevol cas, quan l'ús de dades no personals pugui repercutir en la vida privada de les persones o en altres drets i llibertats, la qual cosa conduiria a estigmatitzar grups complets de la població.

7.3.3. *L'estratègia europea d'intel·ligència artificial. Els set principis de la intel·ligència artificial*

En el marc de la política comunitària, s'han aprovat diferents documents que tenen per objecte impulsar la implementació dels sistemes d'IA i, al mateix temps, establir condicionants que permetin salvaguardar els drets de les persones.

Dins d'aquests documents es pot destacar l'elaborat per un grup independent d'experts d'alt nivell sobre IA, que es va crear per la Comissió Europea el juny del 2018 i que, després de diferents esborranys i sense que suposi un posicionament de la Comissió Europea, va aprovar les *Directrices éticas para una IA fiable*. En aquest document, sense que es configuri com una llista exhaustiva, es destaquen els següents:

a) Acció i supervisió humana: els sistemes d'IA han de permetre societats equitatives que donin suport a l'acció humana i els drets fonamentals, i no han de disminuir, limitar o desviar l'autonomia humana. Ha de ser supervisada per éssers humans, amb les mesures de contingència apropiades.

b) Solidesa i seguretat: la IA confiable requereix que els algoritmes siguin prou segurs i sòlids per afrontar errors o inconsistències durant totes les fases del cicle de vida dels sistemes d'IA. Els sistemes han de ser resistents i resilients davant eventuals intents de manipulacions o de hackeig i han de dotar-se de plans de contingència.

c) Gestió de la privacitat i de les dades: els ciutadans han de tenir un control total sobre les seves pròpies dades. Les dades que els concerneixen no es poden utilitzar per a perjudicar-los ni discriminar-los. S'ha de garantir la privacitat de les dades dels ciutadans en tot el cicle vital de la IA.

d) Transparència: s'ha de garantir la traçabilitat dels sistemes d'IA. Ha de ser transparent, la qual cosa significa que s'ha de poder reconstruir com i per què es comporta d'una

determinada manera, i els qui interactuïn amb aquests sistemes han de saber que es tracta d'IA, així com quines persones en són les responsables.

e) Diversitat, no-discriminació i equitat: els sistemes d'IA han de considerar tota la gamma d'habilitats i requisits humans, i han de garantir adequadament l'accessibilitat. S'ha de tenir en compte la diversitat social des del seu desenvolupament per a garantir que els algoritmes en què es basi no tinguin biaixos discriminatoris directes o indirectes.

f) Benestar social i ambiental: els sistemes d'IA i el desenvolupament tecnològic en general s'han d'utilitzar per a millorar el canvi social positiu, la sostenibilitat mediambiental i la responsabilitat ecològica.

g) Rendició de comptes: s'han d'establir mecanismes per a garantir la responsabilitat i la rendició de comptes dels sistemes d'IA i els seus resultats davant d'auditors externs i interns.

7.4. El Reglament d'intel·ligència artificial: els sistemes d'alt risc

Pel que fa al RIA i la regulació dels sistemes d'IA, s'ha de prestar una atenció especial als sistemes d'alt risc, regulats en l'article 6.

Un sistema d'IA es considera d'alt risc quan està destinat a ser utilitzat com a component de seguretat d'un producte que entri en l'àmbit d'aplicació dels actes legislatius d'harmonització de la Unió o que el producte del qual el sistema d'IA sigui component de seguretat, o el propi sistema d'IA com a producte, hagi de sotmetre's a una avaluació de conformitat de tercers per a la seva introducció en el mercat o la seva posada en servei d'acord amb els actes legislatius d'harmonització de la UE.

A més, l'annex 3 enumera els sistemes que, en tot cas, han de ser considerats d'alt risc i que tenen relació directa amb el funcionament de les administracions públiques. Sense ànim de ser exhaustiu, és el cas dels sistemes relacionats amb la biometria, adreçats a la identificació, però també a la categorització i, fins i tot, al reconeixement d'emocions. Però també els que gestionen infraestructures crítiques, relatius a l'educació i la formació professional; la feina, la direcció de treballadors i l'accés al treball independent; l'accés a serveis privats essencials i públics, l'aplicació de lleis; la migració, asil i frontera, o l'administració de processos de justícia i democràtics.

En relació amb aquests sistemes d'alt risc, l'article 27 del RIA imposa que, prèviament al seu desplegament, s'ha de fer una avaluació d'impacte del dret fonamental.[19]

19.

Abans de desenvolupar un dels sistemes d'IA d'alt risc a què es refereix l'article 6, apartat 2, amb excepció dels sistemes d'IA d'alt risc destinats a ser utilitzats en l'àmbit enumerat a l'annex III, punt 2, els responsables del desenvolupament que siguin organismes de dret públic, o entitats privades que presten serveis públics, i els responsable del desenvolupament de sistemes d'IA d'alt risc a què es refereix l'annex III, punt 5, lletres *b* i *c*, duran a terme una avaluació de l'impacte que la utilització d'aquests sistemes pot tenir en els drets fonamentals. Amb aquesta finalitat, els responsables del desenvolupament duran a terme una avaluació que consistirà en: *a*) una descripció dels processos del responsable del desplegament en els quals s'utilitzarà el sistema d'IA d'alt risc en consonància amb la seva finalitat prevista; *b*) una descripció del període durant el qual es preveu utilitzar cada sistema

Però, a més, l'article 77 del RIA atribueix de manera expressa a les autoritats de control en matèria de drets fonamentals (entre les quals es troben les autoritats de control en matèria de protecció de dades), unes facultats específiques en relació amb el control dels sistemes d'IA d'alt risc.

