European and Comparative Law of Digital Technologies

Marta Infantino
DISPES
University of Trieste
minfantino@units.it

Mandatory Readings

(1) Infantino and Bussani, ‘Rule by Metrics. Performance, Quantification, and the Law’, EJCL (2024)

(2) Future for Life Institute, ‘High-Level Summary of the AI Act’ (2024)

(3) Bradford, ‘Europe's Digital Constitution’ Va J Int’l L (2023)

(4) De Conca, ‘The present looks nothing like the Jetsons: Deceptive design in virtual assistants and the protection of the rights of users’ Computer L & Sec Rev (2023)

Optional Readings

(1) Barfield & Pagallo, Advanced Introduction to Law and Artificial Intelligence, EE, 2020

(2) Hildebrandt, Law for Computer Scientists and Other Folk, OUP, 2020

Sample Exam: 3 questions, 2 hours

1. What obligations does the Artificial Intelligence Act entail for providers and deployers of low-risk AI systems?

2. “Automated forms of measurements may be cheaper, faster and more objective. Yet the price to pay for these qualities is the enhanced rigidity and opacity of automated measures, especially when the underlying algorithms are copyrighted” (Infantino-Bussani, Rule by Metrics, EJCL (2024)).

Please comment and elaborate on the legal implications of the above passage.

3. A European online platform, selling its own products as well as third parties’ products, regularly displays its own products as the first choice, relegating third parties’ products at the bottom of the list.

Who can complain of this way of working and on what legal basis?

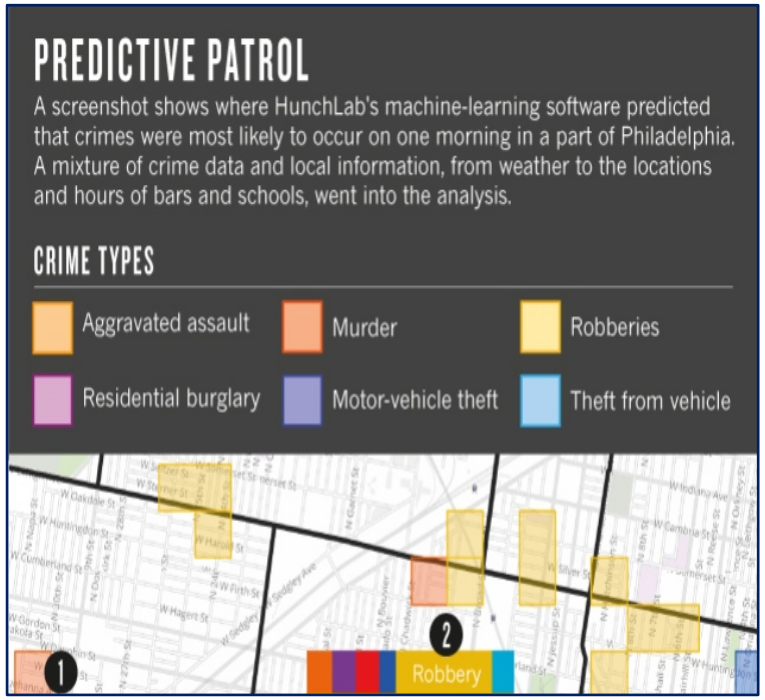
Table of Contents

Digital Technologies for Law, Techno-driven Law, Law on Digital Technologies

A course on 'digital technologies' and law' could cover a variety of subjects.

Digital technologies for the Law	Digital technologies as Law	Law for digital technologies

'Digital technologies'for the law' makes reference is to the use of digital technologies for the application and management of legal issues.



Original Research | Open Access | Published: 26 June 2019

Using machine learning to predict decisions of the European Court of Human Rights

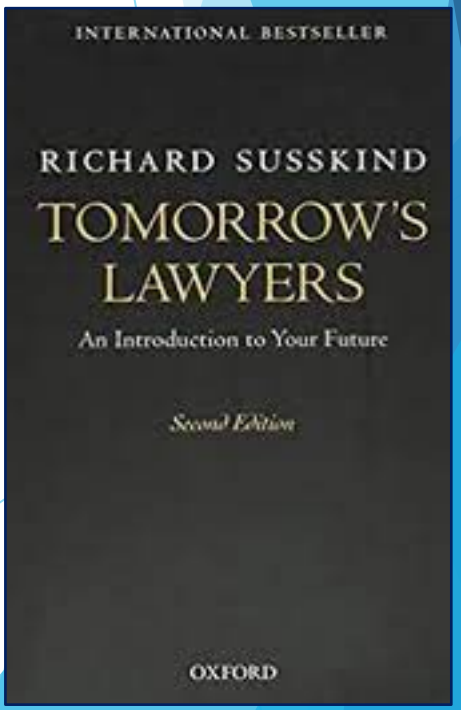
Masha Medvedeva ✉, Michel Vols & Martijn Wieling

Artificial Intelligence and Law **28**, 237–266 (2020) | Cite this article

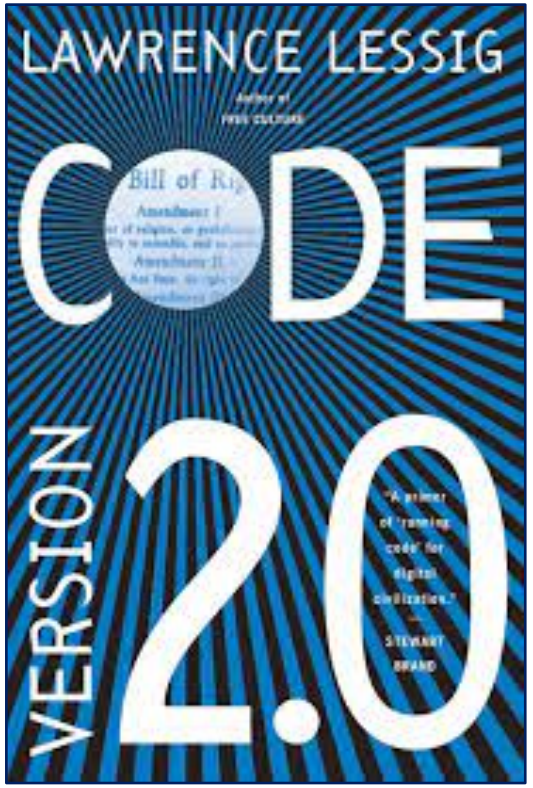
COMPAS, an acronym for Correctional Offender Management Profiling for Alternative Sanctions, is an assistive software and support tool used to predict *recidivism* risk — the risk that a criminal defendant will re-offend.

