

Personal Data Protection in the Era of Artificial Intelligence: Legal Challenges and Solutions

[Protecția datelor personale în era inteligenței artificiale: provocări și soluții juridice]

Mariana-Alina ZISU¹

¹ Legal adviser PhD, member of the Methodological and Professional Guidance Commission of the Suceava College of Legal Advisers and member of the Methodological and Professional Guidance Commission of the "Romanian Order of Legal Advisers" Federation, Romania, stefanoaia.mariana@yahoo.com

Abstract

The rapid development of artificial intelligence (AI) has created a series of unprecedented challenges in the field of personal data protection. AI systems, in particular those based on machine learning and algorithmic analysis, involve massive data processing, often in an opaque manner and difficult for data subjects to control. The main legal risks include the lack of decision-making transparency ('black box'), the difficulty of obtaining informed consent, automated profiling, and the possibility of processing sensitive data without a clear legal basis.

The General Data Protection Regulation (GDPR) provides a solid legal framework at European level, based on principles such as lawfulness, transparency, purpose limitation and the accountability of controllers. However, its application in the context of AI faces practical difficulties, in particular as regards the interpretation of the provisions on automated decisions (Art. 22), impact assessment (Art. 35) and protection by design (Art. 25).

To address these challenges, the European Union has proposed a new regulatory framework through the Artificial Intelligence Act, which introduces a classification of AI systems according to the risk they pose and imposes transparency, security and human oversight obligations for high-risk systems.

Keywords: data protection; risk; mechanism; legal rule; law.

How to cite: Zisu, M.-A. (2025). Personal Data Protection in the Era of Artificial Intelligence: Legal Challenges and Solutions. *Anuarul Universității "Petre Andrei" din Iași, Fascicula: Drept, Științe Economice, Științe Politice*, 34, 251-259.
<https://doi.org/10.63331/upalaw/34/23>

Introducere

În ultimele decenii, dezvoltarea exponențială a tehnologiilor digitale, în special a inteligenței artificiale (IA), a transformat profund societatea contemporană, generând oportunități semnificative în domenii precum sănătatea, educația, securitatea, administrația publică și economia digitală. Totuși, această evoluție tehnologică are un impact considerabil asupra unui drept fundamental al omului: **dreptul la viață privată și protecția datelor cu caracter personal**, consacrat de instrumente juridice internaționale și europene, precum **Convenția nr. 108 a Consiliului European, Carta drepturilor fundamentale a Uniunii Europene** (art. 7 și 8) și **Regulamentul general privind protecția datelor (UE) 2016/679 (GDPR)**.

IA funcționează pe baza procesării unor volume masive de date, inclusiv date personale, pentru a învăța, a prezice comportamente și a lua decizii autonome. Această capacitate tehnologică ridică provocări semnificative pentru protecția juridică a persoanelor vizate, în special în ceea ce privește **transparența algoritmică, responsabilitatea decizională, profilarea, consimțământul informat și securitatea datelor**. Mai mult, sistemele IA pot perpetua sau amplifica discriminările și pot conduce la decizii automatizate care afectează direct drepturile și libertățile fundamentale ale indivizilor.

Deși cadrul legal oferit de GDPR este considerat unul dintre cele mai avansate la nivel global, acesta nu a fost conceput special pentru a răspunde complexității IA. Drept urmare, apar neconcordanțe între exigențele juridice (precum principiul transparenței sau dreptul la explicații) și natura tehnologică opacă a multor sisteme IA („black box”). În acest context, devine necesară o regândire a cadrului normativ, care să includă reglementări specifice pentru IA – inițiativă concretizată în propunerea de *Regulament european privind inteligența artificială* (Artificial Intelligence Act), aflat în proces legislativ.

Această lucrare își propune să analizeze, dintr-o perspectivă juridică și academică, principalele **provocări pe care le ridică utilizarea inteligenței artificiale asupra protecției datelor cu caracter personal**, precum și **soluțiile normative actuale și potențiale**, menite să asigure un echilibru între inovație și respectarea drepturilor fundamentale în era digitală.

Provocările juridice aduse de inteligența artificială în domeniul protecției datelor personale

Inteligența artificială (IA), în special sub forma algoritmilor de învățare automată și a sistemelor autonome de decizie, ridică multiple provocări din perspectiva dreptului la protecția datelor personale. Aceste provocări decurg din modul în care IA colectează, procesează, interpretează și utilizează datele cu caracter personal, deseori fără intervenția directă a factorului uman. Analiza de mai jos evidențiază principalele riscuri și tensiuni juridice generate de aceste tehnologii.