En concret:

> *Article 77*
> **Poders de les autoritats encarregades de protegir els drets fonamentals**
> 1. Les autoritats o organismes públics nacionals encarregats de supervisar o fer respectar les obligacions considerades en el dret de la Unió en matèria de protecció dels drets fonamentals, inclòs el dret a la no-discriminació, pel que fa a l'ús de sistemes d'IA d'alt risc esmentats en l'annex III, tindran la facultat de sol·licitar qualsevol documentació creada o conservada d'acord amb el present reglament i d'accedir-hi, en un llenguatge i format accessibles, quan l'accés a aquesta documentació sigui necessari per al compliment efectiu dels seus mandats, dins dels límits de la seva jurisdicció. L'autoritat o organisme públic pertinent informarà sobre qualsevol sol·licitud d'aquest tipus a l'autoritat de vigilància del mercat de l'estat membre que correspongui.

Un dels reptes serà com s'articulen les competències de les autoritats de control en matèria de protecció de dades, derivades del RIA, amb les competències que els atribueix l'RGPD, quant a la salvaguarda dels drets fonamentals dels ciutadans i el dret que l'article 22 de l'RGPD reconeix a no ser objecte d'una decisió automatitzada, sense un consentiment explícit.[20]

En aquest punt, recentment el Comitè Europeu de Protecció de Dades ha aprovat la Declaració 3/2024, del 16 de juliol, sobre el paper de les autoritats de control en matèria de protecció de dades, en el marc del RIA, en el qual s'analitza el paper rellevant que aquestes autoritats han de desenvolupar per a defensar la privacitat davant l'expansió dels sistemes d'IA.

d'IA d'alt risc i la freqüència amb què està previst utilitzar-lo; *c*) les categories de persones físiques i col·lectius que puguin veure's afectats per la seva utilització en el context específic; *d*) els riscos de perjudici específics que puguin afectar les categories de persones físiques i col·lectius determinades d'acord amb la lletra *c* del present apartat, tenint en compte la informació facilitada pel proveïdor d'acord amb l'article 13; *e*) una descripció de l'aplicació de mesures de supervisió humana, d'acord amb les instruccions d'ús; *f*) les mesures que s'han d'adoptar en el cas que aquests riscos es materialitzin, inclosos els acords de governança interna i els mecanismes de reclamació.

20. Article 22.1 de l'RGPD: «Qualsevol interessat té dret a no ser objecte d'una decisió basada únicament en el tractament automatitzat, inclosa l'elaboració de perfils, que produeixi efectes jurídics que l'afectin o que l'afectin significativament de manera similar».

8. UN CAS CONCRET: EL PAPER DE LA PROTECCIÓ DE DADES EN EL CONTEXT DE LES CIUTATS INTEL·LIGENTS (*SMART CITIES*)

8.1. Concepte de *ciutat intel·ligent* i presa de decisions

Les ciutats intel·ligents són una realitat cada vegada més present avui en dia i es presenten com un model de gestió eficient de les ciutats i dels serveis que aquestes ofereixen.

La base sobre la qual es fonamenten les ciutats intel·ligents és mirar cap al ciutadà des del punt de vista de millorar les seves condicions de vida i satisfer les seves necessitats. Però, evidentment, en funció de com es faci aquesta aproximació, la seva privacitat es pot veure compromesa.

Una ciutat intel·ligent es basa en els usos de tecnologies de la informació i la comunicació (TIC) per a augmentar l'eficiència operacional, millorar la qualitat dels serveis governamentals i, conseqüentment, la qualitat de vida dels seus habitants, optimitzant la gestió dels recursos.

Però la definició de *smart city* va més enllà de l'ús de les tecnologies digitals: també cerca l'eficiència des del punt de vista energètic, l'ús de fonts d'energia renovables integrades, l'aposta per nous mitjans de mobilitat urbana més intel·ligents i sostenibles, així com la millora del subministrament d'aigua i de les instal·lacions d'eliminació de residus per a fer front als reptes econòmics, socials i mediambientals de la ciutat, i fins i tot per a detectar delictes.

Al mateix temps, com indica Font i Llovet, «*smart* s'associa amb la capacitat que tingui una ciutat de crear *més benestar per a la seva ciutadania*, no només a través de la millora dels serveis públics, sinó també, entre altres elements, a través de la implicació de la ciutadania en la presa de decisions».[21]

La gestió es basa en la presa de decisions, i aquestes decisions es fonamenten en dades recollides mitjançant sensors fiables. Com més dades es recullen i es tracten, més fiables són les decisions que s'adopten.

Les decisions que s'adopten han de ser explicables i, quan parlem de decisions basades en sistemes d'IA, es plantegen problemes des del punt de vista de l'ètica i la justícia. Com indica Alemany Garcías:

> [...] muchos modelos de IA, como las redes neuronales profundas, son difíciles de interpretar y explicar. Esto plantea la cuestión de cómo tomar decisiones basadas en sistemas de funcionamiento interno que son oscuros. Los individuos tienen el derecho de entender por qué se toman ciertas decisiones automáticas que les afectan. La carencia de explicación en los sistemas de IA puede ser problemática desde una perspectiva ética y legal.[22]

Aquesta fiabilitat ha d'interpretar-se des del punt de vista dels sensors que recullen aquestes dades, però sobretot a través del tractament d'aquestes dades, cosa que ens portarà necessàriament a parlar del compliment de la normativa de protecció de dades. És evident que

21. Tomàs Font i Llovet, «La ciudad inteligente como actor global», *European Review of Digital Administration & Law*, vol. 2, núm.1 (2021); la traducció és nostra.

22. Juan Alemany Garcías, «Inteligencia artificial y administración. Nuevos retos del sector público», *Revista Española de Derecho Administrativo*, núm. 233 (2024), secció «Estudios».

el valor d'una ciutat intel·ligent no radica en la informació de què disposen, sinó del que fan amb aquesta informació.