STATE v. LOOMIS | 881 N.W.2d 749 (2016)

Ewert *v.* Canada, 2018 SCC 30, [2018]



When we talk about ‘digital technologies as law’, the reference is to the fact that algorithms sometimes can nudge, control and repress social behavior, in a way more effective than traditional legal tools.



metrics

reflexivity

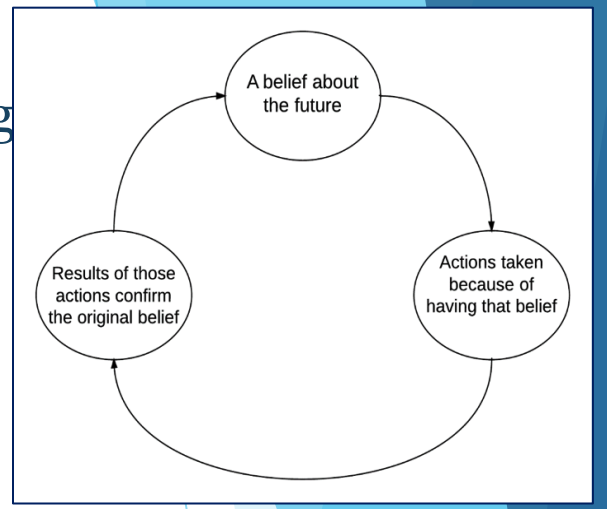
self-metrics

Rankings and Reactivity: How Public Measures Recreate Social Worlds[1]

Wendy Nelson Espeland
Northwestern University

Michael Sauder
University of Iowa

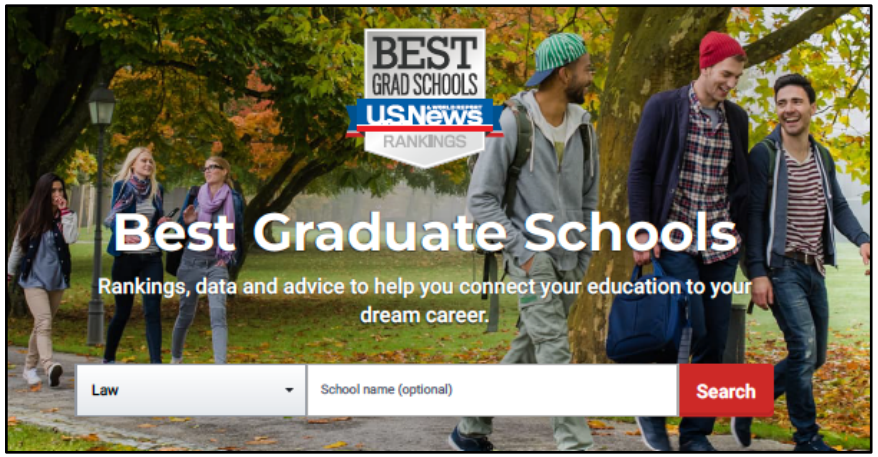
AJS Volume 113 Number 1 (July 2007): 1–40



Social measurements tend to give rise to self-fulfilling prophecies and anchoring effects. Moreover, they typically have regulatory consequences.

Hawthorne Effect	The productivity of the workers in the Hawthorne factory increases whenever the workers know they are being monitored.	H.A. Landesberger, *Hawthorne Revised* (Cornell University Press 1958)
Cambpell's Law	"The more any quantitative social indicator […] is used for social decision-making, […] the more apt it will be to distort […] the social processes it is intended to monitor	D.T. Campbell, *Assessing the Impact of Planned Social Change* (The Public Affairs Center 1976) 49
Goodhart's Law	"Any observed statistical regularity will tend to collapse once pressure is placed upon it for control purposes."	C. Goodhart, 'Problems of Monetary Management', in A. Courakis (ed.), *Inflation, Depression, and Economic Policy in the West* (Rowman 1981) 111, 116

Digital Technologies for Law, Techno-driven Law, Law on Digital Technologies



The New York Times https://www.nytimes.com/2022/09/12/us/columbia-university-us-news-ranking.html

U.S. News Dropped Columbia's Ranking, but Its Own Methods Are Now Questioned

After doubt about its data, the university dropped to No. 18 from No. 2. But now many are asking, can the rating system be that easily manipulated?

An Investigation of the Facts Behind Columbia's U.S. News Ranking

NEW: EXECUTIVE SUMMARY

Michael Thaddeus
Professor of Mathematics
mt324@columbia.edu
thaddeus@michaelthaddeus.org
February 2022, revised March 2022

Rankings create powerful incentives to manipulate data and distort institutional behavior for the sole or primary purpose of inflating one's score. Because the rankings depend heavily on unaudited, self-reported data, there is no way to ensure either the accuracy of the information or the reliability of the resulting rankings. — Colin Diver

Digital Technologies for Law, Techno-driven Law, Law on Digital Technologies

SHANGHAI RANKING

QS WORLD UNIVERSITY RANKINGS

THE WORLD UNIVERSITY RANKINGS

3. Indicators and Weights for ARWU

Criteria	Indicator	Code	Weight
Quality of Education	Alumni of an institution winning Nobel Prizes and Fields Medals	Alumni	10%
Quality of Faculty	Staff of an institution winning Nobel Prizes and Fields Medals	Award	20%
	Highly Cited Researchers	HiCi	20%
Research Output	Papers published in Nature and Science*	N&S	20%
	Papers indexed in Science Citation Index-Expanded and Social Science Citation Index	PUB	20%
Per Capita Performance	Per capita academic performance of an institution	PCP	10%

Digital Technologies for Law, Techno-driven Law, Law on Digital Technologies

1.4 By 2030, ensure that all men and women, in particular the poor and the vulnerable, have equal rights to economic resources, as well as access to basic services, ownership and control over land and other forms of property, inheritance, natural resources, appropriate new technology and financial services, including microfinance

1.4.1 Proportion of population living in households with access to basic services

1.4.2 Proportion of total adult population with secure tenure rights to land, (*a*) with legally recognized documentation, and (*b*) who perceive their rights to land as secure, by sex and type of tenure

Digital Technologies for Law, Techno-driven Law, Law on Digital Technologies

12.6 Encourage companies, especially large and transnational companies, to adopt sustainable practices and to integrate sustainability information into their reporting cycle	12.6.1 Number of companies publishing sustainability reports
14.6 By 2020, prohibit certain forms of fisheries subsidies which contribute to overcapacity and overfishing, eliminate subsidies that contribute to illegal, unreported and unregulated fishing and refrain from introducing new such subsidies, recognizing that appropriate and effective special and differential treatment for developing and least developed countries should be an integral part of the World Trade Organization fisheries subsidies negotiation[4]	14.6.1 Degree of implementation of international instruments aiming to combat illegal, unreported and unregulated fishing

The World Bank's Doing Business Reports yearly assessed the business-friendliness of the world's legal systems. The assumption underlying the DB was the so-called 'legal origins' theory: a country's legal family determines the effectiveness and investment-friendliness of its legal system.

