

REGÂNDIREA DREPTULUI ADMINISTRATIV PENTRU DECIZIILE ALGORITMICE*



Rebecca Williams**

Articolul este o traducere în limba română, realizată de avocat Roxana Mândruțiu, cu acordul expres al autoarei.

Rezumat: Prevalența crescândă a luării deciziilor algoritmice (ADM) de către autoritățile publice ridică o serie de provocări pentru dreptul administrativ sub forma deciziilor tehnice privind parametrii necesari pentru evaluarea acestor sisteme, opacitatea lor, scalabilitatea erorilor, utilizarea corelației în locul cauzalității și așa mai departe. Pentru ca dreptul administrativ să poată oferi orientările necesare pentru utilizarea optimă a acestor sisteme, acesta trebuie să devină mai nuanțat și mai elaborat în mai multe privințe. Cu toate acestea, dacă va fi în măsură să facă față acestei provocări, dreptul administrativ are potențialul nu numai de a contribui în mod util la controlul ADM, ci și de a sprijini activitatea Oficiului Comisarului pentru Informații*** și de a oferi orientări privind interpretarea unor noțiuni precum „informații semnificative” și „proporționalitate” în sensul GDPR.

27

Cuvinte-cheie: decizie algoritmică; control jurisdicțional; inteligență artificială; învățare automată

Abstract: The increasing prevalence of algorithmic decision making (ADM) by public authorities raises a number of challenges for administrative law in the form of technical decisions about the necessary metrics for evaluating such systems, their opacity, the scalability of errors, their use of correlation as opposed to causation and so on. If administrative law is to provide the necessary guidance to enable optimal use of such systems, there are a number of ways in which it will need to become more nuanced and advanced. However, if it is able to rise to this challenge, administrative law has the potential not only to do useful work itself in controlling ADM, but also to support the work of the Information Commissioner's Office and provide guidance on the interpretation of concepts such as 'meaningful information' and 'proportionality' within the General Data Protection Regulation.

Keywords: algorithmic decision making; judicial review; artificial intelligence; machine learning

* Articolul original a apărut în Oxford Journal of Legal Studies, Vol. 42, No. 2 (2022), pp. 468-494, doi:10.1093/ojls/ggab032.

** Rebecca Williams este Profesor de drept public și drept penal la Colegiul Pembroke, Oxford. Poate fi contactat la adresa de email rebecca.williams@law.ox.ac.uk.

Sunt foarte recunoscătoare atât colegilor mei, Profesor Tom Melham, Dr. Vaclav Janecek, Profesor Paul Craig, dr. Reuben Binns și dr. Jenet Williams, pentru observațiile lor pe drafturile anterioare, cât și editorilor anonimi. Orice erori reziduale strecurate în text îmi aparțin.

*** Nota traducătoarei: Oficiul Comisarului pentru Informații (Information Commissioner's Office – ICO) este autoritatea de supraveghere independentă din Regatul Unit cu atribuții în domeniul protecției datelor cu caracter personal și al libertății informației. Instituția are competența de a asigura respectarea legislației relevante, inclusiv UK GDPR și Data Protection Act 2018.

1. INTRODUCERE

Controversa privind algoritmul folosit pentru a genera notele la examenul de Bacalaureat (A levels¹⁾) a readus în prim-plan rolul din ce în ce mai important al algoritmilor în procesul de luare a deciziei publice²⁾, iar de la descrierea făcută de Cathy O'Neill³⁾ despre „Armele matematice de distrugere” (Weapons of Math Destruction) până la preocupările lui Frank Pasquale privind „cutiile negre”⁴⁾, suntem deja conștienți de pericolele pe care le pot prezenta aceste tehnologii. Chiar dacă există dovezi, atât în cazul Bacalaureatului, cât și în alte contexte⁵⁾, că autoritățile publice ar putea limita utilizarea acestor sisteme, presiunea crescândă asupra finanțelor publice și capacitatea sistemelor de a lua decizii mai ieftin decât oamenii fac improbabilă dispariția lor completă⁶⁾. Nici nu ne-am dori neapărat acest lucru; de exemplu, deși algoritmul pentru Bacalaureat a fost o soluție controversată la o problemă ridicată de pandemie⁷⁾, în domenii precum medicina, învățarea automată (*machine learning*) a fost în prima linie a cercetării și dezvoltării⁸⁾.

Scopul acestui articol este, prin urmare, de a analiza modul în care dreptul administrativ, în special, poate răspunde provocărilor reprezentate de luarea de decizii automatizate (ADM) de către autoritățile publice, într-un mod care să optimizeze utilizarea acestora, permițându-ne să valorificăm avantajele lor și să evităm riscurile pe care le pot genera⁹⁾.

¹⁾ B. Staton, L. Hughes, 'A-level and GCSE students to have downgraded results restored', Financial Times (London, 17 August 2020) <www.ft.com/content/273ff590-9651-4e25-aaa4-157d5b2948e1>.

²⁾ A se vedea și: L. Dencik, A. Hintz, J. Redden, H. Warne, 'Data Scores as Governance: Investigating Uses of Citizen Scoring in Public Services. Project Report' (Data Justice Lab, Cardiff University, December 2018) <<https://datajustice.files.wordpress.com/2018/12/data-scores-as-governance-project-report2.pdf>>; M Oswald, 'Algorithm-Assisted Decision-Making in the Public Sector: Framing the Issues Using Administrative Law Rules Governing Discretionary Power' (2018) 376 Philosophical Transactions of the Royal Society 2128, în special fn 7. A se vedea, de asemenea: J. Maxwell, J. Tomlinson, 'Public Law and Technology: Mapping and Analysing Legal Responses in UK Civil Society' [2020] PL 28, [24]. Pentru perspectiva existentă în Statele Unite ale Americii, a se vedea D. Freeman Engstrom și alții, 'Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies' (report submitted to the Administrative Conference of the United States, February 2020) <<https://law.stanford.edu/education/only-at-sls/law-policy-lab/practicums-2018-2019/administering-by-algorithm-artificial-intelligence-in-the-regulatory-state/acus-report-for-administering-by-algorithm-artificial-intelligence-in-the-regulatory-state/#slsnav-report>>. O investigație publicată în The Guardian în 2019 a descoperit că acestea sunt utilizate în 140 din 408 consilii din Regatul Unit: S. Marsh, 'One in Three Councils Using Algorithms to Make Welfare Decisions' The Guardian (London, 15 October 2019) <www.theguardian.com/society/2019/oct/15/councils-using-algorithms-make-welfare-decisions-benefits>.

³⁾ C. O'Neill, Weapons of Math Destruction (Penguin Random House USA 2016).

⁴⁾ F. Pasquale, The Black Box Society: The Secret Algorithms that Control Money and Information (Harvard UP 2015).

⁵⁾ S. Marsh, 'Councils Scrapping Use of Algorithms in Benefit and Welfare Decisions', The Guardian (London, 24 August 2020) <www.theguardian.com/society/2020/aug/24/councils-scrapping-algorithms-benefitwelfare-decisions-concerns-bias> .

⁶⁾ J. Naughton, 'From Viral Conspiracies to Exam Fiascos, Algorithms Come with Serious Side-Effects', The Guardian (London, 6 September 2020) <www.theguardian.com/technology/2020/sep/06/from-viral-conspiraciesto-exam-fiascos-algorithms-come-with-serious-side-effects> . A se vedea, de asemenea: *Patullo v HMRC* [2016] UKUT 270, [2016] BTC 510; *R (Barking and Dagenham College) v The Office for Students* [2019] EWHC 2667, [2020] ELR 152; *R (W) v Birmingham* [2011] EWHC 1147, [2011] Eq LR 721.

⁷⁾ A. Hern, 'Ofqual's A-Level Algorithm: Why Did It Fail to Make the Grade?', The Guardian (London, 21 August 2020) <www.theguardian.com/education/2020/aug/21/ofqual-exams-algorithm-why-did-it-fail-make-grade-a-levels> .

⁸⁾ A se vedea, e.g.: O. Kadioglu, M. Saeed, H. Johannes Greten, T. Efferth, Identification of novel compounds against three targets of SARS CoV-2 coronavirus by combined virtual screening and supervised machine learning. [Preprint]. Bull World Health Organ. E-pub: 21 March 2020. doi:<http://dx.doi.org/10.2471/BLT.20.25594>; S. Whitelaw și alții, 'Applications of Digital Technology in COVID-19 Pandemic Planning and Response' (2020) 2 The Lancet Digital Health 435.

⁹⁾ Pentru detalii, a se vedea T. Melham, R. Williams, Practical Law Public Sector, 8 Decembrie 2020.

2. CE ESTE UN ALGORITM?

Înainte de a analiza cum instrumentarul dreptului public poate contribui în acest domeniu, merită să ne amintim că decizia algoritmică nu reprezintă un concept nou. Hill descrie algoritmii ca fiind „construcții matematice” cu „o structură de control finită, abstractă și eficientă, imposibil de ocolit, care îndeplinesc un scop dat în conformitate cu dispoziții date”¹⁰⁾.

Analiza algoritmilor din sistemul de justiție penală realizată de Law Society citează definiția clasică din informatică, conform căreia un algoritm este „orice procedură de calcul bine definită care ia ca input o valoare (sau un set de valori) și produce ca output o valoare (sau un set de valori)”¹¹⁾.

Astfel, chiar și un simplu arbore decizional desenat pe o foaie de hârtie poate constitui un exemplu de decizie algoritmică¹²⁾, iar astfel de algoritmi au fost adesea utilizați de autoritățile publice¹³⁾. Acest tip de algoritm este utilizat în așa-numitele „sisteme expert” de inteligență artificială (IA), care sunt cunoscute, în mod surprinzător, sub denumirea de sisteme bazate pe reguli. Aceste sisteme sunt complexe, dar transparente, iar cei care le programează au control deplin asupra setului precis de reguli „dacă-atunci” pe care le urmează.

Cu toate acestea, un subset al IA, cunoscut sub numele de învățare automată (*machine learning – ML*), utilizează un algoritm pentru a construi un model matematic pornind de la date, de jos în sus, în loc să construiască toate regulile relevante de sus în jos, așa cum fac sistemele bazate pe reguli.

Există o varietate de forme de ML, inclusiv „învățarea profundă” (*deep learning*), denumită astfel deoarece structura algoritmului cuprinde mai multe straturi conectate. Un strat de intrare conține datele inițiale, un strat de ieșire produce rezultatul corespunzător acelor date, iar între ele există mai multe straturi ascunse alcătuite din „noduri” interconectate. Interconectarea acestor noduri este ceea ce dă acestui tip de învățare profundă denumirea de „rețea neuronală artificială”, ca o referință (de fapt, destul de diferită) la rețelele neuronale biologice¹⁴⁾.

Aceste tipuri de algoritmi sunt mult mai puțin transparente decât sistemele expert sau cele bazate pe reguli¹⁵⁾, însă există metode prin care performanța lor poate fi evaluată.

¹⁰⁾ R.K. Hill, 'What an Algorithm Is' (2015) 29 Philosophy & Technology 35.

¹¹⁾ S. Bhatti și alții, 'Algorithms in the Criminal Justice System: A Report by the Law Society Commission on the Use of Algorithms in the Justice System' (The Law Society of England and Wales, June 2019) 10.

¹²⁾ *Sharman v HM Coroner for Inner North London* [2005] EWCA Civ 967, [2005] Inquest LR 168. A se vedea, de asemenea, V. Mayer-Schönberger, K. Cukier, *Big Data* (John Murray 2013) 73–6. A se vedea, de asemenea, M. Veale, I. Brass, 'Administration by Algorithm? Public Management Meets Public Sector Machine Learning' in K Yeung and M Lodge (eds), *Algorithmic Regulation* (OUP 2019); C Coglianese and D Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 Geo LJ 1147.

¹³⁾ A se vedea, e.g., algoritmul formularului ICA1 pentru clasificarea deținuților menționat în *R (Guittard) v Secretary of State for Justice* [2009] EWHC 2951; și PSI-17-2006, menționat în *R (Lewis) v HM Coroner* [2009] EWHC 661, (2009) 108 BMLR 87.

¹⁴⁾ A se vedea, e.g., J. Schmidhuber, 'Deep Learning in Neural Networks: An Overview' (2016) 61 Science Direct 85.

¹⁵⁾ Pentru o prezentare a diferitelor tehnici algoritmice cu diferite niveluri de transparență, a se vedea The ICO and the Alan Turing Institute, 'Explaining Decisions Made with AI' (20 May 2020) Anexa 2 <<https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-ai/>>.

3. EVALUAREA PERFORMANȚEI ML (MACHINE LEARNING)

Imaginați-vă că un sistem a învățat (cu sau fără supraveghere) să detecteze formele „soare”, respingând în același timp fulgerele. Sistemului i se prezintă apoi o serie de forme pe care trebuie să le identifice, iar rezultatul este prezentat în figura 1.