1. Lipsa transparenței algoritmice („black box”)

Una dintre cele mai acute provocări este opacitatea decizională a sistemelor IA, care funcționează adesea ca „cutii negre” – în sensul că modul în care sunt generate rezultatele nu este ușor de înțeles nici măcar pentru dezvoltatori. Acest aspect contravine principiului transparenței, consacrat de art. 5 alin. (1) lit. a din Regulamentul (UE) 2016/679 (GDPR),

potrivit căruia datele trebuie să fie prelucrate într-un mod „legal, echitabil și transparent față de persoana vizată”¹.

Lipsa transparenței afectează dreptul la informare (art. 13 și 14 GDPR) și dreptul de acces (art. 15), deoarece persoanele vizate nu pot înțelege de ce și cum sunt luate deciziile care le afectează. De asemenea, ridică probleme în exercitarea dreptului la explicații, un concept derivat din art. 22 GDPR, deși nu este explicit reglementat în forma unui drept autonom².

2. Prelucrarea datelor personale sensibile prin inferență

Sistemele IA pot deduce date sensibile (de exemplu, etnie, religie, orientare sexuală) din date aparent banale, precum istoricul de navigare sau expresiile faciale. Conform art. 9 GDPR, aceste categorii speciale de date beneficiază de o protecție sporită și pot fi prelucrate doar în condiții restrictive.

Totuși, deducerea acestor informații prin profilare algoritmică riscă să eludeze cerințele legale privind consimțământul explicit sau temeiul legal necesar³. Astfel, IA creează riscul unei prelucrări indirecte a datelor sensibile, fără cunoștința și acordul persoanei vizate, încălcând principiile legalității și minimizării datelor (art. 5 alin. (1) lit. b și c GDPR).

3. Deciziile individuale automatizate și profilarea

Conform art. 22 GDPR, persoana vizată are dreptul de a nu fi supusă unei decizii bazate exclusiv pe prelucrarea automată, inclusiv profilare, care produce efecte juridice asupra sa sau o afectează semnificativ în mod similar. IA permite adoptarea unor decizii complet automatizate, precum acordarea/refuzarea unui credit, selecția CV-urilor sau stabilirea nivelului de risc în asigurări.

Aplicarea acestui articol este problematică în practică, deoarece este dificil de stabilit dacă decizia este „exclusiv” automatizată sau dacă există o intervenție umană reală. Mai mult, mulți operatori nu respectă obligația de a oferi informații clare despre logica implicată, importanța și consecințele prelucrării, ceea ce duce la un vid de responsabilitate juridică⁴.

4. Dificultatea obținerii unui consimțământ valabil

Condițiile pentru un consimțământ valabil sunt reglementate de art. 4 pct. 11 și art. 7 GDPR, care impun ca acesta să fie „liber exprimat, specific, informat și lipsit de ambiguitate”. În contextul IA, obținerea unui astfel de consimțământ este dificilă, deoarece utilizatorii nu înțeleg complexitatea proceselor algoritmice și posibilele implicații ale utilizării datelor lor.

Consimțământul tinde să devină formal, lipsit de conținut real, fapt ce contravine principiului echității și al responsabilității. Această situație este agravată de practicile de tip „take-it-or-leave-it” întâlnite frecvent în mediul digital⁵.

¹ Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016, art. 5 alin. (1) lit. a.

² S. Wachter, B. Mittelstadt & L. Floridi, “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation”, *International Data Privacy Law*, 7(2), 2017, pp. 76–99.

³ A. Mantelero, “AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment”, *Computer Law & Security Review*, 34(4), 2018, pp. 754–772.

⁴ A. D. Selbst & J. Powles, “Meaningful information and the right to explanation”, *International Data Privacy Law*, 7(4), 2017, pp. 233–242.

⁵ O. Lynskey, “Deconstructing data protection: the ‘added-value’ of a right to data protection in the EU legal order”, *International and Comparative Law Quarterly*, 63(3), 2019, pp. 569–597.

5. Risc de discriminare algoritmică

Algoritmii IA pot învăța din date istorice care conțin prejudecăți sistemice (bias), perpetuând sau chiar amplificând aceste inegalități. Într-un context juridic, aceasta se traduce prin discriminare indirectă, interzisă de dreptul european, inclusiv prin Carta drepturilor fundamentale a UE (art. 21) și legislația antidiscriminare.