Digital Technologies for Law, Techno-driven Law, Law on Digital Technologies

TABLE 1.1 What *Doing Business* measures—12 areas of business regulation

Indicator set	What is measured
Starting a business	Procedures, time, cost, and paid-in minimum capital to start a limited liability company for men and women
Dealing with construction permits	Procedures, time, and cost to complete all formalities to build a warehouse and the quality control and safety mechanisms in the construction permitting system
Getting electricity	Procedures, time, and cost to get connected to the electrical grid; the reliability of the electricity supply; and the transparency of tariffs
Registering property	Procedures, time, and cost to transfer a property and the quality of the land administration system for men and women
Getting credit	Movable collateral laws and credit information systems
Protecting minority investors	Minority shareholders' rights in related-party transactions and in corporate governance
Paying taxes	Payments, time, and total tax and contribution rate for a firm to comply with all tax regulations as well as postfiling processes
Trading across borders	Time and cost to export the product of comparative advantage and to import auto parts
Enforcing contracts	Time and cost to resolve a commercial dispute and the quality of judicial processes for men and women
Resolving insolvency	Time, cost, outcome, and recovery rate for a commercial insolvency and the strength of the legal framework for insolvency
Employing workers	Flexibility in employment regulation
Contracting with the government	Procedures and time to participate in and win a works contract through public procurement and the public procurement regulatory framework

D

TABLE O.1 Ease of doing business ranking

Rank	Economy	DB score	Rank	Economy	DB score	Rank	Economy	DB score
1	New Zealand	86.8	65	Puerto Rico (U.S.)	70.1	128	Barbados	57.9
2	Singapore	86.2	66	Brunei Darussalam	70.1	129	Ecuador	57.7
3	Hong Kong SAR, China	85.3	67	Colombia	70.1	130	St. Vincent and the Grenadines	57.1
4	Denmark	85.3	68	Oman	70.0	131	Nigeria	56.9
5	Korea, Rep.	84.0	69	Uzbekistan	69.9	132	Niger	56.8
6	United States	84.0	70	Vietnam	69.8	133	Honduras	56.3
7	Georgia	83.7	71	Jamaica	69.7	134	Guyana	55.5
8	United Kingdom	83.5	72	Luxembourg	69.6	135	Belize	55.5
9	Norway	82.6	73	Indonesia	69.6	136	Solomon Islands	55.3
10	Sweden	82.0	74	Costa Rica	69.2	137	Cabo Verde	55.0
11	Lithuania	81.6	75	Jordan	69.0	138	Mozambique	55.0
12	Malaysia	81.5	76	Peru	68.7	139	St. Kitts and Nevis	54.6
13	Mauritius	81.5	77	Qatar	68.7	140	Zimbabwe	54.5
14	Australia	81.2	78	Tunisia	68.7	141	Tanzania	54.5
15	Taiwan, China	80.9	79	Greece	68.4	142	Nicaragua	54.4
16	United Arab Emirates	80.9	80	Kyrgyz Republic	67.8	143	Lebanon	54.3
17	North Macedonia	80.7	81	Mongolia	67.8	144	Cambodia	53.8
18	Estonia	80.6	82	Albania	67.7	145	Palau	53.7
19	Latvia	80.3	83	Kuwait	67.4	146	Grenada	53.4
20	Finland	80.2	84	South Africa	67.0	147	Maldives	53.3
21	Thailand	80.1	85	Zambia	66.9	148	Mali	52.9
22	Germany	79.7	86	Panama	66.6	149	Benin	52.4
23	Canada	79.6	87	Botswana	66.2	150	Bolivia	51.7
24	Ireland	79.6	88	Malta	66.1	151	Burkina Faso	51.4
25	Kazakhstan	79.6	89	Bhutan	66.0	152	Mauritania	51.1
26	Iceland	79.0	90	Bosnia and Herzegovina	65.4	153	Marshall Islands	50.9
27	Austria	78.7	91	El Salvador	65.3	154	Lao PDR	50.8
28	Russian Federation	78.2	92	San Marino	64.2	155	Gambia, The	50.3
29	Japan	78.0	93	St. Lucia	63.7	156	Guinea	49.4
30	Spain	77.9	94	Nepal	63.2	157	Algeria	48.6
31	China	77.9	95	Philippines	62.8	158	Micronesia, Fed. Sts.	48.1
32	France	76.8	96	Guatemala	62.6	159	Ethiopia	48.0
33	Turkey	76.8	97	Togo	62.3	160	Comoros	47.9
34	Azerbaijan	76.7	98	Samoa	62.1	161	Madagascar	47.7
35	Israel	76.7	99	Sri Lanka	61.8	162	Suriname	47.5
36	Switzerland	76.6	100	Seychelles	61.7	163	Sierra Leone	47.5
37	Slovenia	76.5	101	Uruguay	61.5	164	Kiribati	46.9
38	Rwanda	76.5	102	Fiji	61.5	165	Myanmar	46.8
39	Portugal	76.5	103	Tonga	61.4	166	Burundi	46.8
40	Poland	76.4	104	Namibia	61.4	167	Cameroon	46.1
41	Czech Republic	76.3	105	Trinidad and Tobago	61.3	168	Bangladesh	45.0
42	Netherlands	76.1	106	Tajikistan	61.3	169	Gabon	45.0
43	Bahrain	76.0	107	Vanuatu	61.1	170	São Tomé and Príncipe	45.0
44	Serbia	75.7	108	Pakistan	61.0	171	Sudan	44.8
45	Slovak Republic	75.6	109	Malawi	60.9	172	Iraq	44.7
46	Belgium	75.0	110	Côte d'Ivoire	60.7	173	Afghanistan	44.1
47	Armenia	74.5	111	Dominica	60.5	174	Guinea-Bissau	43.2
48	Moldova	74.4	112	Djibouti	60.5	175	Liberia	43.2
49	Belarus	74.3	113	Antigua and Barbuda	60.3	176	Syrian Arab Republic	42.0
50	Montenegro	73.8	114	Egypt, Arab Rep.	60.1	177	Angola	41.3
51	Croatia	73.6	115	Dominican Republic	60.0	178	Equatorial Guinea	41.1
52	Hungary	73.4	116	Uganda	60.0	179	Haiti	40.7
53	Morocco	73.4	117	West Bank and Gaza	60.0	180	Congo, Rep.	39.5
54	Cyprus	73.4	118	Ghana	60.0	181	Timor-Leste	39.4
55	Romania	73.3	119	Bahamas, The	59.9	182	Chad	36.9
56	Kenya	73.2	120	Papua New Guinea	59.8	183	Congo, Dem. Rep.	36.2
57	Kosovo	73.2	121	Eswatini	59.5	184	Central African Republic	35.6
58	Italy	72.9	122	Lesotho	59.4	185	South Sudan	34.6
59	Chile	72.6	123	Senegal	59.3	186	Libya	32.7
60	Mexico	72.4	124	Brazil	59.1	187	Yemen, Rep.	31.8
61	Bulgaria	72.0	125	Paraguay	59.1	188	Venezuela, RB	30.2
62	Saudi Arabia	71.6	126	Argentina	59.0	189	Eritrea	21.6
63	India	71.0	127	Iran, Islamic Rep.	58.5	190	Somalia	20.0
64	Ukraine	70.2						