Toate formele din zonele 1, 2, 3 și 4 sunt afișate sistemului. Sistemul identifică drept soare elementele din dreptunghiul mai mic (3+4).

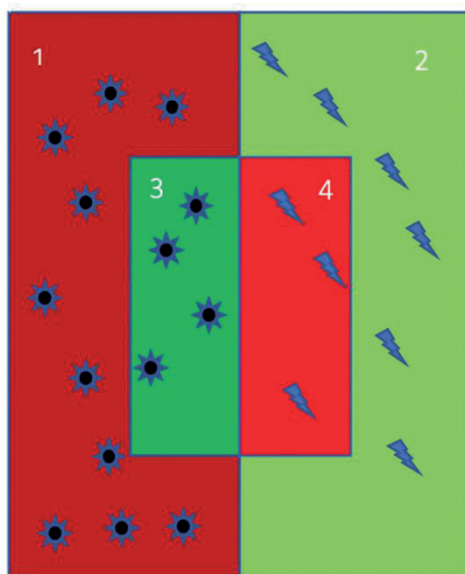


Figura 1. Ilustrarea unui exemplu de rezultate obținute de un sistem de identificare a formelor

Zona 1 conține, prin urmare, forme de soare care nu sunt detectate de sistem (fals negativ)

Zona 2 conține fulgere care sunt respinse corect de sistem (adevărat negativ)

Zona 3 conține forme de soare care sunt recunoscute corect de sistem (adevărat pozitiv) și

Zona 4 conține fulgere care sunt identificate incorect ca soare de către sistem (rezultate fals pozitive). Există diverse modalități de măsurare a preciziei acestui sistem.

De exemplu, „sensibilitatea” (sau „rata de rezultate pozitive reale”)¹⁶⁾ a sistemului este o măsură a numărului de elemente-țintă identificate. Astfel, sensibilitatea acestui sistem ar fi $4/14$; sistemul a identificat corect 4 sori (în zona 3) dintr-un total de 14 sori posibili (zonele 1 și 3). Aceasta poate fi considerată și probabilitatea de detectare.

În schimb, „specificitatea” unui sistem este cunoscută și sub denumirea de „rata negativă adevărată”, identificând câte elemente au fost respinse corect. Așadar, „specificitatea” acestui sistem ar fi $2/3$, deoarece a respins corect 6 (în zona 2) din 9 fulgere (în zonele 2 și 4).

O a treia unitate de măsură, cunoscută sub numele de „precizie”, evaluează câte dintre răspunsurile pozitive au fost adevărate, în comparație cu falsele pozitive. Deci, pentru acest sistem, precizia ar fi $4/7$. Sistemul a identificat 7 elemente (zonele 3 și 4), dar numai 4 dintre ele sunt sori – valori pozitive adevărate.

¹⁶⁾ Uneori denumită „recall” (rată de regăsire).

Un al patrulea indicator, cunoscut sub denumirea de „valoare predictivă negativă”, evaluează câte dintre răspunsurile negative au fost adevărate, în comparație cu cele false. Deci, pentru acest sistem, valoarea ar fi 6/16.

„Precizia”, pe de altă parte, măsoară performanța globală a sistemului.

În acest caz, ar fi numărul de elemente clasificate corect în zonele 3 și 2 (10) ca proporție din toate elementele din toate zonele (23), adică 10/23.

S-ar putea crede că precizia ar fi întotdeauna cel mai bun indicator pentru evaluarea unui anumit sistem, dar, desigur, acest lucru va depinde de gravitatea erorilor. Dacă modelul de mai sus ar avea ca obiectiv detectarea cancerului la pacienți, atunci numărul de rezultate fals negative (adică sori omiși în zona 1) ar putea fi mai problematic decât fulgerele identificate incorect în zona 4 și, prin urmare, sensibilitatea sistemului ar putea fi mai importantă decât precizia sa de ansamblu.

4. ESTE DECIZIA ALGORITMICĂ PROBLEMATICĂ?

Faptul că o decizie este luată de un algoritm nu înseamnă automat că aceasta este problematică. Dimpotrivă, în unele cazuri, poate fi chiar benefică – de exemplu, dacă un algoritm poate fi învățat să identifice celulele canceroase mai rapid decât un om¹⁷⁾.

Chiar și O'Neill, care declară că nu este o adeptă a big data¹⁸⁾ și își dedică lucrarea „concentrării atenției în direcția opusă, asupra daunelor provocate de armele de distrugere în masă și asupra nedreptății pe care acestea o perpetuează”¹⁹⁾, sugerează că ar utiliza datele pentru a descoperi impactul detenției în regim de izolare asupra recidivismului²⁰⁾ și menționează impactul pozitiv pe care luarea deciziilor bazate pe date îl poate avea asupra selecțiilor în baseball²¹⁾. De altfel, nici ființele umane nu sunt infailibile.

Oamenii își pot baza deciziile pe intuiție²²⁾, pot avea prejudecăți conștiente sau inconștiente, pot fi influențați de propriile trăiri sau emoții (de exemplu, performanța echipei lor de fotbal preferate²³⁾) sau pot acționa inconsecvent²⁴⁾ de la un caz la altul. Așadar, este greu de susținut că un proces decizional mai bine informat, mai sistematic, coerent și consecvent ar fi un pas în direcția greșită²⁵⁾.

Cu toate acestea, există mai multe moduri prin care dreptul public va trebui să se adapteze pentru a controla eficient aceste sisteme.

¹⁷⁾ S.M. McKinney și alții, 'International evaluation of an AI system for breast cancer screening' (2020) 577 Nature 89.

¹⁸⁾ *Supra* n 1, 13.

¹⁹⁾ *Ibidem*.

²⁰⁾ *Supra* n 3, 98.

²¹⁾ *Supra* n 3, 27.

²²⁾ R. Brauneis, E. Goodman, 'Algorithmic Transparency for the Smart City' (2018) 20 Yale Journal of Law & Technology, 103, 112.

²³⁾ O. Eren, N. Mocan, 'Emotional Judges and Unlucky Juveniles' (2018) 10(3) American Economic Journal: Applied Economics 171.

²⁴⁾ A se vedea doctrina așteptărilor legitime în dreptul administrativ, abordată în detaliu în cauza *Mandalia v Secretary of State for the Home Department* [2015] UKSC 59, [2015] 1 WLR 4546.

²⁵⁾ Pentru mai multe detalii, a se vedea Kriti Sharma, citată de the House of Lords Select Committee on Artificial Intelligence, AI in the UK: Ready, Willing and Able? (HL 2017-19, 100-I) [118] <<https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>>. A se vedea, de asemenea, J. Cobbe, 'Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making' (2019) 39 LS 636.

5. LEGISLAȚIA

A. PERMISIUNEA DE A UTILIZA DECIZIILE ALGORITMICE (ADM)

Prima chestiune pe care o punem în discuție este dacă o autoritate publică poate utiliza ADM. Articolul 22 din Regulamentul general privind protecția datelor²⁶⁾ prevede că persoanele vizate au dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv pe crearea de profiluri, care produce efecte juridice în ceea ce le privește sau le poate afecta în mod similar, cu excepția cazului în care există o bază legală.

În general, un astfel de temei juridic poate fi asigurat prin consimțământ [articolul 22 alineatul (2) litera (c)], dar este puțin probabil ca aceasta să fie o opțiune pentru autoritățile publice, având în vedere că considerentul 43 din GDPR prevede că consimțământul nu ar putea constitui un temei juridic valabil pentru prelucrarea datelor cu caracter personal într-un caz în care există un dezechilibru evident între persoana vizată și operator, în special în cazul în care operatorul este o autoritate publică și, prin urmare, este puțin probabil ca consimțământul să fi fost acordat în mod liber în raport cu circumstanțele specifice ale situației respective.

Considerentele nu sunt, desigur, obligatorii din punct de vedere juridic, dar nici nu sunt complet irelevante, CJUE statuând că, „deși un considerent din preambulul unui regulament poate clarifica interpretarea care trebuie dată unei norme juridice, acesta nu poate constitui în sine o astfel de normă”²⁷⁾. Prin urmare, pare indicat ca autoritățile publice să opteze pentru o abordare prudentă, considerând că ADM va necesita autorizarea statelor membre sau a UE în legislația „care prevede, de asemenea, măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate” [articolul 22 alineatul (2) litera (b)].

În cazul în care prelucrarea în cauză se referă la date sensibile în sensul articolului 9 (care dezvăluie apartenența rasială sau etnică, opiniile politice, convingerile religioase sau filozofice și apartenența la un sindicat sau date genetice, biometrice, medicale sau referitoare la orientarea sexuală), prelucrarea trebuie să fie necesară din motive de interes public major, să aibă un temei legal, să fie proporțională cu scopul urmărit, să respecte esența dreptului la protecția datelor și să prevadă, din nou, măsuri adecvate și specifice pentru a proteja drepturile și interesele fundamentale ale persoanei vizate [articolul 22 alineatul (4) din RGPD].

Din ianuarie 2021, GDPR este inclus în UK GDPR²⁸⁾. În orice caz, în legislația națională existentă, secțiunea 14 din Legea privind protecția datelor (DPA) din 2018 încorporează articolul 22 alineatul (2) litera (b)²⁹⁾, în timp ce secțiunea 49 prevede că un operator care aplică legea nu poate lua o decizie importantă bazată exclusiv pe prelucrarea automată, cu excepția cazului în care această decizie este prevăzută sau autorizată de lege, și că o decizie este una „semnificativă” dacă produce un efect juridic negativ asupra persoanelor vizate sau le afectează în mod semnificativ. O dispoziție similară este prevăzută în secțiunea 96 pentru cele ale serviciilor de informații.

²⁶⁾ Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului [2016] OJ L119/1 (GDPR).

²⁷⁾ Cauza 215/88 *Casa Fleischhandels* [1989] ECR 2789 [31]

²⁸⁾ Programul Keeling pentru care poate fi găsit la adresa www.gov.uk/government/publications/data-protectionlaw-eu-exit. *Nota traducătoarei:* În conformitate cu Withdrawal Agreement Act 2020 (WAA 2020), dispozițiile dreptului unional – inclusiv Regulamentul general privind protecția datelor (GDPR) și jurisprudența Curții de Justiție a Uniunii Europene (CJUE) – au continuat să se aplice în Regatul Unit până la finalul perioadei de tranziție, încheiate la 31 decembrie 2020. Începând cu 1 ianuarie 2021, GDPR a fost integrat în dreptul intern britanic sub denumirea de UK GDPR, parte din așa-numitul *retained EU law* (dreptul unional păstrat), cu anumite modificări adaptate contextului național.

²⁹⁾ Cu toate că sunt în curs de aprobare modificări care vor face ca secțiunea să facă trimitere la articolul 22 din GDPR.

Prin urmare, concluzia este că, dacă autoritățile publice doresc să se bazeze în totalitate pe ADM, vor avea nevoie de un temei juridic specific care să prevadă măsuri de protecție pentru persoanele vizate.

B. DREPTURILE APLICABILE ÎN CADRUL ADM

În cazul în care autoritatea publică utilizează ADM, aceasta conferă persoanei vizate drepturi suplimentare. În primul rând, în momentul obținerii datelor de la persoana vizată, articolul 13 alineatul (2) litera (f) din GDPR conferă persoanei vizate dreptul de a ști despre existența ADM, inclusiv a creării de profiluri; dreptul la „informații semnificative despre logica implicată”; și dreptul de a cunoaște semnificația și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

Considerentul 71 adaugă că acestea ar trebui să includă „o explicație a deciziei luate în urma unei astfel de evaluări”. Acestea sunt *drepturi pasive*, în sensul că operatorul de date trebuie să furnizeze aceste informații în mod voluntar.

În cazul în care datele sunt transmise ulterior altor operatori și urmează să fie utilizate din nou pentru ADM, persoana vizată are dreptul la aceleași informații, acum în temeiul articolului 14 alineatul (2) litera (g), fie în termen de o lună de la primirea datelor de către noul operator (articolul 14 alineatul (3) litera (a)), fie la momentul primei comunicări cu persoana vizată (articolul 14 alineatul (3) litera (b)), oricare dintre aceste date este mai recentă. Acesta este, de asemenea, un drept pasiv pe care operatorul de date trebuie să îl respecte în mod spontan.

În plus față de aceste drepturi, articolul 15 alineatul (1) litera (h) conferă persoanei vizate *dreptul de a obține în mod activ* aceste informații în orice moment. După cum subliniază Grupul de lucru „Articolul 29” [denumit în prezent Comitetul european pentru protecția datelor (EDPB)], este vorba de o dispoziție de „siguranță”, deoarece persoana vizată ar fi trebuit să primească deja aceste informații, în temeiul drepturilor pasive reglementate la articolul 13 sau 14³⁰⁾. Articolul 22 conferă, de asemenea, persoanelor fizice „cel puțin dreptul de a beneficia de intervenția umană din partea operatorului” pentru a-și exprima punctul de vedere și a contesta decizia.