En aquest sentit, si la base sobre la qual es fonamenten les ciutats intel·ligents és mirar cap al ciutadà des del punt de vista de la millora de les seves condicions de vida, també és important tenir present que, segons com es faci aquesta aproximació al ciutadà, la seva privacitat es pot veure compromesa.

8.2. Les fonts de dades

Són diferents les fonts de les quals es poden extreure dades:

— Internet de les coses (IoT, de l'anglès *internet of things*): mecanismes ubicats a les ciutats que inclouen sensors que recullen en temps real informació sobre condicions mediambientals, usos d'energia, actuacions en infraestructures i més.

— Càmeres de vigilància ubicades estratègicament per a controlar espais públics, la intensitat del trànsit o la seguretat.

— Mòbils i aplicacions: cada vegada és més freqüent la utilització de telèfons intel·ligents i aplicacions mòbils com a fonts de dades, ja sigui mitjançant dades de localitzacions, ja sigui mitjançant patrons d'ús i comportaments d'usuaris, que poden proporcionar informació sobre la mobilitat a la ciutat, però també sobre les preferències dels seus habitants.

— Plataformes de mitjans de comunicació socials: es poden utilitzar igualment com a dipòsits dinàmics de continguts relatius a sentiments en temps real, opinions públiques o tendències dels usuaris d'un determinat territori.

— Plataformes de dades obertes de les administracions públiques: són una altra font d'informació que aporta dades relacionades amb els serveis públics, com el transport o la planificació urbanística, les quals esdevenen immediatament accessibles al públic.

Aquesta llista no és tancada, ja que els avenços tecnològics fan incrementar contínuament les fonts de dades i, en aquest sentit, per exemple, les dades recollides per dispositius que utilitzen les persones per a controlar els aspectes bàsics de la seva salut o la seva activitat poden ser igualment útils per a tractar iniciatives de salut pública o patrons d'estil de vida.

En una primera aproximació, hauríem de partir de la base que aquestes fonts no tracten dades de caràcter personal, però es tracta d'una afirmació que no necessàriament respon a la realitat (sobretot quan es tracta de dades recollides de fonts privades) i, d'altra banda, relacionant-ho amb el risc d'identificabilitat tractat abans, cada vegada és més difícil defensar el nostre anonimat en unes ciutats tan interconnectades.

En qualsevol cas, la quantitat d'informació que es tracta no és assumible per mitjans humans, cosa que obliga a la introducció de les eines tecnològiques. Així ho indica Mellado Ruiz:

> [...] l'explotació de la ingent quantitat d'informació generada contínuament per la ciutat intel·ligent només es pot dur a terme realment mitjançant algoritmes o mitjançant la utilització de la intel·ligència artificial. I aquí resideix realment el gran repte de modernització tecnolò-

gica de les administracions públiques, des de la necessitat d'un autèntic canvi de paradigma en relació amb el personal, les funcions i les estructures necessàries per a la seva assumpció.[23]

8.3. La titularitat del dret a la protecció de dades

Com ja hem dit, una de les grans preocupacions pel que fa al tractament de dades en l'entorn de les ciutats intel·ligents està relacionada amb la propietat de les dades i la privacitat dels ciutadans.

En aquest sentit, cal destacar el posicionament del Tribunal Constitucional quant al dret del titular de les dades a gaudir d'un efectiu poder de disposició i control de les dades.

La Sentència del Tribunal Constitucional (STC) 292/2000 va aprofundir en el dret a la protecció de dades personals en els termes següents:

> […] el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esas posesiones y usos.
>
> […] resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios.

En definitiva, el dret a la protecció de dades i les seves garanties s'estenen als usos als quals se sotmeten les dades. És evident que un tractament de dades que tingui per objecte controlar predictiblement la gestió del trànsit o la infraestructura d'energia i gestió de residus sota els paràmetres d'eficiència i optimització, suposa convertir les ciutats en centres de connectivitat i innovació.

Però, com més connectivitat, més s'incrementen els riscos per a la privacitat, fet que porta els ciutadans i els poders públics a una intersecció entre la protecció de les dades personals i la transformació digital basada en la innovació.

23. Lorenzo Mellado Ruiz, «*Smart cities*: aproximación a sus posibilidades de desarrollo», *La Administración práctica* (Aranzadi), núm. 7 (2024), secció «Análisis Doctrinal».

8.4. El responsable del tractament i la responsabilitat proactiva

Un concepte que ha de tenir-se igualment present en matèria de protecció de dades és el de *responsable del tractament*.

El responsable del tractament o responsable és «la persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que, sol o juntament amb d'altres, determina les finalitats i els mitjans del tractament» (art. 4.7 de l'RGPD).

Responsable del tractament que, en l'àmbit de les ciutats intel·ligents, és ordinàriament el gestor del sistema o servei que pren les decisions en l'àmbit de la prestació corresponent.

En l'àmbit de la protecció de dades, el responsable del tractament és una peça fonamental al voltant de la qual s'articula el compliment de les obligacions que imposa la normativa de protecció de dades (*accountability*). És l'anomenada *responsabilitat proactiva* a què fa referència l'article 5.2 de l'RGPD quan indica que el responsable del tractament és responsable del compliment del que disposa l'apartat 1 («els principis del tractament») i ha de tenir la capacitat per a demostrar-ho.

8.5. La privacitat des del disseny i per defecte

La valoració per part del responsable del tractament és una avaluació jurídica, però també tecnològica, fet que implica l'aplicació del principi de la privacitat des del disseny i per defecte, regulada en l'article 25 de l'RGPD. El terme *privacitat des del disseny* no significa res més que «la protecció de dades a través del disseny de tecnologia». Darrere d'aquesta afirmació es troba la convicció que la protecció de dades en procediments de tractament de dades es troba més garantida quan s'integra des del primer moment, des de la fase inicial de creació d'aquesta tecnologia.