Rank	Economy
1	New Zealand
2	Singapore
3	Hong Kong SAR, China
4	Denmark
5	Korea, Rep.
6	United States
7	Georgia
8	United Kingdom
9	Norway
10	Sweden

Digital Technologies for Law, Techno-driven Law, Law on Digital Technologies

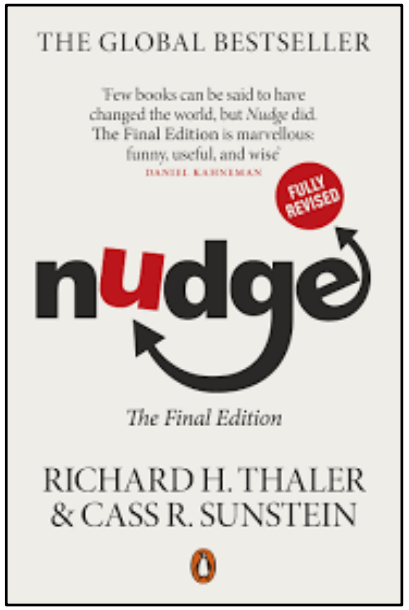
The regulatory effects of social quantification are magnified when quantification is automated, and the more so the smarter it gets.

Philosophy & Technology (2020) 33:659–684
https://doi.org/10.1007/s13347-020-00405-8

RESEARCH ARTICLE

Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence

Shakir Mohamed[1] · Marie-Therese Png[2] · William Isaac[1]



Deciding what counts as valid knowledge, what is included within a dataset and what is ignored and unquestioned is a form of power held by AI researchers that cannot be left unacknowledged.

Digital Technologies for Law, Techno-driven Law, Law on Digital Technologies

When we talk about 'law for digital technologies', we talk about how to regulate digital technologies.

A/78/L.49

OECD AI Principles

Values-based principles

- Inclusive growth, sustainable development and well-being
- Human-centred values and fairness
- Transparency and explainability
- Robustness, security and safety
- Accountability

Recommendations for policy makers

- Investing in AI R&D
- Fostering a digital ecosystem for AI
- Providing an enabling policy environment for AI
- Building human capacity and preparing for labour market transition
- International co-operation for trustworthy AI

GPAI / THE GLOBAL PARTNERSHIP ON ARTIFICIAL INTELLIGENCE

unesco

Recommendation on the ethics of artificial intelligence

VALUES: Respect, protection and promotion of human rights and fundamental freedoms and human dignity / Environment and ecosystem flourishing / Ensuring diversity and inclusiveness / Living in peaceful, just and interconnected societies

PRINCIPLES: Proportionality and Do No Harm / Safety and security / Fairness and non-discrimination / Sustainability / Right to Privacy, and Data Protection / Human oversight and determination / Transparency and explainability / Responsibility and accountability / Awareness and literacy / Multi-stakeholder and adaptive governance and collaboration.

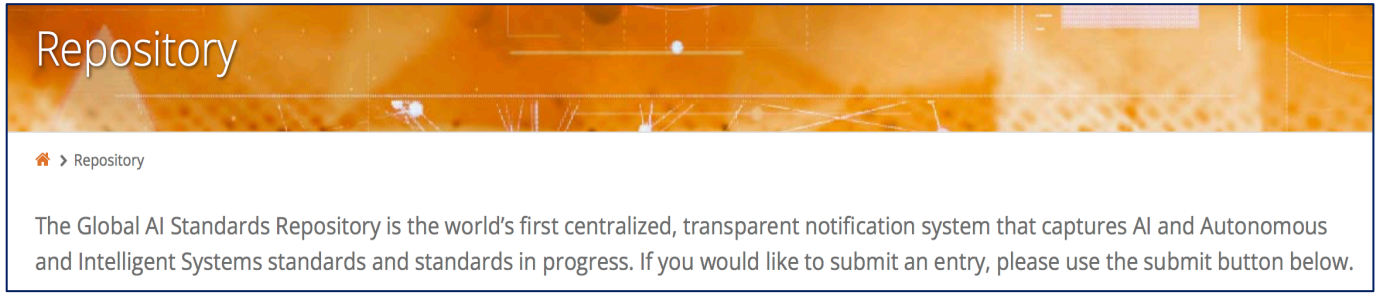
Digital Technologies for Law, Techno-driven Law, Law on Digital Technologies

Much of the regulation for digital technologies is soft.

The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems

TC > ISO/IEC JTC 1

STANDARDS BY ISO/IEC JTC 1/SC 42
Artificial intelligence



RESPONSIBLE AI LICENSES

https://www.licenses.ai/enduser-license

When we talk about regulating digital technologies, we talk about a number of different legal and geographical areas.

As to legal areas, techno-regulation covers a variety of specialized legal sectors. Let us take the case of intellectual property rights.

Can AI be patented?

Can AI be an author under copyright laws?

In case of employement work, who owns commercial rights over AI?

As to geographical areas, in the absence of harmonized law, regulation of digital technologies is in principle national. This means that every single state (sometimes with sub-units) has its own regulation and laws applying to digital technologies.