Se pune atunci întrebarea ce se înțelege mai precis prin „informații semnificative despre logica implicată”, iar dezbaterea academică pe această temă este bine cunoscută.

Goodman și Flaxman au susținut inițial că această dispoziție conferă dreptul la o „explicație completă”, ceea ce ar limita posibilitatea de a utiliza ML care acționează într-un mod mai opac³¹⁾.

Acest argument a fost apoi contrazis de Wachter, Mittelstadt și Floridi, care au susținut că „dreptul de acces [...] conferă doar acces la o explicație *ex ante* a funcționalității sistemului. [...] [E]ste rezonabil să se pună la îndoială faptul că dreptul de acces ar conferi dreptul la explicații *ex post* ale deciziilor deja luate într-un caz dat³²⁾”.

O a treia opinie, exprimată de Selbst și Powles, a susținut, în schimb, că normele legale ar trebui interpretate într-un mod flexibil și ar trebui să permită, cel puțin, persoanelor vizate să își exercite drepturile conferite

³⁰⁾ Article 29 EC Data Protection Working Party, ‘Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679’ COM (2018) 26.

³¹⁾ B. Goodman, S. Flaxman, ‘EU regulations on Algorithmic Decision-Making and a “Right to Explanation”’ (2017) 38(3) AI Magazine 50.

³²⁾ S. Wachter, B. Mittelstadt, L. Floridi, ‘Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation’ (2017) 7 IDPL 76, 83 și 84.

de GDPR, precum și alte drepturi fundamentale³³⁾. O opinie similară este exprimată de Kaminski³⁴⁾, iar această perspectivă este în concordanță cu concluzia EDPB conform căreia „informațiile furnizate ar trebui să fie suficient de detaliate pentru ca persoana vizată să înțeleagă motivele care stau la baza deciziei”, cum ar fi „detalii privind principalele aspecte luate în considerare la luarea deciziei, sursa acestor informații și relevanța acestora³⁵⁾”.

Flexibilitatea și caracterul particular al contextului explicației sunt subliniate atât de Oficiul Comisarului pentru Informații (ICO), cât și în raportul³⁶⁾ Institutului Alan Turing, care identifică șase tipuri de explicații: raționamentul (motivele care au condus la o decizie); responsabilitatea (cine este implicat și cui trebuie să se adreseze persoana vizată); o descriere a datelor care au fost utilizate și a modului în care au fost utilizate; o explicație a modului în care se asigură un tratament egal și echitabil; o explicație a siguranței și performanței sistemului în termeni de fiabilitate, securitate și robustețe; și, în final, o explicație a impactului potențial al sistemului asupra persoanelor și societății³⁷⁾. Aceștia explică:

Cercetările noastre proprii relevă că contextul este un aspect cheie în explicarea deciziilor care implică IA. Prin urmare, când vorbim despre explicații, nu ne referim la o singură abordare sau la furnizarea unui singur tip de informații. În schimb, contextul influențează tipul de explicație pe care îl folosiți pentru a face o decizie asistată de IA clară sau ușor de înțeles de către persoanele fizice³⁸⁾.

În timp ce, pentru a declanșa articolul 22, decizia trebuia să se bazeze exclusiv pe prelucrarea automatizată, după cum observă EDPB, articolul 4 alineatul (4) din GDPR definește crearea de profiluri ca fiind orice formă de prelucrare automatizată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru evaluarea anumitor aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau a prezice aspecte referitoare la performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, încrederea, comportamentul, locația sau deplasările persoanei fizice respective.

Astfel, pentru EDPB, atât timp cât realizarea de profiluri implică o formă de prelucrare automatizată, intervenția umană nu exclude neapărat activitatea din sfera definiției. Prin urmare, drepturile prevăzute la articolele 13-15 se aplică atât timp cât există o formă de prelucrare automatizată în decizie, indiferent dacă decizia se bazează exclusiv pe prelucrarea automatizată (articolul 22) sau nu³⁹⁾. În cazul prelucrării exclusiv automatizate bazate pe consimțământ sau pe un contract, articolul 22 conferă persoanelor fizice „cel puțin dreptul de a obține intervenția umană din partea operatorului pentru a-și exprima punctul de vedere și pentru a contesta decizia.

Acest lucru nu se aplică în mod specific prelucrării bazate pe lege, care, după cum s-a menționat mai sus, este probabil să constituie justificarea aplicabilă pentru autoritățile publice. Cu toate acestea, pare mai probabil că acest lucru se datorează faptului că se anticipează că astfel de garanții vor fi prevăzute în „măsurile adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate” [articolul 22 alineatul (2) litera (b)], care trebuie să fie incluse și în legea respectivă, și nu pentru că GDPR anticipează absența totală a unor astfel de garanții. Acest lucru este confirmat de EDPB, care afirmă că „astfel de măsuri

³³⁾ A. Selbst, J. Powles, ‘Meaningful Information and the Right to Explanation’ (2017) 7 IDPL 233.

³⁴⁾ M. Kaminski, ‘The Right to Explanation, Explained’ (2019) 34 Berkeley Technology Law Journal 189.

³⁵⁾ *Supra* n 30, 25–6.

³⁶⁾ *Supra* n 14. *Nota traducătoarei*: Institutul Alan Turing este Institutul Național al Regatului Unit pentru știința datelor și inteligența artificială, fondat în 2015 și finanțat în mare parte de guvernul britanic. Este numit după Alan Turing, matematicianul britanic, considerat unul dintre pionierii informaticii și inteligenței artificiale.

³⁷⁾ *Ibidem* 20, *inter alia*.

³⁸⁾ *Ibidem* 21.

³⁹⁾ *Supra* n 30, 17.

ar trebui să includă cel puțin posibilitatea pentru persoana vizată de a obține intervenția unei persoane, de a-și exprima punctul de vedere și de a contesta decizia”⁴⁰⁾.

Legislația națională reflectă în mare măsură acest lucru, prevăzând în DPA 2018, secțiunea 14, că, în cazul în care o decizie importantă bazată exclusiv pe prelucrarea automatizată este necesară sau autorizată de lege, operatorul trebuie să notifice în scris persoana vizată, în cel mai scurt timp posibil, cu privire la faptul că a fost luată o astfel de decizie. Persoana vizată are apoi la dispoziție o lună pentru a solicita operatorului fie să reconsidere decizia, fie să ia o nouă decizie care să nu se bazeze exclusiv pe prelucrarea automatizată, declanșând astfel o nouă perioadă de o lună în care operatorul trebuie să examineze, să se conformeze și să informeze persoana vizată.

C. OBLIGAȚIA DE A ASIGURA EGALITATEA ÎN SECTORUL PUBLIC ȘI LEGEA PRIVIND DREPTURILE OMULUI DIN 1998

În plus, Legea egalității din 2010, secțiunea 149(1), prevede că o autoritate publică, în exercitarea funcțiilor sale, trebuie să țină seama în mod corespunzător de necesitatea de a elimina discriminarea, hărțuirea, victimizarea și orice alt comportament interzis de Legea din 2010 și trebuie să promoveze egalitatea de șanse și să favorizeze relațiile bune între persoanele care au o caracteristică protejată relevantă și cele care nu au o astfel de caracteristică.

Secțiunea 1(3) prevede în continuare că luarea în considerare a necesității de a promova egalitatea de șanse implică luarea în considerare, în special, a necesității de a elimina sau de a reduce la minimum dezavantajele suferite de persoanele care împărtășesc o caracteristică protejată relevantă legată de această caracteristică, de a lua măsuri pentru a răspunde nevoilor diferite ale acestor persoane și de a încuraja aceste persoane să participe la viața publică sau la alte activități în care participarea acestora este disproporționat de scăzută.

Caracteristicile protejate relevante sunt vârsta, handicapul, schimbarea de sex, sarcina și maternitatea, rasa, religia sau convingerile, sexul și orientarea sexuală. Protecția este, desigur, asigurată și de Legea privind drepturile omului din 1998.

Ambele forme de protecție au jucat un rol semnificativ în decizia din cauza *Bridges*⁴¹⁾, unul dintre primele cazuri de drept administrativ care a abordat unele dintre aceste chestiuni⁴²⁾.

În acest caz, domnul Bridges a susținut că utilizarea tehnologiei de recunoaștere facială automată (AFR) de către poliția din South Wales (SWP) era ilegală. Curtea de Apel a fost de acord, considerând că utilizarea tehnologiei nu era „în conformitate cu legea”, în sensul articolului 8 alineatul (2) din Convenția europeană a drepturilor omului (CEDO)⁴³⁾, deoarece nu existau orientări clare cu privire la situațiile în care tehnologia putea fi utilizată și la persoanele care puteau fi incluse pe o listă de supraveghere.

⁴⁰⁾ *Ibidem* 27.

⁴¹⁾ *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, [2020] 1 WLR 5037.

⁴²⁾ Acțiuni în justiție fuseseră avute în vedere anterior, ca reacție la deciziile privind examenele A-level (Foxglove, 17 august 2020, accesat la 14 septembrie 2021) și la instrumentul de triere automată a vizelor [Foxglove, 4 august 2020, accesat la 14 septembrie 2021; H. McDonald, „Sistemul de inteligență artificială pentru acordarea vizelor în Regatul Unit este pătător, afirmă organizații pentru drepturile omului”, *The Guardian* (Londra, 29 octombrie 2019), disponibil online, accesat la 18 mai 2021]. Niciunul dintre cazuri nu a ajuns în instanță, întrucât sistemele respective fuseseră între timp abandonate.

⁴³⁾ A se vedea și cauza din Țările de Jos (ECLI:NL:RBDHA:2020:1878) în care o hotărâre a Tribunalului din Haga a stabilit că un sistem denumit SyRI, utilizat de guvernul olandez pentru a detecta diverse forme de fraudă – inclusiv fraude privind beneficiile sociale, alocațiile și impozitele – încalcă articolul 8 din CEDO.

Curtea a constatat, de asemenea, că forțele de poliție nu au făcut tot ce era rezonabil pentru a-și îndeplini obligația care le revenea în temeiul Public Sector Equality Duty (PSED) (Obligația de egalitate în sectorul public).

În prima instanță, în cauza *Bridges*, instanța a audiat un ofițer de poliție cu privire la utilizarea sistemului AFR Locate după finala Ligii Campionilor UEFA din 2017 și până în iunie 2018. În timpul utilizării sistemului, au fost generate 290 de alerte. Optzeci și două dintre acestea erau alerte pozitive reale, iar 208 erau alerte pozitive false⁴⁴.

Aceste statistici se aplicau numai celor care au generat o alertă. Identitatea celor care au trecut de camera de supraveghere fără a genera o alertă nu era cunoscută. Instanța a mai aflat că

[188] 188 dintre alerte erau bărbați (65 %). Dintre cele 188 de alerte privind bărbați, 64 (34 %) erau alerte pozitive reale, iar 124 (66 %) erau alerte pozitive false. În ceea ce privește femeile, dintre 102 alerte, 18 (18 %) erau alerte pozitive reale și 84 (82 %) erau alerte pozitive false.

O serie de alerte false referitoare la femei au fost corelate în principal cu două persoane pe care furnizorul software-ului AFR le-ar fi numit „lamb”. Un „lamb” este o persoană al cărei chip are trăsături atât de comune, încât poate fi identificat mult mai frecvent.

Același ofițer de poliție a examinat și etnia persoanelor care făceau obiectul unei alerte. Dintre rezultatele pozitive reale (82), 98 % erau „albi nord-europeni”.

Dintre rezultatele pozitive false (208), 98,5 % erau „albi nord-europeni”. Prin urmare, ofițerul a concluzionat că, pe baza experienței sale și a informațiilor de care dispunea, nu a constatat nicio prejudecată bazată pe sex sau etnie.

Cu toate acestea, instanța de fond a audiat și expertul Dr. Jain, profesor de informatică din SUA, în opinia căruia un factor-cheie pentru acuratețea unui astfel de sistem ar fi exactitatea datelor de antrenare (prin aceasta înțelegându-se probabil cât de reprezentative sunt datele de antrenare pentru distribuția reală a exemplelor în lume sau dacă acestea sunt în vreun fel distorsionate). Se pare că SWP nu avea cunoștință de datele utilizate pentru instruirea sistemului, ceea ce înseamnă că nu avea niciun mijloc de a stabili dacă a existat sau nu o prejudecată. În schimb, reprezentantul companiei care furnizează tehnologia AFR utilizată de SWP a demonstrat că sistemul a fost antrenat pe date care conțineau un număr aproximativ egal de fețe masculine și feminine și o gamă largă de etnii, deși, din motive de confidențialitate comercială, nu au fost furnizate mai multe detalii despre date. Răspunsul Dr. Jain la acest argument a fost că, fără posibilitatea de a efectua o evaluare aprofundată a structurii demografice a setului de date utilizat pentru instruirea algoritmului, SWP nu ar fi în măsură să aprecieze dacă setul de date utilizat pentru instruire era sau putea fi părtinitor.