Drept urmare, IA poate conduce la tratament diferențiat nejustificat, care afectează drepturi fundamentale precum egalitatea de tratament sau accesul la justiție. Este necesară o evaluare constantă a algoritmilor și o auditare etică și juridică a acestora pentru a preveni astfel de riscuri⁶.

În concluzie, provocările juridice generate de IA în materie de protecția datelor sunt multiple și complexe. Ele impun o adaptare a normelor existente, dar și o regândire a raportului dintre tehnologie, drepturile fundamentale și responsabilitatea decizională. Dincolo de simpla aplicare a GDPR, este necesară o reglementare specifică a IA, care să ofere garanții clare privind transparența, controlul uman, securitatea datelor și evitarea discriminărilor.

Soluții juridice existente și perspective de reglementare în protecția datelor personale în era inteligenței artificiale

Inteligența artificială reprezintă o provocare majoră pentru ordinea juridică existentă, în special în ceea ce privește protecția datelor cu caracter personal. Deși sistemele IA nu sunt fundamental incompatibile cu normele actuale, ele tensionează anumite principii și necesită o adaptare a cadrului normativ. În această secțiune sunt analizate **măsurile juridice deja în vigoare**, precum și **direcțiile de evoluție a reglementării**, în special la nivelul Uniunii Europene.

1. Cadrul juridic existent: aplicabilitatea și limitele GDPR

Regulamentul general privind protecția datelor (GDPR) rămâne instrumentul de bază pentru reglementarea prelucrării datelor personale în Uniunea Europeană. Acesta oferă o serie de garanții fundamentale relevante pentru IA, inclusiv:

- **Principiile prelucrării datelor** (legalitate, transparență, minimizare, exactitate, responsabilitate – art. 5 GDPR);
- **Drepturile persoanelor vizate** (acces, rectificare, opoziție, portabilitate, ștergere – art. 12–22);
- **Obligații pentru operatori și persoane împuternicite**, inclusiv în materie de evaluare a impactului asupra protecției datelor (DPIA – art. 35);
- **Limitarea deciziilor automatizate** cu efect juridic sau similar semnificativ (art. 22).
Totuși, aplicarea acestor norme în contextul IA ridică dificultăți practice:
- **Transparența algoritmică** este dificil de realizat în cazul modelelor complexe (deep learning), ceea ce limitează exercitarea efectivă a drepturilor.
- Conceptul de **consimțământ informat** își pierde semnificația reală într-un ecosistem bazat pe sisteme automate opace.
- Dreptul de a nu fi supus unei **decizii exclusiv automatizate** (art. 22) este greu de implementat, în lipsa unor criterii clare privind intervenția umană semnificativă.

⁶ S. Barocas & A. D. Selbst, “Big Data’s Disparate Impact”, *California Law Review*, 104(3), 2016, pp. 671–732.

În concluzie, deși GDPR oferă un cadru general aplicabil IA, **nu este suficient de specific** pentru a aborda toate riscurile generate de noile tehnologii⁷.

2. Reglementarea sectorială și soft law

În lipsa unor norme dedicate IA, diverse instituții au emis **ghiduri, recomandări și standarde etice** cu scopul de a orienta dezvoltarea responsabilă a IA:

- **Comitetul european pentru protecția datelor (EDPB)** a publicat opinii privind aplicarea art. 22 GDPR și privind evaluarea impactului algoritmic⁸;
- **Comisia Europeană** a emis, prin Grupul de experți în AI, „*Ethics Guidelines for Trustworthy AI*” (2019), care enunță principii precum supravegherea umană, transparența și responsabilitatea;
- Alte autorități naționale, cum ar fi CNIL (Franța) și ICO (UK), au emis ghiduri privind IA și prelucrarea datelor.

Deși aceste documente nu au forță juridică obligatorie, ele contribuie la dezvoltarea unui **cadru de bune practici**, complementând legislația hard law. Însă, în absența unor norme coercitive, eficiența lor este limitată.

3. Perspective de reglementare: Regulamentul privind inteligența artificială (AI Act)

Ca răspuns la provocările menționate, Uniunea Europeană a propus în 2021 un **Regulament privind inteligența artificială (Artificial Intelligence Act)**, care reprezintă primul cadru normativ supranațional dedicat în mod explicit IA⁹. Regulamentul este încă în proces legislativ, dar propune o abordare structurată a riscurilor:

- **Clasificarea sistemelor IA** în funcție de riscul pentru drepturile și siguranța persoanelor: risc inacceptabil (interzis), risc ridicat (reglementat strict), risc limitat (cerințe minime), risc scăzut/neglijabil (fără obligații speciale).
- Sistemele cu **risc ridicat** (de exemplu, recunoaștere facială, evaluare comportamentală, selecție automată pentru locuri de muncă) vor fi supuse unor obligații stricte:
 - transparență și explicabilitate;
 - documentație tehnică detaliată;
 - supraveghere umană semnificativă;
 - cerințe de acuratețe, robustețe și securitate cibernetică.