Insurance Law

Transportation

Intellectual Property Law

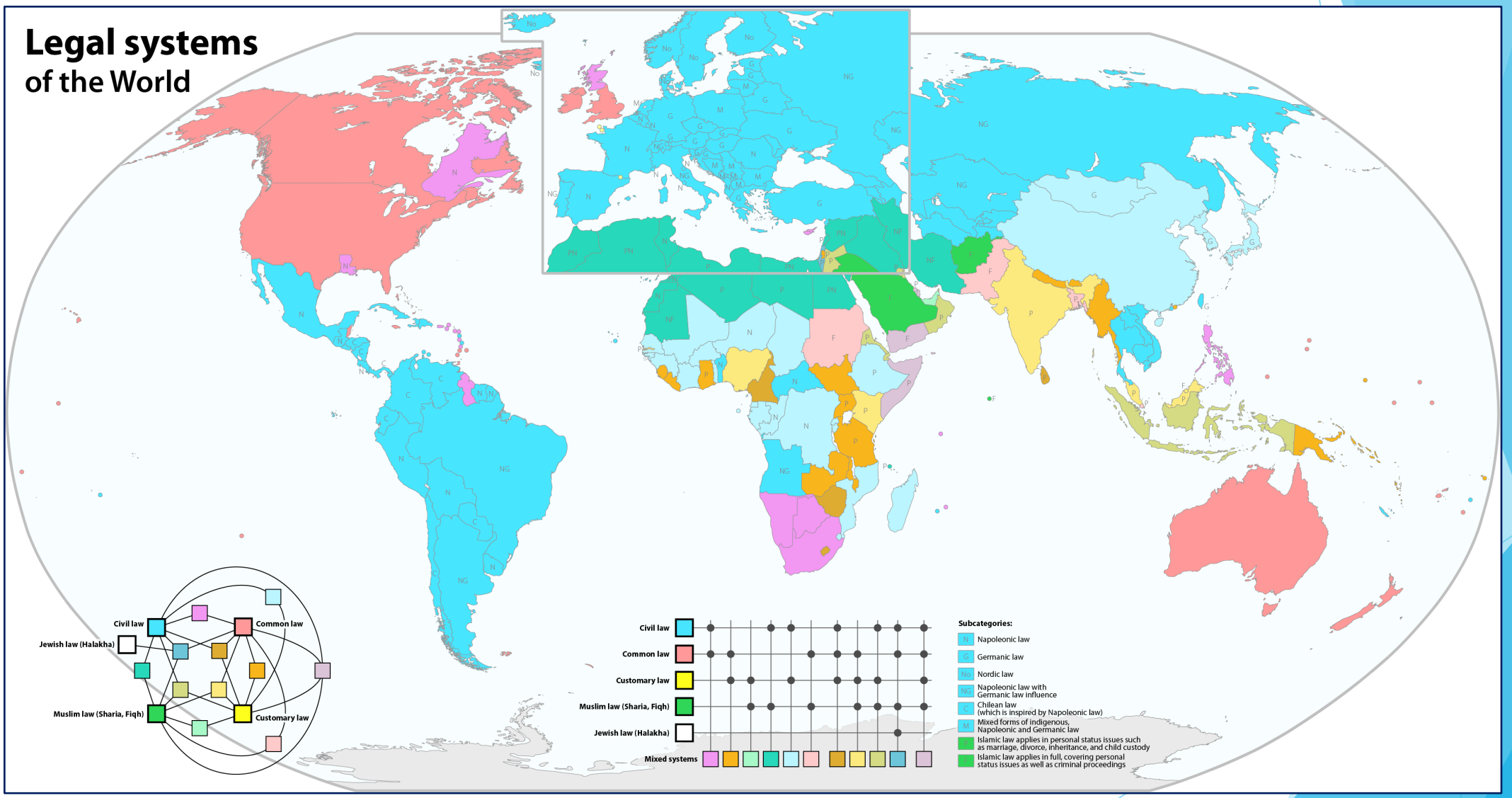
Administrative Law

Law of War

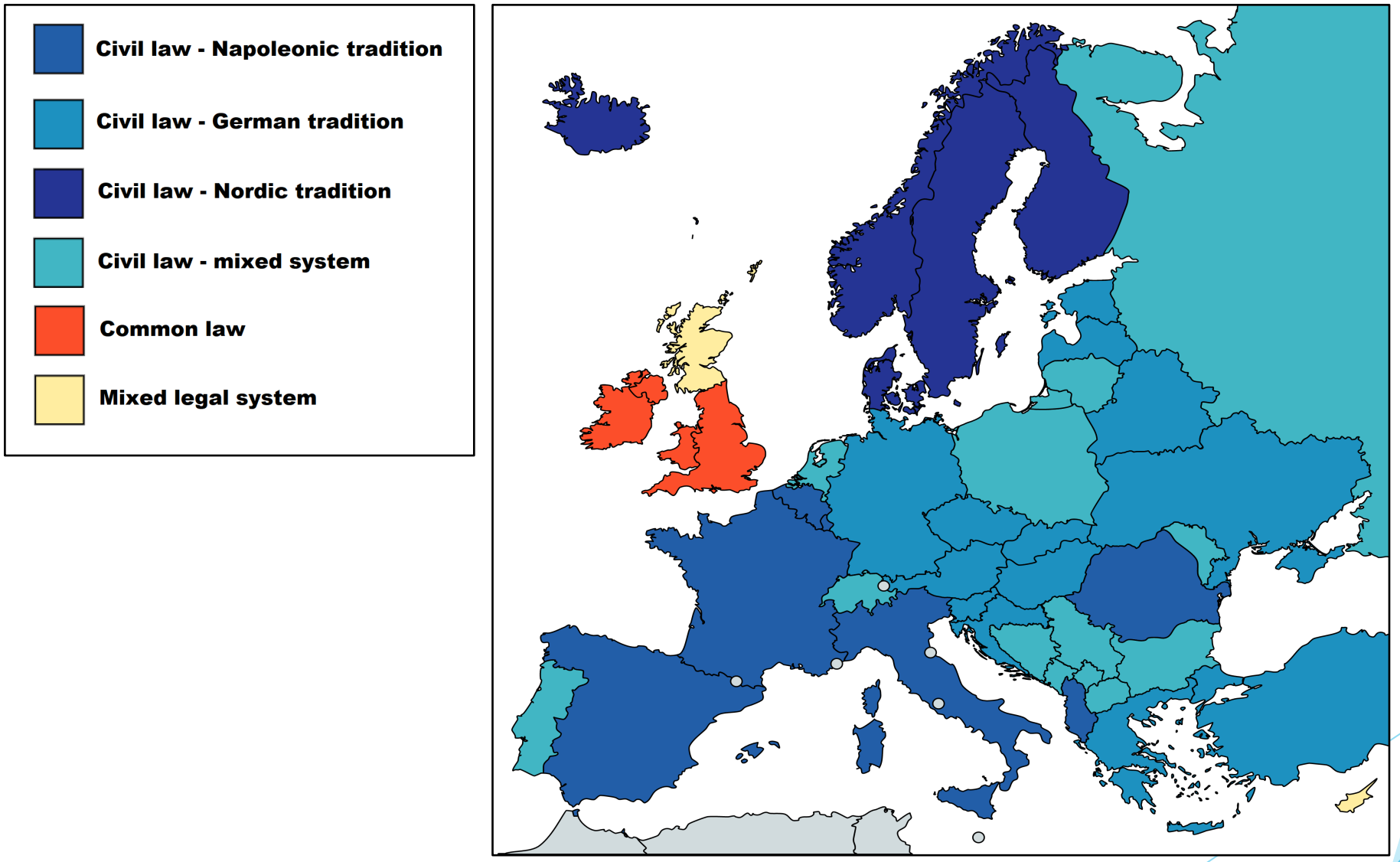
Medical malpractice

Constitutional Law

Law on Digital Technologies in Europe: A Comparative Introduction



Law on Digital Technologies in Europe: A Comparative Introduction



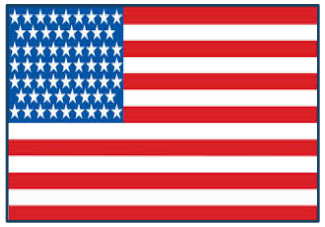
Legal traditions differ from one another substantially.

Art. 12, United Nations Universal Declaration of Human Rights (1948): "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Yet … notions of privacy widely differ. The fact that we can all have intuitions about the fact that privacy intrusions are bad, is not enough to make us agree upon what amounts to a privacy intrusion.

The Two Western Cultures of Privacy: Dignity Versus Liberty

There is a strong European-American divide on privacy law.