În recurs, Curtea de Apel a formulat două observații cu privire la aceste probe.

Una dintre acestea era că ofițerul audiat în cauză nu era un expert tehnic în software-ul în cauză, prin care se presupune că se referea la știința datelor. Și aceasta deși Curtea de Apel a considerat că „nu este rolul acestei instanțe să se pronunțe asupra diferitelor puncte de vedere exprimate de [cei doi martori]. Acest lucru nu ar fi adecvat într-o acțiune în contencios administrativ, cu atât mai puțin în recurs⁴⁵”, ea a procedat totuși într-un mod foarte similar.

Și, într-adevăr, este dificil de înțeles cum s-ar fi putut evita acest lucru. Simplul fapt de a afirma că SWP nu a mers prea departe, fără a indica ce măsuri suplimentare ar fi fost necesare, nu ar fi fost de ajutor.

⁴⁴) Pentru definiția acestor termeni și alte detalii, a se vedea n 16 *supra* și pasajele adiacente.

⁴⁵) *Supra* n 41, [199].

Pentru a oferi îndrumare, era inevitabil ca instanța din cauza *Bridges*, așa cum se va întâmpla fără îndoială în viitoarelor cereri în contencios administrativ de acest tip, să se angajeze într-o analiză detaliată a probelor tehnice.

În ceea ce privește fondul, în furnizarea acestor orientări, al doilea punct subliniat de Curtea de Apel a fost că, deși înțelegea că ștergerea imediată a datelor persoanelor care nu generaseră o alertă era o garanție integrală a protecției datelor, acest lucru nu însemna că software-ul nu avea o prejudecată încorporată care trebuia evaluată și care putea fi evaluată numai prin accesul la aceste date. Curtea a continuat susținând că SWP nu a încercat să se asigure, nici direct, nici prin verificări independente, că programul software în cauză nu avea o prejudecată inacceptabilă pe motive de rasă sau sex.

Deși Curtea a înțeles preocupările legate de confidențialitatea comercială, lipsa de informații rezultată (care include, cel mai probabil, și setul de date de antrenament) „nu permite unei autorități publice să își îndeplinească obligația proprie, care nu poate fi delegată, în temeiul articolului 149”⁴⁶⁾.

Și, într-adevăr, Curtea concluzionase anterior că „pentru a confirma dacă un sistem AFR este părtinitor, ar trebui să se cunoască cel puțin datele statistice din baza de date, cum ar fi numărul de bărbați și de femei și diferitele rase luate în considerare”⁴⁷⁾.

S-ar putea considera, așadar, că, dacă o autoritate publică dorește să utilizeze un astfel de algoritm, va trebui, în primul rând, să obțină aceste date în cadrul contractului său cu furnizorul privat al sistemului. Însă, întrucât acest lucru poate fi nerealist din punct de vedere comercial, pare să existe o nevoie urgentă de a furniza o metodă alternativă de conformare cu PSED. După cum sugerează dovezile prezentate de dr. Jain, accesul la datele reale nu este necesar atât timp cât există „un anumit tip de evaluare exhaustivă a structurii demografice a setului de date de instruire a algoritmului”.

Dar pericolul în acest caz este că autoritatea publică ar trebui să aibă încredere că proprietarul setului de date furnizează aceste informații în mod corect și, invers, proprietarul setului de date ar putea fi preocupat de faptul că divulgarea prea multor informații ar putea duce la dezvăluirea datelor sensibile din punct de vedere tehnic/comercial.

Prin urmare, este preferabil să existe o formă de verificare reglementată prin lege, prin care entitatea de verificare să poată avea acces la datele sensibile din punct de vedere comercial (așa cum face, de exemplu, oficiul de brevete) pentru efectuarea verificărilor necesare.

Utilizarea unui sistem care a primit o „marcă de conformitate” de la o astfel de entitate ar fi atunci conformă cu PSED. În prezent, însă, nu există un astfel de sistem, iar cauza *Bridges* se ocupă doar de un singur set de teste care trebuie efectuate.

6. COMMON LAW

După cum se arată în secțiunea de mai sus, până în prezent, prevederile legale au reglementat și au fost utilizate pentru a viza ADM-ul autorităților publice, dar se pare că, în viitor, normele de control judiciar din *common law* vor juca, de asemenea, un rol important⁴⁸⁾.

⁴⁶⁾ *Ibidem*.

⁴⁷⁾ *Ibidem* [193].

⁴⁸⁾ Pentru detalii, a se vedea R. Binns, ‘Algorithmic Decision-Making: A Guide for Lawyers’ (2020) 25 JR 2.

Controlul jurisdicțional exercitat în materie de contencios administrativ are un rol arbitral, fiind activat exclusiv în cazurile în care o autoritate publică a încălcat dispoziții legale exprese și limitative, fără a se substitui aprecierii oportunității deciziei administrative⁴⁹⁾.

Chestiunile juridice a căror respectare este verificată în contencios administrativ sunt următoarele: decizia să fie luată doar de către o autoritate publică competentă⁵⁰⁾; autoritatea publică nu trebuie să-și limiteze sau să-și delege atribuțiile⁵¹⁾; autoritatea publică trebuie să respecte procedura prevăzută de lege, ceea ce înseamnă, printre altele, că nu trebuie să fie pârinitoare; trebuie să audieze persoanele competente și să-și motiveze decizia⁵²⁾; trebuie să țină seama de toate considerentele relevante, iar nu de considerente străine în luarea deciziei sale⁵³⁾; decizia sa finală să respecte principiul proporționalității⁵⁴⁾.

Deși nerespectarea acestor norme sunt toate motive de control jurisdicțional care pot fi invocate împotriva unei autorități publice, controlul jurisdicțional nu presupune că instanța este în totală contradicție cu interesele autorităților publice. Rolul instanței care exercită controlul jurisdicțional este acela al „judecătorului care veghează”, pentru a oferi îndrumări pozitive *ex ante*, precum și pentru a verifica *ex post* legalitatea deciziei autorității.

Consolidarea legalității deciziilor luate de autoritățile publice poate avea ca rezultat creșterea încrederii și a sentimentului de siguranță al cetățenilor față de acestea, facilitând astfel obținerea cooperării și a conformării din partea publicului. După cum se explică în orientările ICO și ale Institutului Alan Turing, acest lucru este valabil în special în contextul ADM, unde „cu cât indivizii au mai multe informații despre modelul de IA care ia decizii în legătură cu ei, cu atât sunt mai încrezători în ceea ce privește interacțiunea cu aceste sisteme⁵⁵⁾.

7. LEGĂTURA DINTRE CELE DOUĂ SETURI DE NORME

Aceste reguli de *common law* nu sunt doar relevante în sine, ci există și două moduri în care ele se leagă de legislația discutată mai sus. În primul rând, dreptul administrativ s-a dezvoltat în mod special pentru a

⁴⁹⁾ *R v Secretary of State for the Environment ex p Hammersmith and Fulham LBC* [1991] 1 AC 521, 561 (Lord Donaldson).

⁵⁰⁾ A se vedea, e.g., *Moyna v Secretary of State for Work and Pensions* [2003] UKHL 44, [2003] 1 WLR 1929; *Pendragon Plc v Revenue and Customs Commissioners* [2015] UKSC 37, [2015] 1 WLR 2838, [49]–[51]; *R v Monopolies and Mergers Commission ex p South Yorkshire Transport* [1993] 1 WLR 23 (HL).

⁵¹⁾ A se vedea, e.g., *Carltona v Commissioners of Works* [1943] 2 All ER 560; *R (CCWMP) v Birmingham Justices* [2002] EWHC 1087, [2002] Crim LR 37; *R v Inhabitants of Leake* (1833) 5 B & Ad 469; *British Oxygen v Minister of Technology* [1971] AC 610.

⁵²⁾ A se vedea, e.g.: *Dimes v Grand Junction Canal Co* (1852) 3 HLC 759; *R v Amber Valley DC, ex p Jackson* [1985] 1 WLR 298; *Ex p Kirkstall Valley* [1996] 3 All ER 304; *R v UFC, ex p Institute of Dental Surgery* [1994] 1 WLR 242; *M Elliott*, ‘Has the Common Law Duty to Give Reasons Come of Age Yet?’ [2011] PL 56; *Secretary of State for the Home Department v AF* (No 3) [2009] UKHL 28, [2010] 2 AC 269, ulterior *A v United Kingdom* (2009) 49 EHRR 625 (GC) și *R (Bourgass) v Secretary of State for Justice* [2015] UKSC 54, [2016] AC 384.

⁵³⁾ *R v Governor of Brixton Prison ex p Soblen* [1963] 2 QB 243, 302; *Bancoult* [2013] EWHC 1502, [2014] Env LR 2; *R v Rochdale MBC ex p Cromer Ring Mill* [1982] 3 All RR 761; *R v Westminster Corporation v LNWR* [1905] AC 426; *Tesco Stores v Secretary of State for the Environment* [1995] 1 WLR 759.

⁵⁴⁾ *Associated Provincial Picture Houses v Wednesbury Corporation* [1948] 1 KB 223 (CA); *Ex p Barry* [1997] AC 584; *Tandy* [1998] AC 714; *R (Quila) v Home Sec* [2011] UKSC 45, [2012] 1 AC 621; *R (Wandsworth v Schools Adjudicator)* [2003] EWHC 2969, [2004] ELR 274; *R (Law Society v Legal Services Commission)* [2010] EWHC 2550, [2011] ACD 16; *A v Home Secretary* [2004] UKHL 56, [2005] 2 AC 68.

⁵⁵⁾ *Supra* nota 15, 57.

controla procesele decizionale, ceea ce îl face un cadru ideal pentru a găsi definiții ale unor expresii precum „măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate” [articolul 22 (2) (b) din GDPR] sau „informații semnificative privind logica implicată” [articolul 13 (2) (f) din GDPR]. De fapt, uneori acest rol este impus în mod explicit de legislație. De exemplu, GDPR face frecvent trimitere la conceptul, bine cunoscut în dreptul administrativ, de „proporționalitate”, sugerând, printre altele, că prelucrarea datelor sensibile în scopuri de interes public major, arhivare, cercetare științifică sau istorică trebuie să fie „proporțională cu scopul urmărit⁵⁶⁾”.

În al doilea rând, persoanele afectate de o anumită decizie bazată pe prelucrare automată (ADM) se vor adresa inițial autorității competente – ICO (Information Commissioner’s Office) –, iar decizia luată de ICO poate fi contestată în fața Camerei Generale de Reglementare a Tribunalului de primă instanță și, în ultimă instanță, prin acțiune în contencios administrativ (*judicial review*)⁵⁷⁾.

Prin urmare, este foarte probabil ca dreptul comun al controlului jurisdicțional (*judicial review*) să joace un rol important atât prin intermediul legislației relevante, cât și complementar față de aceasta – fie prin fundamentarea controlului de legalitate și a recursurilor privind deciziile ICO, fie prin controlul direct al utilizării în dreptul public a deciziilor automatizate (ADM).

Întrebarea firească este cum adaptăm motivele de nelegalitate aplicabile în contenciosul administrativ pentru a asigura dezvoltarea optimă a deciziilor automatizate (ADM).

8. CONTROLUL ÎN CONTENCIOS ADMINISTRATIV ȘI ADM

A. RESPECTAREA PROCEDURII

39

Deși în discuțiile non-juridice despre deciziile automatizate (ADM) se face adesea referire la ideea de „bias” (prejudecată), pentru juriștii specializați în drept public este evident că acest temei, în sensul său tehnic din dreptul administrativ, este puțin probabil să fie util, având în vedere concentrarea sa foarte specifică asupra intereselor personale directe⁵⁸⁾.

Totuși, dreptul administrativ a urmărit adesea, în trecut, să controleze nu doar echitatea unui sistem decizional odată ce acesta a fost ales de autoritatea publică, ci chiar modul în care a fost ales acel sistem de luare a deciziilor în sine⁵⁹⁾. Dacă această tendință continuă, este foarte probabil ca, în viitor, instanțele să fie chemate să analizeze nu doar alegerea utilizării ADM, ci și amploarea aplicării sale și, mai ales, alegerea unei anumite forme de ADM în detrimentul alteia.

⁵⁶⁾ GDPR, art. 9 (2) (g) and (j). A se vedea, de asemenea, *e.g.*, art 14 (5) (b), art 19.

⁵⁷⁾ Împotriva deciziilor emise de Oficiul Comisarului pentru Informații (ICO) se formulează o acțiune la First-tier Tribunal (General Regulatory Chamber). Totuși, art. 163 alin. (3) din Legea privind protecția datelor din 2018 (DPA 2018) sugerează că motivele de drept pot include temeiuri similare celor utilizate în contenciosul administrativ (*judicial review*). Ulterior, calea de atac continuă, în ordine ierarhică, prin Upper Tribunal, ajungând — deși rareori — la **High Court King’s Bench Division** — unde este soluționată acțiunea clasică de contencios administrativ. A se vedea, de exemplu: *Information Commissioner’s Office, ICO Disclosure Log – Response IRQ0686975* (2017), disponibil la: <https://ico.org.uk/media/about-the-ico/disclosure-log/2172601/irq0686975-response.pdf>.