Acest regulament nu se substituie GDPR, ci îl **complementează** prin norme tehnice și procedurale, adaptate specificității IA. Este o inițiativă care semnalează **o tendință de „tehn constituționalism”**¹⁰, adică integrarea drepturilor fundamentale în designul tehnologic.

⁷ M. Tzanou, “Data protection as a fundamental right: The European Court of Justice and the European Data Protection Board”, *European Law Review*, 44(3), 2019, pp. 308-324.

⁸ EDPB, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2020.

⁹ European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), COM(2021) 206 final.

¹⁰ Giovanni De Gregorio, “The Rise of Techno-Constitutionalism: A Legal Approach to Digital Power”, *Columbia Journal of European Law*, 27(1), 2021, pp. 71–121.

4. Introducerea conceptului de IA „etică și responsabilă”

Un alt demers important constă în promovarea ideii de „IA centrată pe om”, care să respecte principiile statului de drept, ale democrației și ale drepturilor fundamentale. În acest sens:

- Se discută despre **obligații de audit algoritmic**, menite să detecteze discriminarea sau riscurile sistemice;
- Se propun **mecanisme de responsabilizare algoritmică** – inclusiv prin desemnarea unor „oficieri de IA” sau comitete etice interne în companiile mari;
- Se insistă pe **alfabetizarea digitală și juridică** a utilizatorilor, pentru a înțelege modul în care IA le influențează deciziile și viața personală.

În viitor, este posibil să asistăm la **convergența dintre protecția datelor, dreptul concurenței, drepturile consumatorilor și etica digitală**, într-un cadru legal mai integrat și orientat către protecția persoanei.

În fața avansului accelerat al inteligenței artificiale, soluțiile juridice existente – în special GDPR – constituie o bază solidă, dar insuficientă. Este necesară o **evoluție legislativă multistratificată**, care să cuprindă atât norme hard law (ex. AI Act), cât și mecanisme soft law (ghiduri, audituri etice), însoțite de o **reformă culturală** în ceea ce privește designul și utilizarea tehnologiilor. Numai printr-o abordare integrată, interdisciplinară și anticipativă pot fi garantate drepturile fundamentale ale persoanei în era algoritmilor.

Studii de caz relevante în domeniul protecției datelor personale în era inteligenței artificiale

Pentru a înțelege implicațiile reale ale IA asupra protecției datelor personale, este esențială analiza unor **studii de caz semnificative**. Acestea ilustrează modul în care tehnologia poate genera conflicte juridice și sociale, dar și cum autoritățile de reglementare sau instanțele au reacționat la astfel de situații. În cele ce urmează, sunt prezentate patru studii de caz relevante din spațiul european și internațional, din perspectiva dreptului la viață privată și protecția datelor.

1. Sistemul de recunoaștere facială al companiei Clearview AI

Context: Clearview AI este o companie americană care a creat o bază de date biometrică prin extragerea de imagini faciale din rețele sociale și surse publice online, fără consimțământul persoanelor vizate. Această tehnologie a fost oferită agențiilor de aplicare a legii din mai multe țări.

Probleme juridice:

Clearview AI a fost acuzată de **încălcarea principiilor GDPR**, în special:

- Lipsa unui temei legal valabil pentru prelucrarea datelor biometrice (art. 6 și 9 GDPR);
- Absența informării persoanelor vizate (art. 13 și 14);
- Lipsa consimțământului explicit și neexistența unui interes legitim care să justifice prelucrarea.

Așadar, autoritățile de protecție a datelor din mai multe țări europene, printre care **CNIL (Franța)** și **ICO (Marea Britanie)**, au constatat că activitățile companiei încalcă GDPR. În 2022, CNIL a obligat Clearview AI să șteargă datele cetățenilor francezi și să înceteze activitatea de colectare de imagini¹¹.

¹¹ CNIL, *Clearview AI: la CNIL met en demeure la société de cesser la réutilisation de photographies accessibles en ligne*, 2022, <https://www.cnil.fr>.