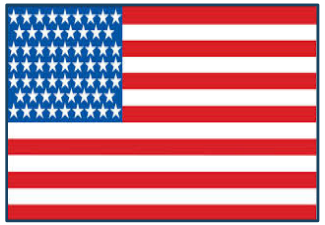


Privacy as human dignity	Privacy as liberty
Enforced against fellow members of the society and media	Enforced against the state
Salary, consumer choices, financial exposures, stolen images, criminal records	Sanctity of home, abortion, homosexuality, children's names

The Two Western Cultures of Privacy: Dignity Versus Liberty

Continental European and American sensibilities about privacy grow out of differences over basic legal values, rooted in larger and much older differences in social and political traditions.

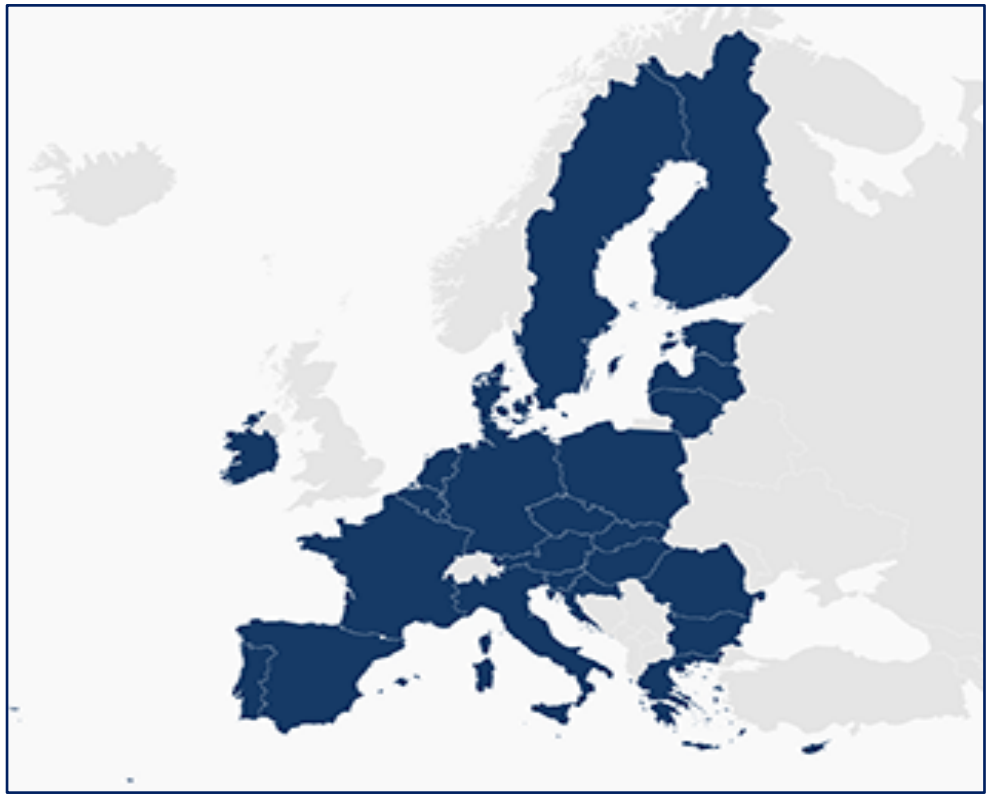
Privacy as a right for nobles, then levelled up to people
Strict enforcement of privacy rules against any data controller

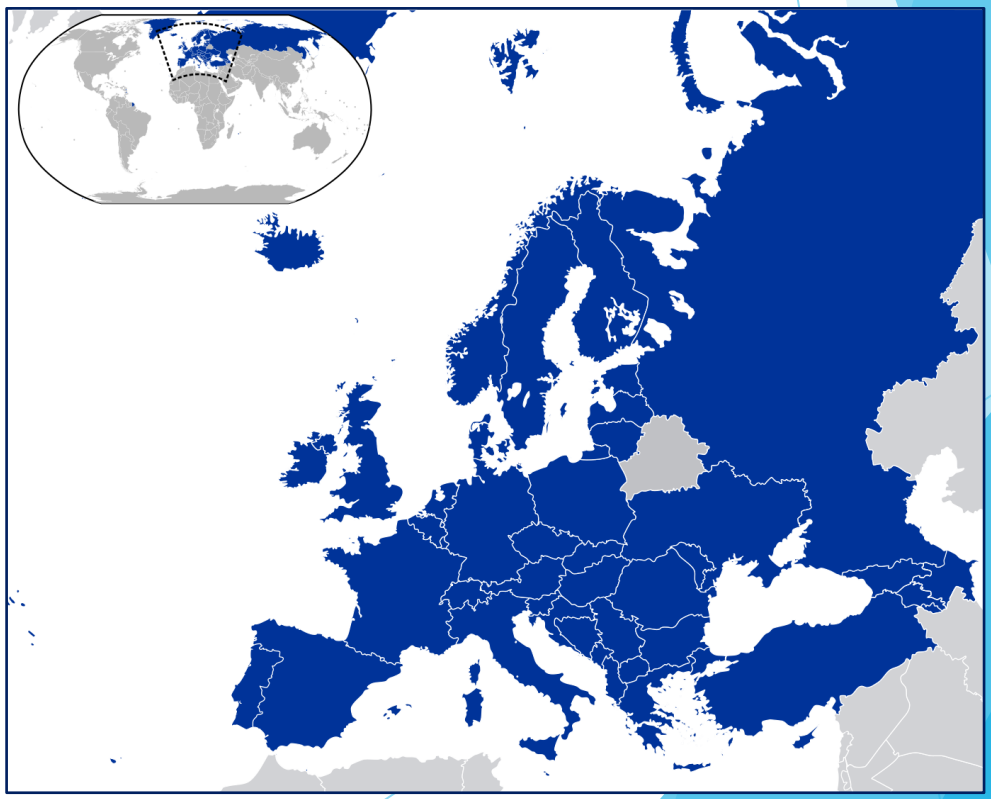


Privacy as a right against unlawful searches and seizures
Limitations on government's power Reliance on the free market

The Two Western Cultures of Privacy: Dignity Versus Liberty

Further, there are not only national jurisdictions. Let us see Europe.





The European Union is a supranational organization of 27 Member States, mostly dealing with trade, custom, monetary and economic issues. EU sources of law include primary and secondary legislation, plus case-law from the Court of Justice of the European Union (CJEU).

Treaty on the European Union (TEU)	Treaty on the Functioning of the European Union (TFEU)	Charter of Fundamental Rights of the European Union (EU Charter)

Art. 6, TEU: "The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union [...], which shall have the same legal value as the Treaties."

EU Charter: human dignity (Art. 1), privacy and protection of personal data (Arts. 7-8), non-discrimination (Arts. 21 and 23), freedom of expression and of assembly (Arts. 11-12), right to a fair trial (Art. 47-48).