A més, la privacitat per defecte suposa que el responsable del tractament ha d'aplicar les mesures tècniques i organitzatives adequades amb la intenció de garantir que, per defecte, únicament es tracten les dades personals necessàries per a cadascuna de les finalitats específiques del tractament. Aquesta obligació s'aplica a la quantitat de dades personals recollides, a l'abast del tractament, al termini de conservació i a l'accessibilitat de les dades.

Així s'exposa en el considerant 78 de l'RGPD:

> La protecció dels drets i les llibertats de les persones físiques pel que fa al tractament de dades personals exigeix que s'adoptin les mesures tècniques i organitzatives adequades amb la finalitat de garantir que es compleixen els requisits d'aquest reglament. Per tal de poder demostrar la conformitat amb aquest reglament, el responsable del tractament ha d'adoptar polítiques internes i aplicar mesures que compleixin en particular els principis de protecció de dades des del disseny i per defecte. Aquestes mesures poden consistir, entre d'altres, a reduir al màxim el tractament de dades personals, pseudonimitzar al més aviat possible les dades personals, donar transparència a les funcions i el tractament de dades personals, permetre als interessats supervisar el tractament de dades i al responsable del tractament, crear i millorar elements de seguretat. Cal encoratjar els productors de les aplicacions, dels productes i dels serveis basats en el

> tractament de dades personals perquè tinguin en compte el dret a la protecció de dades quan els desenvolupen, dissenyen, seleccionen i usen i que s'assegurin amb la deguda atenció a l'estat de la tècnica, que els responsables i els encarregats del tractament estan en condicions de complir les seves obligacions en matèria de protecció de dades. Els principis de la protecció de dades des del disseny i per defecte també s'han de tenir en compte en el context dels contractes públics.

En qualsevol cas, la normativa que regula la protecció de dades des del disseny i per defecte no determina quines mesures tècniques i organitzatives concretes cal implementar. La determinació de les mesures necessàries ha de ser el resultat d'una anàlisi prèvia feta pel responsable del tractament i, per extensió, pels desenvolupadors de les solucions tecnològiques que ha d'emprar el responsable del tractament.

En l'àmbit de les ciutats intel·ligents, s'ha arribat a reivindicar l'aplicació de la «inclusió per disseny i per defecte»,[24] que, en paraules del seu autor,

> [...] quan una innovació de qualsevol tipus pugui afectar directament o indirectament la qualitat de vida de persones amb discapacitat, s'exigirà en tot cas que, des del mateix moment en què es comenci a dissenyar, es garanteixi que no generarà cap tipus d'exclusió per a aquelles, i que si hi ha diverses solucions possibles, s'optarà sempre per la més inclusiva.

8.6. Les bases legitimadores del tractament: compliment d'una obligació legal o d'una missió d'interès públic com a legitimadora de l'actuació de les administracions públiques

Un dels errors que acostumen a cometre els responsables del tractament és considerar que no es tracta de dades de caràcter personal i, per contra, com hem vist, el concepte ampli de *dades personals* produeix que aquesta afirmació, moltes vegades, no sigui veritat.

Ni que sigui en el moment de la recollida de les dades, aquestes dades són personals, sens perjudici que es puguin sotmetre, per al seu tractament, a un procediment d'anonimització o pseudoanonimització.

En aquest sentit, no hem de perdre de vista el compliment de dos aspectes relatius al tractament de dades: l'existència d'una base legitimadora i el respecte dels principis en matèria de protecció de dades.

Pel que fa a les bases legitimadores, ja ens hem referit al consentiment com a base del tractament, però hem vist que en el cas de les relacions entre els ciutadans i l'Administració no pot ser considerat com a vàlid.

Per aquesta raó, hem d'analitzar quines són les bases jurídiques que han de permetre el tractament de dades personals i, prèviament a l'anàlisi, no podem oblidar que, quan parlem de ciutats intel·ligents, estem parlant de municipi, de poders públics o d'actuació dels governants.

Des del punt de vista de la protecció de dades, això significa que els estrategues polítics, quan gestionen les ciutats intel·ligents, han de gestionar la complexitat en el govern de

24. José Luis Piñar Mañas, «Derecho, ética e innovación tecnológica» (la traducció és nostra).

les dades respectant la privacitat dels ciutadans, complint amb la transparència i, en general, aplicant i complint les previsions legals.

Abans de parlar de les previsions legals en matèria de protecció de dades, cal recordar que, en l'àmbit del dret administratiu, el control de les decisions adoptades es fa al voltant de la motivació o justificació de les decisions, i quan parlem de decisions adoptades prenent com a base el tractament de dades, hem de ser capaços de justificar que aquest, que ha conduït a una determinada decisió, ha estat idoni o adequat. I això s'ha de fer des del dret administratiu en sentit estricte, és a dir, ens hem de trobar en condicions d'explicar una determinada decisió que s'ha d'enfocar des del punt de vista de la motivació de l'acte administratiu, i no del dret fonamental a la protecció de dades, sens perjudici que aquest sigui un paràmetre que, en el marc general de la decisió, també hagi de ser valorat.

Tal com hem dit, l'aproximació a la qüestió des del punt de vista de la protecció de dades és prèvia, ja que suposa parlar de bases legals per al tractament de dades i, posteriorment, dels principis i regles sobre la protecció de les persones físiques quant al processament de les seves dades personals.

L'article 6.1 de l'RGPD estableix que el tractament és lícit si és necessari per al compliment d'una obligació legal aplicable al responsable del tractament (6.1*c*) o bé és necessari per al compliment d'una missió duta a terme en interès públic (6.1*e*). L'article 6.3 estableix que la base del tractament indicat en les lletres *c* i *e* de l'apartat 1 ha de ser establerta pel dret de la Unió o pel dret dels estats membres que s'apliqui al responsable del tractament.