⁵⁸⁾ *Dimes* (n 52).

⁵⁹⁾ A se vedea, de exemplu, cerința ca un tribunal să fie independent și imparțial, conform articolului 6 din CEDO, și nu pur și simplu justificabil în sine ca metodă de luare a deciziilor politice: *Amber Valley* (nota 52); *Kirkstall Valley* (nota 52).



ICO (Autoritatea britanică pentru protecția datelor) a prezentat în mod util o serie de forme diferite de ADM, indicând, de exemplu, în ce măsură acestea sunt explicabile⁶⁰⁾, adăugând și recomandarea că „[m]odelul ales trebuie să aibă un nivel de interpretabilitate adecvat pentru cazul de utilizare și pentru impactul pe care îl va avea asupra destinatarului deciziei”⁶¹⁾.

Prin urmare, nu este deloc de neconceput ca instanțele să fie chemate, în viitor, să analizeze asemenea alegeri pentru a stabili dacă acestea constituie o procedură echitabilă.

În acest sens, merită menționat cazul *Ivory Coast*⁶²⁾, discutat mai jos, care a analizat doctrina echității ca factor contrabalansator în determinarea gradului de rigiditate cu care o politică putea fi aplicată în acel caz.

Și în acest context, instanțele vor trebui să dezvolte atât competența tehnică necesară pentru a înțelege diferențele dintre diversele sisteme de ADM, cât și un set justificabil de principii care să permită evaluarea adecvării fiecărui sistem în funcție de contextul concret.

Istoria dreptului administrativ arată că, în mod inevitabil, cu cât o procedură seamănă mai mult cu o procedură judiciară, cu atât este considerată mai echitabilă (mai ales având în vedere trimiterea din articolul 6 al CEDO la „instanțe independente și imparțiale”), însă această abordare este puțin probabil să fie suficient de nuanțată pentru a face altceva decât să respingă aplicarea ADM în întregime.

Dacă dorim atât să valorificăm potențialele beneficii ale acestor sisteme, cât și să ne asigurăm că ele sunt alese și aplicate în mod echitabil, dreptul public va trebui să dezvolte un mecanism mai avansat de corelare între sistemele potrivite și contextele în care acestea sunt aplicate.

Un temei strâns legat de controlul jurisdicțional privind corectitudinea procedurală, care va permite instanțelor să facă acest lucru, este dreptul referitor la transparență și motivare.

Se pare că acest aspect va contribui în mod semnificativ la interpretarea expresiei „informații semnificative privind logica implicată”, pe măsură ce instanțele vor începe să dea sens acestei prevederi, dar și prin posibilitatea de a aplica acest temei de control în mod autonom.

Două seturi de reguli abordează aceste aspecte: cele referitoare la obligația de a motiva o decizie (dacă există o asemenea obligație) după luarea deciziei⁶³⁾ și cele care stabilesc dreptul reclamantului de a fi informat cu privire la acuzațiile împotriva sa, în vederea asigurării unui proces echitabil⁶⁴⁾. Cele două sunt adesea corelate, în sensul că motivele oferite ulterior unei decizii sunt frecvent relevante pentru un eventual apel, moment în care ele capătă mai degrabă funcția de notificare/ înștiințare prealabilă.

Această corelare este susținută și de modul în care elementele menționate sunt tratate în ghidul emis de ICO, în care se precizează:

Este esențial ca persoanele să înțeleagă motivele care stau la baza rezultatului unei decizii automatizate sau al unei decizii umane asistate de un sistem de inteligență artificială. Dacă decizia nu a fost cea așteptată sau dorită, înțelegerea motivării permite evaluarea dacă raționamentul deciziei este defectuos. În cazul în care doresc să o conteste, cunoașterea motivelor le ajută să formuleze o argumentare coerentă în sprijinul contestației⁶⁵⁾.

⁶⁰⁾ *Supra* n 14.

⁶¹⁾ *Ibidem* 48.

⁶²⁾ *EK (Ivory Coast)* [2014] EWCA Civ 1517, [2015] Imm AR 367.

⁶³⁾ A se vedea, e.g., *UFC* (n 52); *Elliott* (n 52).

⁶⁴⁾ A se vedea, e.g., *AF* (N 3) (n 52), ulterior *A* (n 52).

⁶⁵⁾ *Supra* nota 14, 23.

Obligația de a notifica este consacrată în *common law* și chiar în contextul procedurilor cu informații clasificate (*closed material procedures* – *CMPs*) s-a stabilit că pârâtului trebuie adesea să i se comunice „esența” cazului declanșat împotriva sa⁶⁶⁾.

În cauza *Bourgass*⁶⁷⁾, Lord Reed a afirmat:

Dreptul unui deținut de a formula observații este, în mare parte, lipsit de valoare dacă nu cunoaște fondul cazului declanșat împotriva lui... Nu este necesară, de regulă, dezvăluirea probelor primare... [dar] este necesară o comunicare autentică și semnificativă a motivelor pentru care [s-a luat decizia]⁶⁸⁾.

Prin urmare, afirmațiile generale privind comportamentul deținutului sau gradul său de risc nu au fost considerate suficiente. Rezultă, astfel, că nu ar fi permis ca o autoritate publică să utilizeze un sistem ADM care operează într-un mod excesiv de opac („cutie neagră” – *black box*), într-un context în care legea impune în mod normal o prezentare minimală (*gisting*) a cazului (de exemplu, acolo unde este în joc libertatea persoanei)⁶⁹⁾.

Această concluzie este susținută și de hotărârea pronunțată în cauza *Houston Federation of Teachers v. Houston Independent School District (HISD)*⁷⁰⁾, care privea utilizarea de către HISD a punctajelor generate prin Educational Value-Added Assessment System (EVAAS) – un algoritm dezvoltat de o entitate privată.

Profesorii au argumentat că au fost privați de o modalitate semnificativă de a se asigura că punctajele lor fuseseră calculate corect, deși aceste punctaje puteau fi folosite pentru a le rezilia contractele din cauza rezultatelor nesatisfăcătoare. Ca răspuns la această acuzație, HISD a solicitat respingerea cererii printr-o hotărâre sumară (*summary judgment*), însă cererea a fost respinsă pe motiv că:

„Profesorii HISD nu dispun de un mecanism efectiv de a verifica corectitudinea calculului punctajelor EVAAS și, în consecință, sunt expuși în mod inechitabil riscului de a fi privați, din greșeală, de interese patrimoniale protejate constituțional în legătură cu locurile lor de muncă⁷¹⁾”.

Odată ce reclamanții au obținut judecarea fondului cauzei, acesta s-a soluționat și HISD a încetat să mai utilizeze punctajele EVAAS⁷²⁾.

În Franța, legislația a mers și mai departe, impunând utilizatorilor ADM să facă public codul sursă, iar Legea Republicii Digitale impune publicarea oricărui cod sursă utilizat de guvern. Într-un sistem bazat pe norme, acest lucru este probabil foarte util, în timp ce, într-un context de învățare automată, ar putea fi mult mai puțin util⁷³⁾.

În concluzie, pare probabil ca, în viitor, să se introducă acțiuni în justiție pentru a contesta atât nivelul de transparență al unui anumit sistem ADM, cât și chestiunea strâns legată de alegerea acelui sistem în detrimentul altuia, care ar fi putut fi mai transparent. Prin urmare, instanțele vor trebui să continue lucrările

⁶⁶⁾ *Ibidem*.

⁶⁷⁾ *Bourgass* (n 52).

⁶⁸⁾ *Ibidem* 100.

⁶⁹⁾ Oswald (n 2) textul de la n 7. Este adevărat că în cauza din SUA Statul Wisconsin v Loomis 2016 WI 68,371 Wis 2d 235, 881 NW 2d 749 acest motiv a avut mai puțin succes. Dar acesta nu a fost un motiv necesar de decizie în cazul Loomis, deoarece instanța a dat dreptate reclamantului din alte motive (a se vedea detalii *infra*, textul de la n 108).

⁷⁰⁾ *Houston Federation of Teachers v Houston Independent School District* 251 F Supp 3d 1168 (SD Tex 2017).

⁷¹⁾ *Ibidem*.

⁷²⁾ *M Cummings*, ‘Federal Lawsuit Settled between Houston’s Teacher Union and HISD’, Houston Public Media (Houston, 10 October 2017) <www.houstonpublicmedia.org/articles/news/2017/10/10/241724/federal-lawsuit-settled-between-houstons-teacher-union-and-hisd/>.

⁷³⁾ Cu privire la limitele obligației de transparență, a se vedea *L. Edwards, M. Veale*, ‘Slave to the Algorithm? Why a “Right to an Explanation” Is Probably Not the Remedy You Are Looking For’ (2016) *Duke Law & Technology Review* 18.

pe care le-au început în contextul CMP⁷⁴⁾, printre altele, pentru a stabili cu precizie câtă transparență este necesară în diferite contexte și când, dacă este cazul, după cum a afirmat instanța din cauza *Houston*, „considerentele legate de costuri” ar trebui să prevaleze asupra „acurateței” (ori, s-ar putea adăuga, asupra oricăruia dintre ceilalți indicatori detaliați mai sus).

B. JURISDICȚIE (COMPETENȚĂ)

După cum se știe, regulile referitoare la competență (jurisdicție) impun ca autoritatea publică să interpreteze corect orice condiție prealabilă pentru exercitarea puterii sale. Astfel, dacă legea prevede că „dacă [are loc evenimentul X], autoritatea publică poate sau trebuie să facă [lucrul Y]”, autoritatea publică trebuie să înceapă prin a evalua corect dacă evenimentul X a avut sau nu loc în realitate. Dar mai este valabil acest principiu dacă existența unei astfel de condiții prealabile X este determinată de un sistem ADM (automat de luare a deciziilor), și nu de un decident uman?

Parțial, răspunsul depinde de natura sistemului. În timp ce sistemele ADM bazate pe învățare automată (*machine learning*) pot funcționa ca o „cutie neagră”⁷⁵⁾, sistemele bazate pe reguli nu funcționează astfel⁷⁶⁾ și, în cazul unui sistem bazat pe reguli, va fi mai întâi necesar să se atribuie sistemului un set de criterii care să fie utilizate pentru a decide dacă a fost sau nu îndeplinită condiția X. Acest proces va necesita în continuare judecata umană, care probabil va continua să impună respect într-un mod tradițional. Cu toate acestea, deși suntem obișnuiți cu posibilitatea ca ADM să facă procesul decizional mai puțin transparent, procesul de transmitere a acestor criterii către o mașină printr-un sistem bazat pe reguli ar putea, de fapt, să îl facă mai transparent.

42

Acest proces de specificare a criteriilor relevante pentru un sistem bazat pe reguli poate însemna, prin urmare, că există posibilitatea ca instanța să aibă mai multe elemente de analizat decât ar avea în cazul unui factor de decizie uman. Același lucru se poate aplica și transparenței variabilelor de intrare într-un model de regresie. De fapt, chiar și atunci când se utilizează un sistem ML, dacă acesta este un sistem bazat pe „învățare supravegheată”⁷⁷⁾, i se va furniza un set de date etichetate, iar aceste alegeri de etichetare pot fi, de asemenea, mai transparente și, prin urmare, deschise revizuirii.

Prin urmare, rezultatul global ar putea fi o reducere a respectului, întrucât ceea ce este în prezent decis în mod general, implicit și chiar inconștient de către oameni într-un domeniu general de apreciere se transformă într-o serie de decizii tehnice detaliate și explicite care, prin însăși transparența lor, sunt mai deschise controlului judiciar. Chiar și așa, acest lucru pare a fi o parte inevitabilă a procesului de automatizare și un preț necesar de plătit.

Cu toate acestea, în cazul în care ADM utilizează ML, apar o serie de întrebări suplimentare. Decizia din cauza *South Yorkshire Transport*⁷⁸⁾ sugerează că o modalitate de a asigura o delimitare între calea de atac (recurs) și controlul de legalitate pe fond este ca instanța să plaseze definiția unei condiții X în limite rezonabile și să lase apoi la latitudinea autorității publice luarea unei decizii în cadrul acestor limite. Dar care

⁷⁴⁾ A se vedea, e.g., diferența între *AF (No 3) (n 52)* și *Home Office v Tariq* [2011] UKSC 35, [2012] 1 AC 452.

⁷⁵⁾ *Supra*, nota 4.

⁷⁶⁾ A se vedea *supra*, nota 15.

⁷⁷⁾ Spre deosebire de învățarea nesupravegheată, în cadrul căreia sistemului i se oferă date neetichetate, pe care le analizează identificând în mod autonom trăsături și tipare.