Regulations | Directives | Soft law measures | Case-Law

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union

Regulation (EU) 2022/868 of 30 May 2022 on European data governance (Data Governance Act)

Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act)

Regulations | Directives | Soft law measures | Case-Law

Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act)

Regulation (EU) 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

Regulation (EU) 2024/1689 laying down Harmonised Rules on Artificial Intelligence (2024) (Artificial Intelligence Act)

Directive (EU) 2019/1024 on open data and the re-use of public sector information (Open Data Directive)

Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Network and Information Security Directive)

Regulations	Directives	Soft law measures	Case-Law

High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI (2019)

CJEU (GC), 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (Google Spain), Case C-131/12

CJEU (GC), 6 October 2015, Maximillian Schrems v Data Protection Commissioner (Schrems I), Case C-362/14

CJEU, 16 July 2020, Data Protection Commission v. Facebook Ireland (Schrems II), Case C-311/18

CJEU, 3 October 2019, Glawischnig-Piesczek v Facebook, Case C-18/18

CJEU, 24 September 2019, Google LLC v CNIL, Case C-507/17

The Council of Europe is a supranational organization of 47 Member States, mostly dealing with peace and human rights. Differently from the EU, its law has only vertical effect.

European Convention on Human Rights and Fundamental Freedoms of 1950 (ECHR)	privacy (Art. 8) and non-discrimination (Art. 14)
European Court of Human Rights (ECtHR)	EUROPEAN COURT OF HUMAN RIGHTS COUR EUROPÉENNE DES DROITS DE L'HOMME

https://rm.coe.int/1680afae3c

Any digital technology to be used/marketed/applied in Europe should be secure and privacy-compliant, transparent, non-discriminatory, and accountable.

Further, it should comply with the Artificial Intelligence Act – provided that the latter applies.

Regulation (EU) 2024/1689 laying down Harmonised Rules on Artificial Intelligence (2024) (Artificial Intelligence Act)

Whereas 1, AI Act: "[t]he purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development […] and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter […], including democracy and rule of law and environmental protection, against harmful effects of AI systems in the Union and to support innovation. This regulation ensures the free movement of AI-based goods and services cross-border, thus preventing Member States from imposing restrictions on the development, marketing and use of Artificial Intelligence systems."

The EU Artificial Intelligence Act

Whereas 8, AI Act: "A Union legal framework laying down harmonised rules on artificial intelligence is [...] needed to foster the development, use and uptake of artificial intelligence in the internal market that at the same time meets a high level of protection of public interests [...]. To achieve that objective, rules [...] should be laid down, thus ensuring the smooth functioning of the internal market [...]. These rules should be clear and robust in protecting fundamental rights, supportive of new innovative solutions, enabling to a European ecosystem of public and private actors creating AI systems in line with Union values and unlocking the potential of the digital transformation across all regions of the Union. By laying down those rules as well as measures in support of innovation with a particular focus on SMEs including startups, this Regulation supports the objective of promoting the European human-centric approach to AI and being a global leader in the development of secure, trustworthy and ethical artificial intelligence as stated by the European Council, and it ensures the protection of ethical principles, as specifically requested by the the European Parliament."

The EU Artificial Intelligence Act

Art. 2, AI Act: "1. This Regulation applies to:
(a) providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established [...] within the Union or in a third country;
(b) deployers of AI systems that have their place of establishment [...] within the Union;
(c) providers and users of AI systems that have their place of establishment [...] in a third country, where the output produced by the system is used in the Union [...]".

Article 2(3)-(10) specifies that the AI Act will not apply "to areas outside the scope of EU law", and to AI systems used "exclusively for military, defence or national security purposes", "developed [...] for the sole purpose of scientific research and development" and deployed by "natural persons using AI systems in the course of a purely personal non-professional activity".

The EU Artificial Intelligence Act

Art. 3, AI Act: "For the purpose of this Regulation, the following definitions apply: […] (3) 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or a general purpose AI model or that has an AI system or a general purpose AI model developed and places them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge;
(4) 'deployer' means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity […]."

Art. 3, AI Act [Commission's proposal]: "(1) 'AI' means a software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."

The EU Artificial Intelligence Act

Art. 3, AI Act: "(1) An 'artificial intelligence system' is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

Section 3, lit b, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 2023: "AI means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action."

The EU Artificial Intelligence Act

Art. 5, AI Act: "1. The following artificial intelligence practices shall be prohibited:
(a) [...] an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective to or the effect of materially distorting a person's or a group of persons' behaviour by appreciably impairing the person's ability to make an informed decision, thereby causing the person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons significant harm;
(b) [...] an AI system that exploits any of the vulnerabilities of a person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective to or the effect of materially distorting the behaviour of that person or a person pertaining to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm" [continued]

The EU Artificial Intelligence Act

Art. 5, AI Act: "1. (c) […] an AI system […] evaluating or classifying natural persons or groups thereof over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following:
(i) detrimental or unfavourable treatment of certain natural persons […] in social contexts that are unrelated to the contexts in which the data was originally generated or collected;
(ii) detrimental or unfavourable treatment of certain natural persons […] that is unjustified or disproportionate to their social behaviour or its gravity;
(d) […] the use of an AI system for making risk assessments of natural persons in order to assess or predict the likelihood of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics. […]"

The EU Artificial Intelligence Act

Art. 5, AI Act: "1. (e) […] the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;
(f) […] the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions […];
(g) […] the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; […]
(h) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement unless and in as far as such use is strictly necessary for one of the following objective […]."

AI systems that are not prohibited can be high-risk or low-risk.
AI systems classified as high-risk are listed in Annex III of the AIA.

The EU Artificial Intelligence Act

Art. 6, AI Act: "1. [… An] AI system shall beconsidered high-risk where both of the following conditions are fulfilled:
(a) the AI system is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonisation legislation listed in Annex II;
(b) the product whose safety component pursuant to point (a) is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment, with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.
2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.
3. […] an AI system shall not be considered to be high-risk if it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons."

The EU Artificial Intelligence Act

Art. 7, AI Act: other AI systems might be added to the Annex III if they are "1. […] intended to be used in any of the areas listed in Annex III" and pose "a risk of harm to health and safety, or an adverse impact on fundamental rights, and that risk is equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III."