Els subapartats *c* i *e* de l'article 6.1 de l'RGPD són les bases legitimadores que habitualment permeten a les administracions públiques el tractament de dades personals.

Respecte a aquesta qüestió, el segon paràgraf de l'article 6.3 de l'RGPD estableix:

> La finalitat del tractament s'ha de determinar en aquesta base jurídica o bé, pel que fa al tractament a què es refereix l'apartat 1, lletra *e*, ha de ser necessària per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable del tractament. Aquesta base jurídica pot contenir disposicions específiques per a adaptar l'aplicació de les normes d'aquest reglament, entre les quals: les condicions generals que regeixen la licitud del tractament efectuat pel responsable; els tipus de dades objecte de tractament; els interessats afectats; les entitats a les quals es poden comunicar dades personals i les finalitats d'aquesta comunicació; la limitació de la finalitat; els terminis de conservació de les dades, així com les operacions i els procediments del tractament, incloses les mesures per a garantir un tractament lícit i equitatiu, com les relatives a altres situacions específiques de tractament d'acord amb el capítol IX. El dret de la Unió o dels estats membres ha de complir un objectiu d'interès públic i ha de ser proporcional a la finalitat legítima perseguida.

Sobre això, el considerant 45 de l'RGPD assenyala:

> Si s'efectua en compliment d'una obligació legal aplicable al responsable del tractament, o si és necessari per a complir una missió realitzada en interès públic o en l'exercici de poders públics, el tractament ha de tenir una base en el dret de la Unió o dels estats membres. Aquest reglament no requereix que cada tractament individual es regeixi per una norma específica. Una mateixa norma pot ser suficient com a base per a diverses operacions de tractament de dades basades en una obligació legal aplicable al responsable del tractament, o si

> el tractament és necessari per complir una missió realitzada en interès públic o en l'exercici de poders públics. La finalitat del tractament també s'ha de determinar en virtut del dret de la Unió o dels estats membres. A més, aquesta norma pot especificar les condicions generals d'aquest reglament que regeixen la licitud del tractament de dades personals, establir especificacions per a determinar el responsable del tractament, el tipus de dades personals objecte de tractament, els interessats afectats, les entitats a les quals es poden comunicar les dades personals, les limitacions de la finalitat, el termini de conservació de les dades i altres mesures per a garantir un tractament lícit i lleial. També s'ha de determinar, en virtut del dret de la Unió o dels estats membres, si el responsable del tractament que du a terme una missió en interès públic o en l'exercici de poders públics ha de ser una autoritat pública o una altra persona física o jurídica de dret públic, o, quan s'ha de fer en interès públic, incloses les finalitats sanitàries com la salut pública i la protecció social i també la gestió dels serveis de sanitat de dret privat, com ara una associació professional.

A més, com ha posat de manifest reiterada jurisprudència (per totes, vegeu la STC 39/2016, del 3 de març), per tal de comprovar si una mesura restrictiva d'un dret fonamental respecta el principi de proporcionalitat, cal que compleixi tres requisits: que sigui susceptible d'aconseguir l'objectiu proposat (judici d'idoneïtat); que sigui necessària, en el sentit que no n'existeixi una altra de més moderada per a la consecució d'aquest propòsit amb la mateixa eficàcia (judici de necessitat), i, finalment, que sigui ponderada o equilibrada, és a dir, que se'n derivin més beneficis o avantatges per a l'interès general que perjudicis sobre altres béns o valors en conflicte (judici de proporcionalitat en sentit estricte), és a dir, si la ingerència produïda per dita mesura en el titular del dret objecte de restricció és la mínima per a assolir el fi legítim pretès amb la seva adopció.

En resum, això ens portarà a analitzar prèviament el marc normatiu de gestió de l'activitat corresponent, que atribueix al responsable del tractament la competència per a actuar, en el marc de les previsions legals, i que actuarà com a base legitimadora (la normativa de trànsit, la normativa de gestió de residus, la normativa de videovigilància...) per a aplicar posteriorment els principis i les regles en matèria de protecció de dades.

8.7. El tractament per a finalitats diferents: el test de compatibilitat

Un dels principis que ha de respectar-se en el tractament de dades és el de finalitat. D'acord amb aquest principi, les dades han d'utilitzar-se per a la finalitat per a la qual van ser recollides inicialment, i no per a finalitats diferents. En l'àmbit de les ciutats intel·ligents, ens podem trobar amb dades que es volen utilitzar per a finalitats diferents a les previstes inicialment en el moment de la recollida.

Això obliga a aplicar la previsió de l'article 6.4 de l'RGPD, coneguda pel test de compatibilitat, en els termes següents:

> 4. Quan el tractament per a una finalitat diferent d'aquella per a la qual es van recollir les dades personals no està basat en el consentiment de l'interessat, o en el dret de la Unió o dels estats membres, que constitueix una mesura necessària i proporcional en una societat

democràtica per a salvaguardar els objectius esmentats en l'article 23, apartat 1, el responsable del tractament, amb l'objecte de determinar si el tractament amb una altra finalitat és compatible amb la finalitat per a la qual es van recollir inicialment les dades personals, ha de tenir en compte, entre d'altres:

a) Qualsevol relació entre les finalitats per a les quals s'han recollit les dades personals i les finalitats del tractament posterior previst.

b) El context en què s'han recollit les dades personals, en particular respecte de la relació entre els interessats i el responsable del tractament.

c) La naturalesa de les dades personals, en especial quan es tracten categories especials de dades personals, de conformitat amb l'article 9, o dades personals relatives a condemnes i infraccions penals, de conformitat amb l'article 10.

d) Les possibles conseqüències per als interessats del tractament posterior previst.

e) L'existència de les garanties adequades, que poden incloure el xifrat o la pseudonimització.