⁷⁸⁾ *Supra* n 50.

dintre diferiții indicatori enumerați mai sus ar trebui să aibă prioritate în evaluarea performanței sistemului pentru a decide dacă acesta a fost „rezonabil” în cauza *South Yorkshire*?

Va fi o decizie luată de un sistem care funcționează bine în ceea ce privește sensibilitatea? Precizia? Acuratețea? Ce factori ar trebui să conducă la alegerea unuia dintre acești indicatori în detrimentul altuia? Și aceștia sunt doar câțiva dintre indicatorii potențial relevanți⁷⁹⁾. Am văzut deja că, în cauza *Bridges*⁸⁰⁾, Curtea de Apel a considerat că evaluarea acurateței și în special a părtinirii (care ar putea fi considerată ca o acuratețe inegală între subgrupuri) efectuată de SWP era inadecvată în temeiul PSED. Pare a fi doar o chestiune de timp până când vor fi contestați și indicatorii utilizați pentru a evalua dacă un sistem ADM a luat o decizie corectă cu privire la îndeplinirea sau neîndeplinirea unei condiții X dintr-o lege, în scopul stabilirii competenței autorității publice.

Acestea sunt probleme noi, pe care legislația nu a fost nevoită să le abordeze până în prezent, dar pare de neevitat ca, dacă autoritățile publice vor continua să utilizeze ADM, astfel de chestiuni să fie supuse, mai devreme sau mai târziu, controlului jurisdicțional. Și când se va întâmpla acest lucru, așa cum a demonstrat cauza *Bridges*, va fi esențial ca instanțele să aibă o înțelegere detaliată a aspectelor tehnice, precum și a doctrinei juridice, pentru a putea răspunde la aceste întrebări într-un mod care să ofere orientări utile pentru cei care operează sistemele, precum și protecția necesară pentru cei care fac obiectul acestora.

Nu există, desigur, niciun motiv intrinsec pentru care ADM bazate pe ML ar trebui să fie mai puțin precise decât oamenii pe care îi înlocuiesc; dimpotrivă⁸¹⁾. Cu toate acestea, există două motive pentru care ar trebui să fim mai precauți cu privire la eventualele erori pe care un astfel de sistem le-ar putea comite.

Primul motiv decurge din modul în care sunt create astfel de sisteme, astfel cum a fost identificat în cauza *Bridges*. Este evident că este foarte probabil ca factorii de decizie umani să aibă prejudecăți implicite care duc la crearea unor cercuri vicioase. Dar, ceea ce este esențial, acest lucru nu este intenționat. Factorii de decizie umani sunt, în principiu, instruiți și pregătiți să ia decizii obiective, prejudecățile lor constituind un impediment care apare accidental.

Dificultatea sistemelor ADM constă însă în faptul că acestea sunt instruite pe baza datelor existente, ceea ce face ca orice prejudecată sau inegalitate socială care există în prezent în lume ca urmare a acestor decizii umane părtinitoare să fie în mod explicit încorporată în crearea lor. Prejudecățile din aceste date, spre deosebire de o serie de principii obiective, sunt cele pe care sistemele sunt instruite în mod specific să le reproducă. Acest lucru nu înseamnă neapărat că ele vor ajunge să fie „mai” părtinitoare decât factorii de decizie umani, dar înseamnă (i) că certitudinea noastră că vor apărea rezultate părtinitoare este chiar mai mare decât în cazul factorilor de decizie umani; și (ii) că, deși pot și trebuie, desigur, să existe obligații impuse factorilor de decizie umani de a urma cursuri de formare pentru a încerca să se debaraseze de prejudecățile lor, inconștiente sau conștiente, știm mult mai puțin despre amploarea acestor prejudecăți umane sau despre succesul probabil al metodelor care ar putea fi utilizate pentru a le elimina.

Pe de altă parte, în cazul unui sistem ADM, putem măsura cu precizie această prejudecată și putem evalua direct succesul sau eșecul încercărilor noastre de a o evita⁸²⁾. Iar faptul că putem face aceste lucruri sporește obligația care ne revine în acest sens.

⁷⁹⁾ A se vedea și F-score: media dintre precizie și rata de regăsire (*recall*).

⁸⁰⁾ *Supra* n 41.

⁸¹⁾ A se vedea *supra*, e.g., n 23.

⁸²⁾ A se vedea, e.g.: N. Mehrabi și alții, ‘A Survey on Bias and Fairness in Machine Learning’ ArXiv Research Paper (arXiv:1908.09635v2 [cs.LG] 2019) <<https://arxiv.org/abs/1908.09635>>; D. Pedreshi, S. Ruggieri, F. Turini, ‘Discrimination-Aware Data Mining’ (Proceedings of the 14th Association for Computer Machinery SIGKDD International Conference on Knowledge Discovery and Data Mining,

În al doilea rând, există și îngrijorarea că, dacă un astfel de sistem are într-adevăr un defect, impactul său va fi resimțit pe scară largă. După cum a explicat Institutul AI Now de la Universitatea din New York, un sistem ADM defectuos poate fi utilizat la o scară mult mai mare decât deciziile oricărui om. Chiar dacă sistemul ADM generează un procent mai mic de erori (decizii greșite), va lua mult mai multe decizii în total și, prin urmare, vor fi afectate mai multe persoane⁸³⁾. Și, în orice caz, faptul că într-un sistem ADM pot exista chiar mai puține erori (dar mai semnificative) înseamnă că responsabilitatea de a le identifica și corecta este mai mare.

În plus, în special, dar nu exclusiv, în cazul învățării nesupravegheate, un sistem ML va determina, pe baza propriilor criterii, momentul în care o anumită condiție X dintr-un act normativ a fost îndeplinită. Acest lucru va ridica, de asemenea, problema factorilor pe care i-a luat în considerare pentru a ajunge la această concluzie, o chestiune relevantă pentru un alt motiv de nelegalitate în contencios care se referă exact la această chestiune.

C. LUAREA ÎN CONSIDERARE A FACTORILOR RELEVANȚI

După cum reiese din unele citate din secțiunea de mai sus privind motivarea, unul dintre motivele principale pentru care transparența raționamentului este esențială este faptul că astfel se pot contesta factorii care au fost avuți în vedere de către factorul de decizie în luarea deciziei⁸⁴⁾.

Acest lucru va garanta că factorii de decizie au acționat în mod corespunzător⁸⁵⁾ sau pe baza unor considerente relevante⁸⁶⁾, asigurându-se totodată că au luat în considerare toate elementele relevante. Ponderea care trebuie acordată considerentelor revine ulterior factorului decizional⁸⁷⁾.

44

Este evident că acest motiv de nelegalitate poate fi foarte relevant pentru controlul ADM, în special în contextul unei potențiale «părtiniri» sau, mai precis, al discriminării în astfel de sisteme. Acest lucru este cu atât mai adevărat cu cât însăși cauza *Wednesbury* a dat exemplul bazării pe o caracteristică inadmisibilă și discriminatorie (părul roșu) ca fiind ceva interzis⁸⁸⁾.

Există două etape potențiale în care este probabil să apară această chestiune a relevanței, în primul rând atunci când un factor de decizie uman trebuie să stabilească câtă relevanță să acorde rezultatului unei determinări efectuate de un sistem ADM și, în al doilea rând, deoarece sistemul ADM însuși va fi luat în considerare diverși factori în elaborarea unei determinări, fie pentru a o transmite unui om, fie pentru a o executa pe cont propriu. Acest lucru demonstrează că legea are nevoie de o definiție clară, precisă și certă a ceea ce este relevant și a ceea ce nu este relevant în diferite circumstanțe. Cu toate acestea, suntem încă departe de acest obiectiv. Astfel, de exemplu, uneori este posibil să se ia în considerare costul financiar ca

August 2008); C. Dwork și alții, 'Fairness through Awareness' (Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, January 2012); M. Hardt, E. Price, N. Srebro, 'Equality of Opportunity in Supervised Learning' (Proceedings of the 30th International Conference on Neural Information Processing Systems, December 2016).

⁸³⁾ M. Whittaker și alții, 'AI Now Report 2018' (AI Now Institute 2018) 18 <https://ainowinstitute.org/AI_Now_2018_Report.pdf>.

⁸⁴⁾ A se vedea, e.g., *Governor of Brixton Prison* (n 53) 302; *Bancoult* (n 53).

⁸⁵⁾ *R v Westminster Corporation v LNWR* (n 53).

⁸⁶⁾ *Rochdale MBC* (n 53).

⁸⁷⁾ *Tesco* (n 53).

⁸⁸⁾ *Associated Provincial Picture Houses* (n 54).

factor relevant în luarea unei decizii⁸⁹⁾, în timp ce, în alte cazuri, nu este posibil⁹⁰⁾, dar nu este imediat evident când sau de ce.

Dacă legea nu este în prezent în măsură să clarifice un factor relativ familiar cum ar fi costul economic, se pare că va întâmpina și mai multe provocări în ceea ce privește ADM.

Dacă, de exemplu, un factor de decizie uman ia în considerare rezultatul unui sistem ADM, atunci relevanța acestui rezultat poate depinde de calitatea sa, în special în cazul sistemelor ML. Dar, așa cum s-a detaliat mai sus, această calitate poate fi măsurată prin intermediul unei varietăți de indicatori diferiți, care nu toți indică aceeași direcție. Aici ne confruntăm cu aceeași provocare ca și înainte: rezultatul unui ADM trebuie considerat relevant atunci când este precis?

Are sensibilitate? Specificitate? Sau alt indicator? Din nou, pare probabil că vor fi potrivite diferite metode de măsurare și că acestea vor face sistemul mai mult sau mai puțin potrivit în diferite contexte⁹¹⁾. Prin urmare, dreptul public are de lucru pentru a stabili care dintre aceste metode de măsurare ar trebui să se aplice în fiecare caz.

În schimb, în prezent, odată ce un factor este considerat relevant, ponderea exactă care trebuie acordată acelui factor este la latitudinea factorului de decizie⁹²⁾.

Cu toate acestea, în contextul PSED, putem deja observa că acest lucru nu este valabil pentru unele considerente legate de egalitatea anumitor categorii protejate.

Și nu este imposibil să ne imaginăm că am putea dori să mergem mai departe în *common law*. Dacă, de exemplu, este evident că un sistem ADM are un efect deosebit de problematic în raport cu o anumită categorie de persoane, atunci, chiar dacă acestea nu sunt protejate de PSED, am putea foarte bine să ne întrebăm dacă acesta este un element relevant pe care am dori ca factorul decizional să îl ia în considerare în mod activ la evaluarea performanței și, prin urmare, a relevanței sistemului ADM. Și am putea dori să facem acest lucru cu mai puțină deferență față de factorii de decizie decât cea de care beneficiază aceștia în temeiul doctrinei *Tesco*⁹³⁾.

În ceea ce privește sistemul ADM în sine, totul depinde, din nou, de tipul exact al sistemului. După cum s-a menționat mai sus în legătură cu competența jurisdicțională⁹⁴⁾, pentru anumite tipuri de sisteme, în anumite moduri, acești factori ar putea fi de fapt mai transparenți în contextul ADM decât în cazul luării deciziilor de către oameni, deoarece vor fi rezultatul unor alegeri conștiente în formarea sistemului, etichetarea datelor utilizate pentru regresie, stabilirea regulilor pentru un sistem bazat pe reguli etc.

Cu toate acestea, în cazul în care se utilizează ML, acesta se bazează pe inferențe statistice, nu pe raționament, astfel încât, atunci când un astfel de sistem utilizează un factor anume, acesta nu identifică factorul respectiv ca fiind relevant pentru decizia pe care o ia în același mod în care ar face-o un om, ci recunoaște pur și simplu că, din punct de vedere statistic, factorul respectiv este adesea corelat cu rezultatul relevant.

De exemplu, o companie de marketing a putut utiliza datele de profil YouGov pentru a stabili cele mai populare 10 mărci preferate de „Brexiteri” și de „Remainers” în cadrul referendumului privind Brexit din 2016⁹⁵⁾.

⁸⁹⁾ Barry (n 54).

⁹⁰⁾ Tandy (n 54).

⁹¹⁾ *Supra*, text între nn 75 și 78.

⁹²⁾ *Tesco* (n 53).

⁹³⁾ *Ibidem*.

⁹⁴⁾ *Supra*, textul de la n 75.

⁹⁵⁾ E. James, „The Top 10 Brands Favoured by Remainers and Brexiters’ Campaign (1 August 2016) <www.campaignlive.co.uk/article/top-10-brands-favoured-remainers-brexiters/1403991>.