Acest caz demonstrează cum **IA aplicată în domeniul recunoașterii faciale** poate conduce la **supraveghere masivă și încălcarea gravă a vieții private**, necesitând intervenția fermă a autorităților de reglementare.

2. Cazul Uber și utilizarea IA în gestionarea forței de muncă

În 2021, mai mulți șoferi Uber din Regatul Unit și Olanda au dat în judecată compania pentru utilizarea IA în deciziile automatizate privind evaluarea performanței, suspendarea sau încetarea contractelor.

Probleme juridice:

- Posibila încălcare a **art. 22 GDPR**, privind interzicerea deciziilor automatizate fără intervenție umană semnificativă;
- Lipsa transparenței în procesul decizional algoritmic;
- Încălcarea dreptului de acces și de a obține explicații clare privind logica deciziilor automate.

Un tribunal din Amsterdam a constatat că Uber a **refuzat în mod abuziv accesul șoferilor la informațiile privind deciziile IA**, încălcând art. 15 și 22 din GDPR. Compania a fost obligată să ofere mai multă transparență și să justifice algoritmiile folosiți¹².

Acest caz evidențiază riscurile **automatizării deciziilor în relațiile de muncă** și subliniază necesitatea ca IA să fie supusă unor standarde de **transparență și contestabilitate**, mai ales în raporturile asimetrice angajator-angajat.

3. Sistemul de scoring social SyRI în Olanda

SyRI (System Risico Indicatie) a fost un sistem automatizat folosit de guvernul olandez pentru detectarea fraudei în domeniul prestațiilor sociale, folosind date din registre publice și private.

Probleme juridice:

- Lipsa transparenței algoritmice;
- Potențialul de discriminare socială sistemică;
- Încălcarea dreptului la viață privată, garantat de **art. 8 CEDO**.

În 2020, o instanță din Haga a declarat sistemul **neconstituțional**, considerând că încalcă **drepturile fundamentale**, în special dreptul la viață privată și la protecția datelor¹³.

Această decizie este un precedent important în limitarea **folosirii IA de către autoritățile publice**, în special când aceasta poate genera **profilări sociale automate** și afectează în mod disproporționat anumite grupuri vulnerabile.

4. Facebook / Cambridge Analytica – Profilare politică masivă

În 2018, a fost dezvăluit că datele personale a circa 87 de milioane de utilizatori Facebook au fost colectate și folosite, fără consimțământ explicit, de către Cambridge Analytica pentru campanii de influențare electorală.

Probleme juridice:

- Lipsa consimțământului valabil pentru utilizarea datelor;
- Prelucrarea de date sensibile prin **profilare psihografică și politică**;
- Nerespectarea obligațiilor de informare și securitate a datelor.

¹² Court of Amsterdam, Judgment of 11 March 2021, Case C/13/692003 / HA RK 20-302, Uber B.V. v. Worker Info Exchange.

¹³ Rechtbank Den Haag, ECLI:NL:RBDHA:2020:865, SyRI case, Netherlands, February 2020.

Facebook a fost amendată cu 5 miliarde USD de către FTC în SUA, iar în UE a fost cercetată de mai multe autorități pentru încălcări ale GDPR. În Regatul Unit, ICO a constatat lipsa unei baze legale pentru transferul și utilizarea datelor în scopuri electorale¹⁴.

Acest caz a scos în evidență riscurile majore asociate cu **profilarea algoritmică în scopuri politice**, subliniind nevoia de **reglementări stricte privind utilizarea IA în sfera democratică și de transparență electorală digitală**.

În concluzie, studiile de caz prezentate demonstrează că sistemele IA pot aduce beneficii semnificative, dar și **riscuri grave pentru drepturile fundamentale**, în special în ceea ce privește **viața privată și protecția datelor**. Ele evidențiază:

- Necesitatea unei **reglementări specializate** care să țină cont de specificul tehnologic al IA;
- Importanța **transparenței algoritmice și a supravegherii umane reale**;
- Rolul crucial al autorităților de protecție a datelor și al **instanțelor de contencios administrativ** în apărarea drepturilor persoanei într-un mediu digitalizat.

În acest context, **dreptul trebuie să evolueze proactiv**, nu doar reactiv, pentru a face față provocărilor aduse de era digitală.