Cal recordar que aquest test de compatibilitat no és aplicable quan la base legitimadora és el consentiment de l'interessat.

8.8. Un problema addicional: l'intercanvi intersectorial de dades (*cross-sectorial data sharing*)

En el cas de les ciutats intel·ligents, ens trobem amb una dificultat afegida, la freqüent utilització de l'intercanvi intersectorial de dades (compartició de dades entre els diferents gestors de serveis), el qual s'ha considerat vital per al desenvolupament amb èxit de les ciutats intel·ligents i necessari per a proporcionar solucions eficients als problemes que es puguin crear dins de les ciutats. Aquesta compartició de dades afavoreix la col·laboració de les autoritats afectades i la presa de decisions amb més informació.[25]

Però, evidentment, implica problemes addicionals, com poden ser la integració de les dades, la governança i la seguretat d'aquestes, la interoperabilitat; però també el rol dels subjectes que hi intervenen, en trobar-se afectades diferents prestacions o serveis, cadascuna de les quals està sota el control del corresponent responsable del tractament, sens perjudici que, en funció del cas, pugui existir la figura del corresponsable del tractament, definida en l'article 26 de l'RGPD.[26]

25. Aaron Joyce i Vahid Javidroozi, «Smart city development: Data sharing vs. data protection legislations», *Cities*, núm. 148 (2024).

26. Quan dos o més responsables determinen conjuntament els objectius i els mitjans del tractament, se'ls considera corresponsables del tractament. Els corresponsables han de determinar de manera transparent i de mutu acord les seves responsabilitats respectives, en el compliment de les obligacions imposades per aquest reglament, en particular pel que fa a l'exercici dels drets de l'interessat i a les seves obligacions de subministrament d'informació a què es refereixen els articles 13 i 14, atès que les responsabilitats dels corresponsables es regeixin pel dret de la Unió o dels estats membres. Aquest acord pot designar un punt de contacte per als interessats.

En resum, l'intercanvi intersectorial de dades, en termes de privacitat, pot ser un problema addicional a l'hora de comprovar el compliment de la normativa de protecció de dades i el respecte a la privacitat.

8.9. Les ciutats intel·ligents des de la vessant tecnològica: plataforma de ciutat intel·ligent

A l'hora de configurar una ciutat intel·ligent, es pot fer una aproximació també des del punt de vista dels requeriments tecnològics que són exigibles. En aquest àmbit, es pot destacar la norma d'estandardització UNE 178104:2017, aprovada l'any 2017 per l'Associació Espanyola de Normalització amb el títol «Sistemas integrales de gestión de la ciudad inteligente. Requisitos de interoperabilidad para una plataforma de ciudad inteligente».

Aquesta norma indica que aspira a:

— Identificar les capacitats que ha de tenir una plataforma de ciutat.
— Estructurar les funcionalitats/capacitats en un model congruent de capes.
— Identificar els components i mòduls necessaris per a dotar la ciutat amb les funcionalitats exigides i que els posen en el model de capes.
— Descriure els requisits que han de complir aquests components pel que fa a la interoperabilitat, disponibilitat, actuació i seguretat.

Aquestes normes tècniques d'estandardització es configuren com un *soft law*, ja que són aprovades, en definitiva, per una entitat privada de base associativa, aliena estrictament a l'exercici de les funcions públiques. Com indica Velasco Rico:[27]

> Com se sap, les normes UNE són de compliment voluntari, encara que les administracions i la legislació sectorial puguin exigir la seva observança en determinats supòsits (per exemple, en l'àmbit de la contractació pública, es pot requerir el seu compliment en el plec de prescripcions tècniques). En aquest cas, veiem que les administracions, que podrien regular la matèria exercint les seves potestats (normatives, de foment, de policia, etc.), prefereixen col·laborar amb el sector privat per a generar cànons no vinculants que provinguin d'un consens comú entre tots els actors rellevants per als projectes de ciutat intel·ligent. Aquestes pautes seran principalment aplicades pels municipis i les àrees metropolitanes, atès que les matèries i els instruments objecte de regulació són de la seva competència. Aquesta forma de producció de normes de caràcter tècnic comporta la plasmació de «nous paradigmes entre el públic i el privat». Això és una mostra més de la interrelació entre l'esfera pública i la iniciativa privada en el nou escenari de la ciutat intel·ligent.

En qualsevol cas, la mateixa norma UNE afegeix que no és objecte d'aquest document definir els protocols concrets de comunicació, els tipus de bases de dades, les solucions

27. Clara Velasco Rico, «La ciudad inteligente: entre la transparencia y el control», *Revista General de Derecho Administrativo* (Iustel), núm. 50 (gener 2019); la traducció és nostra.

tècniques concretes dels components de la plataforma, o la semàntica associada a l'intercanvi d'informació, si bé es donen algunes indicacions per a permetre la compatibilitat d'aplicacions i permetre l'operació i el desenvolupament dels serveis ciutadans per entitats diferents dels desenvolupadors de les plataformes.

En resum, la normativa de protecció de dades, tot i la rellevància que té, no és objecte d'anàlisi en la reglamentació tècnica referida (més enllà d'algunes indicacions), ni tracta el procediment de recollida de les dades des de la vessant de les solucions tecnològiques que s'han d'adoptar. Això suposaria, si no s'implementa aquesta anàlisi en la fase de recollida, una vulneració del principi de la privacitat des del disseny.

8.10. El document de treball sobre ciutats intel·ligents del Grup de Berlín

En l'anàlisi de la protecció de dades en l'àmbit de les ciutats intel·ligents, podem destacar el document de treball de l'anomenat Grup de Berlín.