Este dificil de imaginat că poziția adoptată în acest referendum ar putea fi un factor relevant pentru o decizie de drept administrativ, dar să presupunem pentru o clipă că ar putea fi. Dacă s-ar crea un sistem ADM pentru a lua această decizie ipotetică și acesta ar ajunge la același calcul, și anume că HP Sauce era marca preferată a susținătorilor Brexitului și, prin urmare, achiziționarea acestei mărci era strâns corelată cu votul pentru Brexit, ar fi permis ca acel sistem ADM să utilizeze achiziționarea HP Sauce ca factor relevant în sine? Din perspectiva umană, în care sperăm că relevanța considerentelor noastre se bazează pe contribuția lor cauzală la rezultatul dorit, o astfel de abordare ar părea inadmisibilă, dar dacă ne-am concentra doar pe acuratețea sistemului, un sistem ADM ar putea foarte bine să depășească un factor de decizie uman, așa cum se poate întâmpla în alte contexte. Este clar, așadar, că în abordarea acestui tip de chestiuni, dreptul (i)relevanței va trebui să fie considerabil mai sofisticat decât este în prezent.

Un al doilea aspect este că, indiferent de tipul precis de sistem utilizat, va fi important să se stabilească că persoanele potrivite sunt responsabile de luarea deciziilor relevante. Pe de o parte, alegerile făcute în proiectarea sistemului ar putea fi considerate pur tehnice și adecvate pentru cei care proiectează și produc sistemul, atât timp cât rezultatul sistemului este satisfăcător în raport cu indicatorii relevanți menționați mai sus. Cei care iau aceste decizii „tehnice” vor fi, după toate probabilitățile, ca în cazul COMPAS, EVAAC și AFR Locate, companii private. Dar, dimpotrivă, așa cum demonstrează decizia din cauza *Bridges*⁹⁶⁾, atribuțiile autorităților publice nu se extind doar la rezultatele acestor sisteme, ci și la datele care intră în ele. Prin urmare, este esențial ca deciziile politice reale privind factorii relevanți să fie luate de autoritățile publice și ca aceste autorități să fie trase la răspundere pentru aceste alegeri în mod obișnuit. Dacă acest lucru înseamnă că autoritățile publice trebuie să meargă mai departe „în amonte” în ancheta lor sau chiar în proiectarea sistemelor înainte de achiziționare, ca în cazul *Bridges*, și dacă acest lucru înseamnă că deciziile lor în acest domeniu sunt supuse unui grad de deferență puțin mai redus din partea instanțelor, acest lucru pare un preț necesar de plătit, având în vedere posibila pierdere a răspunderii care ar putea rezulta în caz contrar. Acest lucru ne conduce, la rândul său, la luarea în considerare a unui alt motiv relevant de control.

D. LIMITAREA PUTERII DISCREȚIONARE ȘI PRINCIPIUL NON-DELEGĂRII

Este bine cunoscut faptul că o autoritate publică nu poate delega mai departe pe scara ierarhică competențele care i-au fost deja delegate. Cu toate acestea, sarcinile numeroase și variate care revin autorităților publice – în special funcționarilor de rang înalt – fac imposibilă evitarea totală a delegării⁹⁷⁾.

În mod similar, instanțele au recunoscut utilitatea și necesitatea politicilor publice din perspectiva coerenței, cât și a eficienței, iar instanțele au urmărit să atingă un echilibru – așa cum s-a observat, de exemplu, în contextul din cauza *Ivory Coast*⁹⁸⁾ –, subliniind că autoritățile publice nu trebuie să „își limiteze puterea discreționară” prin angajamente excesiv de rigide, fie prin contract⁹⁹⁾, fie prin politici administrative inflexibile¹⁰⁰⁾. Acest principiu a determinat o gamă variată de reacții jurisprudențiale. Deși poziția tradițională, exemplificată prin cauza *British Oxygen*¹⁰¹⁾, este aceea că factorii de decizie nu trebuie să fie surzi la alte

⁹⁶⁾ *Supra* n 41. A se vedea și Oswald (n 2).

⁹⁷⁾ A se vedea, *e.g.*, *Carltona* (n 51); *CCWMP* (n 51).

⁹⁸⁾ A se vedea, de exemplu, contrastul dintre opiniile exprimate de judecătorii Sales LJ și Floyd LJ în cauza *Ivory Coast* (nota 66) și a se remarca încercarea explicită a judecătorului Sales LJ de a realiza un echilibru, la paragraful 40. Îi mulțumesc lui Jack Beatson pentru discuția purtată pe marginea acestui aspect.

⁹⁹⁾ *Inhabitants of Leake* (n 51).

¹⁰⁰⁾ *British Oxygen* (n 51).

¹⁰¹⁾ *Ibidem*.

considerente relevante, în unele spețe instanțele au cerut ca politica să joace un rol chiar mai redus¹⁰²⁾, în timp ce, în altele, inclusiv în contexte strict umane de luare a deciziei, s-a permis aplicarea aproape automată a respectivei politici¹⁰³⁾.

Aceste motive de control în contencios au implicații semnificative pentru utilizarea deciziilor automatizate (ADM) de către autoritățile publice, indiferent de tehnologia utilizată.

În primul rând, este esențial – așa cum s-a subliniat și anterior – ca furnizarea sistemului ADM de către o entitate privată să nu elimine și nici să înlocuiască responsabilitatea autorității publice. Acest principiu a fost consfințit în mod clar de Curtea de Apel în cauza *Bridges*¹⁰⁴⁾.

În al doilea rând, aceste fundamente indică faptul că va fi dificil pentru autoritățile publice să justifice o dependență exclusivă de algoritmi, în sensul în care factorul uman ar urma recomandarea sistemului, fără o reflecție sau analiză suplimentară¹⁰⁵⁾. O astfel de dependență exclusivă ar putea fi permisă doar printr-o reglementare expresă în legislația primară – precum cea prevăzută la articolul 49 din Legea privind protecția datelor din 2018 (DPA 2018) sau la articolul 22 lit. (b) din GDPR – dar chiar și în acest caz, legislația ar trebui să includă „măsuri adecvate pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate”. Această cerință legislativă poate presupune aplicarea doctrinelor referitoare la interdicția de a limita puterea discreționară și la non-delegare.

Chiar și în prezența unui element uman în procesul decizional, acesta ar putea să nu fie suficient. În cauza *Bridges*¹⁰⁶⁾, Curtea de Apel nu a considerat că existența unei „plase de siguranță umane” reprezintă un minim necesar. De fapt, instanța nu a fost convinsă în privința impactului real al implicării umane. Deși instanța inferioară (*Divisional Court*) a fost impresionată de faptul că o intervenție nu avea loc decât după decizia a două persoane – dintre care cel puțin una era un ofițer de poliție – de a acționa în urma unei potriviri pozitive generate de sistemul AFR (*Automated Facial Recognition*), Curtea de Apel a oferit trei motive pentru a respinge această abordare:

1. pentru că *Public Sector Equality Duty (PSED)* vizează procesul decizional, nu corectitudinea rezultatului într-un caz concret;
2. pentru că „ființele umane pot, de asemenea, să greșescă, mai ales în contextul identificării”;
3. pentru că, în orice caz, aspectul relevant era acela că „Poliția din Țara Galilor de Sud (SWP) nu a obținut informații proprii referitoare la posibilele prejudecăți (*bias-uri*) ale software-ului utilizat”.

Cu alte cuvinte, obligația *Public Sector Equality Duty (PSED)* care revenea Poliției din Țara Galilor de Sud (SWP) în această speță a fost, conform celor arătate anterior, aceea de a verifica dacă setul de date utilizat pentru antrenarea sistemului AFR (recunoaștere facială automată) era sau nu afectat de prejudecăți (*bias*). Această obligație cu caracter procedural nu putea fi îndeplinită și nici eludată prin simpla verificare umană a rezultatului generat de sistem, cu atât mai mult cu cât persoana umană implicată ar fi putut, la rândul său, să greșescă.

Această posibilitate de eroare conduce către a doua implicație a doctrinelor privind interdicția delegării și limitarea excesivă a puterii discreționare: chiar și în prezența unui factor uman, este esențial ca acesta să nu manifeste o încredere excesivă în tehnologie. Fenomene precum *automation bias* (tendința persoanelor

¹⁰²⁾ *Stringer* [1970] 1 WLR 1281.

¹⁰³⁾ A se vedea, e.g., *Ivory Coast* (n 62).

¹⁰⁴⁾ *Supra* n 41.

¹⁰⁵⁾ Cum se pare că s-a întâmplat în anumite cauze dezlegate definitiv pe care le vom detalia mai jos, e.g., *Loomis* (n 69). A se vedea și *Houston* (n 70).

¹⁰⁶⁾ *Supra* n 41.

fără expertiză tehnică de a acorda o credibilitate disproporționată informațiilor furnizate de tehnologie, chiar și atunci când alte surse oferă date contradictorii) și *automation complacency* (reducerea vigilenței în monitorizarea tehnologiei, pe fondul unei suspiciuni mai scăzute față de erori și a unei încrederi sporite în acuratețea sistemului) sunt bine documentate în alte domenii¹⁰⁷). În acest sens, principiile de drept public privind non-delegarea și interdicția de limitare a puterii discreționare oferă un cadru conceptual valoros pentru a preveni astfel de tendințe periculoase.

Această abordare se regăsește și în decizia *Supreme Court of Wisconsin* în cauza *Loomis*¹⁰⁸), unde inculpatul fusese condamnat, printre altele, pe baza unui punctaj de risc generat de sistemul COMPAS – un instrument dezvoltat de compania privată Northpointe¹⁰⁹) –, utilizat pe scară largă în SUA pentru a evalua riscul de recidivă și alți factori criminogeni. Curtea a stabilit că „punctajele de risc generate de COMPAS nu pot fi utilizate ca factor determinant pentru a decide dacă un inculpat poate fi supravegheat în mod sigur și eficient în comunitate”¹¹⁰), nici pentru a stabili dacă acesta ar trebui încarcerat sau pentru a determina severitatea sentinței. Totodată, instanța a statuat că „o instanță trebuie să explice factorii care, alături de evaluarea COMPAS, susțin în mod independent sentința impusă”¹¹¹). Evaluarea COMPAS este doar unul dintre numeroșii factori care pot fi luați în considerare și cântăriți în procesul de individualizare a pedepsei”.

În mod similar, în jurisprudența engleză, legalitatea¹¹²) *sistemelor de alocare a resurselor* (*Resource Allocation Systems*¹¹³)) utilizate de consiliile locale pentru distribuirea beneficiilor destinate persoanelor cu dizabilități s-a sprijinit pe faptul că aceste sisteme reprezentau doar un punct de plecare și erau „suficient de flexibile” pentru a permite adaptarea deciziilor la circumstanțele individuale ale beneficiarilor.

Într-adevăr, există un pericol mai general ca utilizarea ADM să încurajeze depersonalizarea și rigiditatea politicilor¹¹⁴). La prima vedere, acest lucru poate părea contraintuitiv; la urma urmei, unul dintre obiectivele-cheie ale „big data” este de a dezvolta soluții mai precise și mai personalizate, nu mai puține. Astfel, de exemplu, suntem familiarizați cu ideea de marketing personalizat sau micro-targetat¹¹⁵) și de medicină de precizie¹¹⁶).

¹⁰⁷) ISMP Canada, ‘Understanding Human Over-reliance on Technology’ (2016) 16(5) ISMP Canada Safety Bulletin 1; K. Goddard, A. Roudsari, J.C. Wyatt, ‘Automation Bias: A Systematic Review of Frequency, Effect Mediators, and Mitigators’ (2012) 19 Journal of the American Medical Informatics Association 121; R. Parasuraman, D.H. Manzey, ‘Complacency and Bias in Human Use of Automation: An Attentional Integration’ (2010) 52 Human Factors 381. A se vedea, de asemenea: C. Knight, ‘Automated Decision-Making and Judicial Review’ (2020) 25 JR 21; Claimant’s statement of facts and grounds in Foxglove, ‘How We Got the Government to Scrap the Visa Streaming Algorithm – Some Key Legal Documents’ (4 August 2020) par. 53-8 <www.foxglove.org.uk/news/c6tv7i7om2jze5pxs409k3oo3dyel0>.

¹⁰⁸) *Supra* n 69.

¹⁰⁹) Northpointe, ‘Practitioners Guide to COMPAS’ (17 August 2012) <www.northpointeinc.com/files/technical_documents/FieldGuide2_081412.pdf>.

¹¹⁰) *Supra* n 69, par. 44 și 99.

¹¹¹) Se aplică același test ca în cauza *Stringer* (n 102).

¹¹²) Care, cel puțin în anumite situații, implică folosirea software-ului Quickheart – a se vedea *W* (n 6).

¹¹³) *R (Savva) v Royal Borough of Kensington and Chelsea* [2010] EWCA Civ 1209, [2011] PTSR 761; *KM v Cambridge* [2012] UKSC 23, [2012] 3 All ER 1218.

¹¹⁴) A se vedea, e.g., Lord Sales, ‘Algorithms, Artificial Intelligence and the Law’ (2020) 25 JR 46, [15].

¹¹⁵) A se vedea Q. André și alții, ‘Consumer Choice and Autonomy in the Age of Artificial Intelligence and Big Data’ (2018) 5 Customer Needs and Solutions 28.