Concluzie

Evoluția rapidă a inteligenței artificiale (IA) determină o transformare profundă a modului în care datele personale sunt colectate, analizate și utilizate, generând provocări juridice semnificative. Din perspectiva dreptului european, în special a **Regulamentului general privind protecția datelor (GDPR)**, constatăm că există un cadru solid de principii – precum legalitatea, transparența, limitarea scopului și responsabilitatea – însă **acest cadru nu este pe deplin adaptat complexității tehnologiilor IA**.

Mecanismele tradiționale de protecție, cum ar fi **consimțământul informat, dreptul de opoziție sau interzicerea deciziilor automatizate fără intervenție umană** (art. 22 GDPR), se confruntă cu limite în aplicare atunci când sistemele IA funcționează ca „cutii negre”, dificil de explicat chiar și de către dezvoltatori. Aceste limitări evidențiază **o tensiune între logica normativă a dreptului și logica tehnologică a IA**¹⁵.

Cazurile analizate – de la utilizarea recunoașterii faciale de către Clearview AI, la algoritmii opaci ai Uber sau la sistemele de profilare socială, precum SyRI – demonstrează că IA poate deveni un instrument de **supraveghere, excludere și discriminare**, dacă nu este controlată și reglementată în mod responsabil. Din acest motiv, dreptul nu trebuie să rămână pasiv, ci să devină **proactiv și anticipativ**, dezvoltând mecanisme capabile să guverneze etic și democratic tehnologia¹⁶.

Adoptarea viitorului **Regulament privind inteligența artificială (AI Act)** este un pas esențial în această direcție, oferind un cadru normativ diferențiat în funcție de riscul pe care sistemele IA îl implică. Totodată, integrarea IA în sfera publică și privată ar trebui să fie însoțită de:

- **auditi algoritmice independente**;
- **reguli de transparență și responsabilitate clar definite**;

¹⁴ UK Information Commissioner's Office (ICO), "Investigation into the use of data analytics in political campaigns", Final Report, 2018.

¹⁵ P. De Hert & V. Papakonstantinou, "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", *Computer Law & Security Review*, 34(2), 2018, pp. 179–194.

¹⁶ P. Nemitz, *Constitutional democracy and technology in the age of artificial intelligence. Philosophical Transactions of the Royal Society A*, 376(2133): 20180089, 2018.

- garantarea supravegherii umane semnificative.

În concluzie, **protecția datelor personale în era IA** nu mai poate fi concepută exclusiv ca o chestiune de conformitate juridică, ci trebuie abordată ca o **dimensiune esențială a demnității umane, a libertății individuale și a echității sociale**. Numai printr-un dialog constant între drept, tehnologie și etică se poate asigura o dezvoltare responsabilă a inteligenței artificiale, în deplin respect față de valorile fundamentale ale statului de drept.

References

- S. Barocas & A. D. Selbst, "Big Data's Disparate Impact", *California Law Review*, 104(3), 2016.
- CNIL, *Clearview AI: la CNIL met en demeure la société de cesser la réutilisation de photographies accessibles en ligne*, 2022, <https://www.cnil.fr>.
- Court of Amsterdam, Judgment of 11 March 2021, Case C/13/692003 / HA RK 20-302, Uber B.V. v. Worker Info Exchange.
- G. De Gregorio, "The Rise of Techno-Constitutionalism: A Legal Approach to Digital Power", *Columbia Journal of European Law*, 27(1), 2021.
- P. De Hert & V. Papakonstantinou, "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", *Computer Law & Security Review*, 34(2), 2018.
- EDPB, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 2020.
- European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, COM(2021) 206 final, 2021.
- O. Lynskey, "Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order", *International and Comparative Law Quarterly*, 63(3), 2019.
- A. Mantelero, "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment", *Computer Law & Security Review*, 34(4), 2018.
- P. Nemitz, *Constitutional democracy and technology in the age of artificial intelligence. Philosophical Transactions of the Royal Society A*, 376(2133): 20180089, 2018.
- Rechtbank Den Haag, ECLI:NL:RBDHA:2020:865, SyRI case, Netherlands, February 2020.
- Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016, art. 5 alin. (1) lit. a.
- A. D. Selbst & J. Powles, "Meaningful information and the right to explanation", *International Data Privacy Law*, 7(4), 2017.
- M. Tzanou, "Data protection as a fundamental right: The European Court of Justice and the European Data Protection Board", *European Law Review*, 44(3), 2019.
- UK Information Commissioner's Office (ICO), "Investigation into the use of data analytics in political campaigns", Final Report, 2018.
- S. Wachter, B. Mittelstadt & L. Floridi, (2017). "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law*, 7(2), 2017.