El Grup Internacional de Treball sobre la Protecció de Dades en les Telecomunicacions (International Working Group on Data Protection in Technology, IWGDPT) es va constituir l'any 1983 en el marc de l'Assemblea Global de Privacitat (Global Privacy Assembly, GPA), organització de caire mundial que aglutina, entre d'altres, les autoritats de control en matèria de protecció de dades dels diferents hemisferis. L'IWGDPT està liderat per la secretaria de l'entitat, que, des de la seva constitució, ha estat assumida per l'autoritat de protecció de dades de Berlín.

Aquest grup s'ha centrat en la protecció de les dades i la intimitat relacionada amb les qüestions de la tecnologia de la informació en un sentit ampli, amb una atenció especial als desenvolupaments relacionats amb internet, i ha elaborat documents de treball rellevants en l'anàlisi d'aquestes matèries.

Pel que fa a les ciutats intel·ligents, el 29 i 30 de novembre de 2022 es va adoptar el document de treball sobre les ciutats intel·ligents que analitza els problemes que es poden presentar en matèria de protecció de dades i el respecte del principi d'intimitat en cadascuna de les etapes d'ús de les dades en aquest context (recollida, tractament i decisió), i que formula unes recomanacions que caldria seguir per a una implantació adequada, en termes de privacitat, de les ciutats intel·ligents, aplicant el principi de privacitat des del disseny i per defecte.

En aquest sentit, aquest document de treball destaca una sèrie de passos que els responsables del tractament haurien de tenir presents en cadascuna de les etapes.

8.10.1. *Responsabilitat i govern*

Un primer pas seria aconseguir i demostrar conformitat amb tots els principis de protecció de dades i protecció dels drets individuals abans de l'inici de qualsevol processament. En aquest sentit, les ciutats i els seus gestors han d'assegurar que es faci una avaluació de responsabilitat i de govern rigorosa, incloent-hi les avaluacions d'impacte de la protecció de dades quan siguin pertinents.

Una de les qüestions clau, tal com hem anat destacant en aquest article, és especificar si el processament es refereix a individus identificables. En aquest sentit, la identificabilitat ha de ser considerada en relació amb un processament de dades específic, però també com a conseqüència de processaments associats.

A tall d'exemple, això suposa valorar si quan s'instal·len sensors per a mesurar la concurrència en un lloc públic, aquests recullen dades que permeten identificar directament les persones o si aquesta tecnologia, combinada amb una altra que estigui operativa al mateix lloc públic (per exemple, càmeres de circuit tancat), podria permetre la identificació indirecta d'individus.

8.10.2. *Imparcialitat*

Les aplicacions de les ciutats intel·ligents sempre haurien d'estar inspirades per la imparcialitat. Les dades de baixa qualitat o les que no reflecteixen la varietat dels grups de població poden conduir a decisions injustes o discriminatòries.

Addicionalment, s'han d'establir mecanismes de transparència apropiats per a informar els individus del processament i adoptar mesures tècniques i d'organització per a assegurar que l'establiment de pràctiques de garantia de la intimitat des del primer moment de la recollida de les dades forma part de les obligacions del responsable.

8.10.3. *Minimització de dades*

L'aplicació del principi de minimització de dades permet assegurar que els responsables només recullen dades que són pertinents, adequades i necessàries per a un propòsit específic i legítim. En un context de ciutat intel·ligent el propòsit és, moltes vegades, entendre tendències, per exemple, l'assistència als llocs públics o la densitat de trànsit, fet que es pot verificar sense tractar dades personals, a distància (l'anomenat *bird's eye view*).

A tall d'exemple, la utilització d'imatges captades per les autoritats públiques des de drons, pràctica cada vegada més estesa, pot ser invasiva de la privacitat, segons com es faci.

8.10.4. *Limitació de la finalitat*

Les ciutats tenen múltiples papers en les vides dels seus ciutadans, i van des de la gestió del trànsit fins a la seguretat pública, el control d'emissions i la gestió de residus (per a esmentar les més rellevants). Els sistemes tècnics de tractament de dades haurien de reflectir de manera diferenciada les finalitats per a les quals les dades són recollides i haurien de separar igualment les activitats de tractament, per a garantir que les dades recollides no són utilitzades per a una finalitat diferent, sense que es faci una avaluació prèvia, documentada i fonamentada en una base legal (com podria ser el test de compatibilitat de l'article 6.4 de l'RGPD, del qual abans hem tractat).

8.10.5. *Integritat i confidencialitat*

L'expansió de les activitats de processament a les ciutats ha suposat un increment molt significatiu dels punts de recollida, del volum de dades tractades i de les necessitats d'emmagatzematge d'aquestes dades, i tot això representa desafiaments nous per a mantenir la integritat i la confidencialitat de les dades personals, amb els consegüents riscos en termes de seguretat.

Aquesta vessant és especialment rellevant atenent a l'increment substancial dels ciberatacs que s'ha produït, partint de la base del caràcter avaluable econòmicament de les dades no tan sols sota el paràmetre del rescat que poden exigir els ciberdelinqüents per a alliberar-les, sinó també pel valor intrínsec que poden tenir (pensem, per exemple, en la importància, en termes econòmics, dels resultats en la fase final d'una determinada investigació mèdica).

8.10.6. *Dret a ser informat*

La transparència del processament és un desafiament especialment rellevant per a les ciutats intel·ligents. La fase de recollida de dades sovint és passiva, ja que l'individu no és conscient que es produeix, ni n'és informat prèviament. Per aquesta raó i per la manca de transparència que es pot donar en el moment de la recollida, el titular de les dades pot perdre el control d'aquestes, fet que pot venir acompanyat de la pèrdua de confiança en la ciutat i en les institucions per a tractar les dades personals de manera transparent.