¹¹⁶) A se vedea, e.g., M. Panahiazar și alții, ‘Empowering Personalized Medicine with Big Data and Semantic Web Technology: Promises, Challenges and Use Cases’ (Proceedings of the 14th Association for Computer Machinery SIGKDD International Conference on Knowledge Discovery and Data Mining, August 2008) <www.ncbi.nlm.nih.gov/pmc/articles/PMC4333680/>; V. Gligorijevic, N. Malod-Dognin, N. Przulj, ‘Integrative Methods for Analyzing Big Data in Precision Medicine’ (2016) 16 Proteomics 741.

S-a sugerat chiar că legislația ar trebui să se îndrepte într-o direcție similară pentru a personaliza norme precum standardul de neglijență¹¹⁷⁾.

Cu toate acestea, există unele diferențe fundamentale între aceste exemple. În cazul medicinei, după cum s-a menționat mai sus, deși datele pot fi utilizate pentru a identifica o terapie potențială, este mult mai puțin probabil ca terapia respectivă să fie aplicată unui anumit pacient fără o verificare suplimentară pentru a se asigura că pacientul sau boala acestuia are într-adevăr codul genetic relevant. Astfel, de exemplu, cercetările au stabilit că vemurafenibul funcționează numai în tratamentul pacienților cu cancer care au rezultat pozitiv la testul pentru mutația V600E BRAF.

Dar pacienții sunt testați individual pentru a se vedea dacă au sau nu această mutație înainte de a li se oferi un tratament cu acest medicament¹¹⁸⁾.

În schimb, în cazul marketingului țintit sau chiar al regimurilor juridice personalizate propuse, nu există o etapă de testare individualizată specifică fiecărui caz; odată ce un sistem prezice că o persoană va îndeplini un anumit criteriu, nu mai există teste suplimentare și este foarte posibil să nu fie posibilă testarea dacă acea persoană aparține într-adevăr acelei categorii. Astfel, deși la un anumit nivel regimurile „personalizate” par atractive, în afara medicinei ele sunt personalizate doar până la un anumit punct.

Prin urmare, este perfect posibil ca un sistem automatizat de luare a deciziilor în contextul executiv¹¹⁹⁾, care este individualizat la nivel macro, dar numai în această măsură limitată, să fie totuși mai puțin personalizat la nivel micro decât o decizie luată de un factor de decizie uman care aplică o regulă generală standard pe care o poate adapta dacă acest lucru este impus de situația particulară. În acest context, este interesant faptul că, în cazul rezultatelor examenelor de nivel A, un sistem automatizat bazat pe date agregate a fost în cele din urmă abandonat în favoarea evaluărilor individualizate ale profesorilor¹²⁰⁾. O altă distincție între utilizarea micro-țintirii în medicină (și a reclamelor micro-țintite) și utilizarea datelor în procesul decizional executiv al autorităților publice este capacitatea pacientului sau a reclamantului de a-și da consimțământul. Astfel, chiar și într-un context în care știința trebuie să funcționeze încă la un nivel mai macro, deoarece nu știm încă cine poate beneficia sau nu de un tratament, rămâne în continuare alegerea pacientului dacă acceptă o șansă redusă a unui rezultat foarte bun, în comparație cu șansa mai mare a unui tratament destul de toxic și posibil ineficient¹²¹⁾.

În schimb, așa cum s-a menționat la început, consimțământul nu poate funcționa cu adevărat în cazul luării deciziilor de către o autoritate publică¹²²⁾.

Rezultă că, dacă micro-targetarea nu este la fel de precisă ca luarea unei decizii individuale de la caz la caz, ea trebuie delimitată de individualizarea reală, iar această distincție trebuie păstrată de doctrina de drept administrativ împotriva limitării puterii discreționare.

Dacă nu este păstrată această doctrină, există riscul ca, odată ce un sistem ADM este pus în aplicare, acesta să atragă inevitabil factorii de decizie către capătul spectrului de revizuire din cauza *Coasta de Fildes*,

¹¹⁷⁾ O. Ben-Shahar, A. Porat, 'Personalizing Negligence Law' (2016) 91 NYU L Rev 628.

¹¹⁸⁾ Cancer Research UK, 'Vemurafenib (Zelboraf)' <www.cancerresearchuk.org/about-cancer/cancer-in-general/treatment/cancer-drugs/drugs/vemurafenib>.

¹¹⁹⁾ Adică în contexte de luare a deciziilor care nu țin de domeniul medical, de către funcționari care acționează în calitate de reprezentanți ai autorităților publice, și nu de către medici care își exercită profesia. A se vedea și S. Palmer, „Public, Private and the Human Rights Act 1998: An Ideological Divide” (2007) 66 CLJ 559.

¹²⁰⁾ S. Weale, H. Stewart, 'A-Level and GCSE Results in England to Be Based on Teacher Assessments in U-Turn' The Guardian (London, 17 August 2020) <www.theguardian.com/education/2020/aug/17/a-levels-gcse-results-england-based-teacher-assessments-government-u-turn>.

¹²¹⁾ Așa cum e cazul în anumite situații legate de medicamentele pentru cancerul la rinichi, cum e Avastin.

¹²²⁾ *Supra* textul de la n 27.

în care se acordă prioritate eficienței și rapidității sistemului automatizat și de rutină, chiar dacă acestea conduc la injustiție sau nedreptate în cazuri individuale¹²³⁾.

Și dacă am combina acest aspect cu argumentele prezentate mai sus, cei mai susceptibili de a suferi astfel de nedreptăți sunt și cei mai susceptibili de a se afla deja într-o situație dezavantajoasă. Acest lucru se datorează tocmai faptului că aceste dezavantaje existente sunt încorporate în sistem prin utilizarea datelor.

E. VERIFICĂRI DE FOND: CARACTER REZONABIL ȘI PROPORȚIONALITATE

Este, de asemenea, posibil ca ADM să fie contestate prin intermediul verificărilor de suprapunere din cauza *Wednesbury*¹²⁴⁾ – caracter nerezonabil și proporționalitate¹²⁵⁾.

Am văzut deja că proporționalitatea este prevăzută în mod expres în anumite contexte, cum ar fi tratarea datelor (sensibile) în temeiul articolului 9 din GDPR. Aceste motive pot fi din nou relevante în două etape diferite în legătură cu ADM: în primul rând, decizia de a utiliza un anumit sistem ADM; și, în al doilea rând, revizuirea rezultatelor unui astfel de sistem. Este bine cunoscut faptul că aspectul „necesității” proporționalității se referă, în esență, la întrebarea dacă s-a folosit un baros pentru a sparge o nucă.

Prin urmare, o întrebare-cheie în alegerea ADM va fi dacă ADM este un baros și dacă, de exemplu, luarea deciziilor folosind augmentarea nu ar fi mai potrivit decât ADM completă. Poate exista, de asemenea, o problemă de „echilibru echitabil”, care se referă la aspectul final al proporționalității. Acest lucru ar necesita o examinare a beneficiilor ADM în raport cu impactul și potențialele dezavantaje ale acestuia, cum ar fi potențiala lipsă de transparență sau efectul său potențial dăunător asupra grupurilor minoritare (chiar și în afara PSED). Orientările ICO par a fi deosebit de relevante în acest caz, afirmând că:

50

atunci când intenționați să utilizați IA pentru a lua decizii cu privire la persoane, trebuie să aveți în vedere:

(1) contextul în care veți face acest lucru;

(2) impactul potențial al deciziilor pe care le luați;

(3) ce ar trebui să știe o persoană despre o decizie, astfel încât să puteți alege un model de IA care poate fi explicat în mod adecvat

și

(4) prioritizarea furnizării tipurilor de explicații relevante¹²⁶⁾.

În ceea ce privește revizuirea rezultatelor unui sistem ADM, adecvarea în contextul proporționalității este relativ slabă; atât timp cât există „ceva” care leagă mijloacele utilizate de scopurile urmărite, măsura poate rezista contestării¹²⁷⁾. Cu toate acestea, în mod contraintuitiv, în ceea ce privește raționalitatea, adecvarea poate fi de fapt mai puternică, astfel încât, în cauza *Wandsworth*¹²⁸⁾, instanța a anulat o măsură pe motiv

¹²³⁾ *Supra* n 62. A se vedea, de asemenea, experiența din Houston (n 70) în textul de la n 74.

¹²⁴⁾ *Supra* n 88. *Nota traducătoare:* prin standardul de nerezonabilitate *Wednesbury*, definit de Lord Diplock, se înțelege că decizia este atât de irațională și de revoltătoare în sfidarea logicii elementare sau a standardelor morale acceptate, încât nicio persoană rezonabilă care și-ar fi pus în mod real problema nu ar fi luat o astfel de decizie.

¹²⁵⁾ A se vedea, e.g., *Bank Mellat v Her Majesty's Treasury* [2013] UKSC 39, [2014] AC 700.

¹²⁶⁾ *Supra* n 14, 41.

¹²⁷⁾ *Quila* (n 54). A se vedea, de asemenea, *R. Williams*, 'Structuring Substantive Review' [2017] PL 99.

¹²⁸⁾ *Wandsworth v Schools Adjudicator* (n 54).

că „nu era rațional capabilă” să atingă obiectivul relevant și deoarece legătura dintre mijloace și scopuri era „extrem de speculativă”.

În mod similar, în cauza *Law Society*¹²⁹⁾, măsura a fost respinsă deoarece s-a constatat că produce mai mult rău decât bine. Prin urmare, se pare că astfel de motive ar putea, de exemplu, să ofere o modalitate utilă de a contesta buclele de feedback dăunătoare¹³⁰⁾ în care sistemul creează de fapt chiar ceea ce ar trebui să depisteze.

Un exemplu ar fi cazul în care un sistem prezice recidiva, conducând la închisoare în loc de o pedeapsă neprivativă de libertate, când se știe că, de fapt, încarcerarea crește șansele de recidivă. Astfel de bucle sunt, în fond, „incapabile din punct de vedere rațional să ajute” și „înrautățesc lucrurile în loc să le îmbunătățească”. Este probabil ca aceste abordări mai puțin reverențioase să fie necesare pentru ca dreptul public să poată exercita controlul necesar în acest domeniu.

De asemenea, este de remarcat faptul că, dacă un ADM discriminează, acesta nu va fi, probabil, necesar din motive de proporționalitate. Dacă este inutil să se trateze un grup într-un mod atât de dezavantajos, cum poate fi necesar să se trateze astfel un alt grup?¹³¹⁾

Prin urmare, și în acest caz se pare că este necesar să se clarifice nu doar limitele exercitării controlului de fond¹³²⁾, ci și ca motivele să fie suficient de clare și precise pentru a putea fi aplicate în scopul de a ghida utilizarea optimă a ADM.

9. CONCLUZIE

Este incontestabil faptul că posibilitatea de a justifica deciziile administrative pe date, în loc de judecăți personale oferă un potențial considerabil în ceea ce privește acuratețea și obiectivitatea. Mai mult, capacitatea de a automatiza acest proces poate conduce la o luare a deciziilor mai coerentă, previzibilă și eficientă.

Cu toate acestea, după cum s-a evidențiat în această analiză, tranziția către sisteme de decizie automatizată (ADM) generează o serie de provocări — de la aspecte tehnice privind alegerea parametrilor adecvați pentru evaluarea acestor sisteme, la probleme legate de lipsa de transparență (*black boxes*), scalabilitatea erorilor și altele asemenea.

Pentru ca dreptul administrativ să furnizeze un cadru normativ adecvat care să permită utilizarea optimă a acestor sisteme, este necesară o rafinare și o sofisticare a instrumentelor sale doctrinare și jurisprudențiale. Dacă reușește acest lucru, dreptul administrativ nu doar că poate exercita un rol activ și valoros în controlul ADM, ci poate, de asemenea, sprijini activitatea *Information Commissioner's Office* (ICO) și poate contribui la interpretarea unor concepte-cheie din GDPR, precum „informațiile semnificative” sau „proporționalitatea”.

¹²⁹⁾ *Law Society v Legal Services Commission* (n 54).

¹³⁰⁾ Pentru detalii, a se vedea *Melham și Williams* (n 9).

¹³¹⁾ A se vedea, e.g., *A v Home Secretary* [2004] UKHL 56, [2005] 2 AC 68.

¹³²⁾ Pentru detalii, a se vedea *Williams* (n 127).

Având în vedere că unul dintre factorii determinanți pentru aplicarea dreptului administrativ este dezechilibrul de putere dintre autoritatea decidentă și indivizi¹³³⁾, iar în paralel observăm un proces de „extindere” a dreptului public dincolo de granițele sale tradiționale¹³⁴⁾, se conturează inclusiv posibilitatea ca acest domeniu juridic să joace un rol mai consistent în supravegherea și reglementarea utilizării ADM.

¹³³⁾ *R v Panel on Takeovers and Mergers, ex p Datafin* [1987] QB 815.

¹³⁴⁾ *Braganza v BP Shipping Ltd and another* [2015] UKSC 17, [2015] 1 WLR 1661.