8.10.7. *Drets individuals*

Els drets dels titulars de les dades també comporten la garantia d'exercici dels drets que la normativa de protecció de dades els reconeix. En aquest sentit, és responsabilitat de les ciutats intel·ligents (els corresponents responsables del tractament) garantir els drets d'accés a les dades, d'oposició al tractament, de rectificació d'errors objectius i de supressió de dades. En el cas de les ciutats intel·ligents, l'existència de processaments múltiples i el *cross-sectorial data sharing* fan especialment rellevant l'establiment de procediments clars i accessibles per a exercir aquests drets.

9. CONCLUSIONS

Les tecnologies disruptives, enteses com les que suposen un canvi radical respecte al passat, s'han integrat en la realitat quotidiana de les persones. El big data i la IA es poden considerar la màxima expressió d'aquest canvi i, tot i les seves diferències, totes dues es fonamenten en el tractament de les dades, personals o no.

En qualsevol cas, la implantació d'aquestes tecnologies ha comportat un increment notable dels riscos per a la protecció de la privacitat de les persones i, d'altra banda, poden derivar en la pèrdua, per part del titular de les dades, del control de la seva privacitat.

No es pot oblidar que el concepte de *dada personal* com la que identifica o fa identificables les persones és un actiu amb valor econòmic que permet a les empreses singularitzar l'oferta dels seus béns i serveis en funció del perfil del consumidor o usuari. De la mateixa manera, la dada personal també és una font d'informació molt valuosa per a les administracions públiques a l'hora de gestionar els serveis públics i prendre decisions en el marc del dret administratiu.

La normativa de protecció de dades garanteix que el tractament de dades estigui emparat per una base legitimadora que, en el cas de les administracions públiques, és habitualment el compliment d'una missió d'interès públic, però també imposa el respecte dels principis en matèria de protecció de dades, com la minimització i la privacitat des del disseny i per defecte.

Al mateix temps, la normativa d'IA aprovada recentment introdueix un marc complementari de control de les decisions basades en aquesta tecnologia, que no exclou la protecció de la privacitat ni l'aplicació de la normativa de protecció de dades quan es tractin dades personals.

Els riscos derivats de la utilització dels sistemes d'IA són igualment un paràmetre que cal considerar a l'hora d'incorporar aquests sistemes als processos de decisió humana o d'avaluar els resultats de sortida d'aquests sistemes, com prediccions, continguts, recomanacions o decisions, que poden influir en entorns físics o virtuals.

Aquests riscos han justificat el posicionament de les autoritats públiques i d'institucions públiques i privades en relació amb l'ús d'aquestes tecnologies, la majoria de les quals han compartit la seva preocupació en relació amb la transparència i l'explicabilitat que ha de derivar-se del processament de dades personals que duguin a terme aquestes tecnologies.

Finalment, s'analitza el paper de la protecció de dades en el context de les ciutats intel·ligents, articulada com a model de gestió eficient de les ciutats i dels serveis que ofereixen. Les ciutats intel·ligents se centren en la millora de les condicions de vida de les persones i parteixen de la informació que tracten a l'hora de prendre decisions.

Les fonts de les quals les ciutats intel·ligents extreuen dades configuren una gran quantitat d'informació, a vegades intercanviada sectorialment, que és tractada mitjançat algoritmes i sistemes d'IA que obliguen a considerar els riscos que, amb caràcter general, es prediquen d'aquests tractaments.

Per aquesta raó, quan la informació són dades personals que identifiquen o permeten identificar la persona, s'han de complir les previsions de la normativa de protecció de dades, addicionalment a les derivades dels components tecnològics que s'estableixin per a garantir una gestió eficient dels processos de decisió.

10. REFERÈNCIES

Alemany Garcías, Juan. «Inteligencia artificial y administración. Nuevos retos del sector público». *Revista Española de Derecho Administrativo*, núm. 233 (2024), secció «Estudios».

Font i Llovet, Tomàs. «La ciudad inteligente como actor global». *European Review of Digital Administration & Law*, vol. 2, núm. 1 (2021).

González Cabanes, F.; Díaz Díaz, N. «¿Qué es la inteligencia artificial?». A: Pérez Guerrero, F. L. (coord.). *Inteligencia artificial y sector público*: *Retos, límites y medios*. València: Tirant Lo Blanch, 2023.

Joyce, Aaron; Javidroozi, Vahid. «Smart city development: Data sharing vs. data protection legislations». *Cities*, núm. 148 (2024). Disponible a: https://www.sciencedirect.com/science/article/pii/S0264275124000738?via%3Dihub

Mellado Ruiz, Lorenzo. «*Smart cities*: aproximación a sus posibilidades de desarrollo». *La Administración Práctica* [Aranzadi], núm. 7 (2024), secció «Análisis Doctrinal».

Piñar Mañas, José Luis. «Derecho, ética e innovación tecnológica». *Revista Española de Derecho Administrativo* [Civitas], núm. 195 (2018).

Ponce Solé, Juli. «Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmes y procedimiento administrativo debido tecnológico». *Revista General de Derecho Administrativo* [Iustel], núm. 50 (gener 2019).

Romeo Casabona, Carlos María. «Definiciones: persona identificada o identificable, el afectado o interesado y el procedimiento de disociación en la protección de datos de carácter personal». A: *Estudios y comentarios legislativos. Comentario a la Ley Orgánica de protección de datos de carácter personal*. Madrid: Civitas, 2010.

Valero Torrijo, Julián. «Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración». *Revista Catalana de Dret Públic*, núm. 58 (2019).

Velasco Rico, Clara. «La ciudad inteligente: entre la transparencia y el control». *Revista General de Derecho Administrativo* [Iustel], núm. 50 (gener 2019).