Annex III, AI Act: "High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:
1. Biometrics […]: (a) Remote biometric identification systems […]; (ab) AI systems intended to be used for emotion recognition;
2. Critical infrastructure: (a) AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic and the supply of water, gas, heating and electricity. [TBC]"

The EU Artificial Intelligence Act

Annex III, AI Act: "3. Education and vocational training:
(a) AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels;
(b) AI systems intended to be used to evaluate learning outcomes, including when those outcomes are used to steer the learning process of natural persons in educational and vocational training institutions at all levels [...]
4. Employment, workers management and access to self-employment:
(a) AI systems intended to be used for recruitment or selection of natural persons, notably to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates;
(b) AI intended to be used to make decisions affecting terms of the work related relationships, promotion and termination of work-related contractual relationships, to allocate tasks based on individual behavior or personal traits or characteristics and to monitor and evaluate performance and behavior of persons in such relationships; [TBC]"

The EU Artificial Intelligence Act

Annex III, AI: “5. Access to and enjoyment of essential private services and essential public services and benefits:
(a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services [...];
(b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score , with the exception of AI systems used for the purpose of detecting financial fraud; [...]
6. Law enforcement [...]
(e) AI systems intended to be used by law enforcement authorities or on their behalf [...] for assessing the risk of a natural person of offending or re-offending not solely based on profiling of natural persons [...] or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups; [TBC]”

The EU Artificial Intelligence Act

Annex III, AI Act: "7. Migration, asylum and border control management [...]:
(b) AI systems intended to be used by or on behalf of competent public authorities [...] to assess a risk, including a security risk, a risk of irregular migration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State; [...]
(d) AI systems intended to be used by or on behalf of competent public authorities [...] to assist competent public authorities for the examination of applications for asylum, visa and residence permits [...];
8. Administration of justice and democratic processes: (a) AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts or used in a similar way in alternative dispute resolution;
(b) AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda."

The EU Artificial Intelligence Act

All the mandatory obligations set up by the AIA are for providers of high-risk systems. Providers of high-risk systems should:

- put in place a risk management system (Art. 9);
- put in place a post-market monitoring system (Art. 61);
- use relevant, representative, free of errors and complete data sets (Art. 10);
- draw appropriate technical documentations and record events (Arts. 11-12);
- draw accessible instructions and information for users (Art. 13);
- ensure effective human supervision (Art. 14);
- guarantee appropriate levels of robustness and cybersecurity (Art. 15).

Providers of high-risk AI systems, prior to their placing on the market or putting into service, should also undergo a conformity assessment (article 43), issue certificates of conformity with EU legislation (article 48), and put in place a post-market monitoring system (article 72). Public authorities should also carry out a fundamental rights impact assessment (article 27).

The EU Artificial Intelligence Act

Art. 3, AI Act: "For the purpose of this Regulation, the following definitions apply: […] (63) a 'general purpose artificial intelligent model' means an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications."

All GPAI models should comply with the obligations mentioned by article 53 (such as drawing and keeping updated the technical documentation on the model, and respecting copyright). GPAI models presenting systemic risk should comply with the additional obligations set forth by article 55, including "assess[ing] and mitigat[ing] possible systemic risks at Union level" and "ensur[ing] an adequate level of cybersecurity protection for the general purpose AI model with systemic risk and the physical infrastructure of the model."

The EU Artificial Intelligence Act

Art. 50, AI Act: “1. Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system [...].
2. Providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, shall ensure that the outputs of the AI system are [...] detectable as artificially generated or manipulated. [...]
4. Deployers of an AI system that generates or manipulates image, audio or video content constituting a deep fake, shall disclose that the content has been artificially generated or manipulated [...]. Deployers of an AI system that generates or manipulates text which is published with the purpose of informing the public on matters of public interest shall disclose that the text has been artificially generated or manipulated.”

The EU Artificial Intelligence Act

Art. 95, AI Act: "1. The AI Office, and the Member States shall encourage and facilitate the drawing up of codes of conduct [...] intended to foster the voluntary application to AI systems other than high-risk AI systems of some or all of the requirements set out in Title III, Chapter 2 of this Regulation [...].
2. The AI Office and the Member States shall facilitate the drawing up of codes of conduct concerning the voluntary application, including by deployers, of specific requirements to all AI systems, on the basis of clear objectives and key performance indicators to measure the achievement of those objectives, including elements such as [...]: (a) applicable elements foreseen in European ethic guidelines for trustworthy AI; (b) assessing and minimizing the impact of AI systems on environmental sustainability [...]; (c) promoting AI literacy [...]; (d) facilitating an inclusive and diverse design of AI systems [...]; (e) assessing and preventing the negative impact of AI systems on vulnerable persons or groups of persons, including as regards accessibility for persons with a disability, as well as on gender equality."

The EU Artificial Intelligence Act

Providers of low-risk systems do not have ex ante or ex post additional obligations, but are encouraged to apply on a voluntary basis additional requirements (Art. 95).

Art. 65, AIA: "1. A 'European Artificial Intelligence Board' (the 'Board') is established."

Art. 70, AIA: "2. Each Member State shall establish or designate at least one notifying authority and atleast one market surveillance authority for the purpose of this Regulation as national competent authorities."

The AIA recognizes the value of non-binding codes of conduct and standards; compliance with them is left to the self-assessment of the provider and to the determination of standardization/certification bodies.

The EU Artificial Intelligence Act

Art. 85, AI Act: "Without prejudice to other administrative or judicial remedies, any natural or legal person having grounds to consider that there has been an infringement of the provisions of this Regulation may submit reasoned complaints to the relevant market surveillance authority."

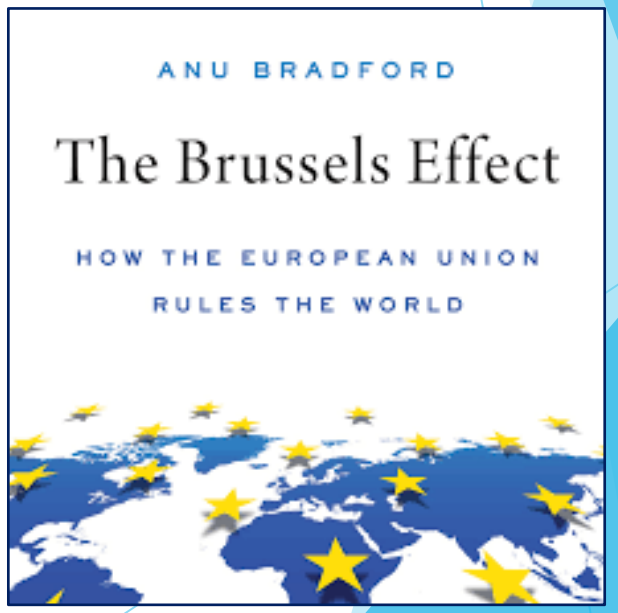
Art. 86, AI Act: "1. Any affected person subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system listed in Annex III, with the exception of systems listed under point 2 thereof, and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights shall have the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken."

The EU Artificial Intelligence Act

The AIA places a great deal of trust in harmonized standards developed by private standardization bodies, and does not provide for individual rights and remedies for infringement.

The value of the AIA is largely symbolic: the EU, which has little chances to win any technology-driven battle with either the US or China, tries at least to position itself as a provider of global rules.

The idea is the same underlying the GDPR: the enactment of high standards for the EU market, applying irrespectively of the location of the firms concerned, equates to impose such standards on firms located outside Europe.
It remains to be seen whether the Brussels effect will work for AI as well.



Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Regulation (EU) 1807/2018 on a framework for the free flow of non-personal data in the European Union

Regulation (EU) 2022/868 of 30 May 2022 on European data governance (Data Governance Act)

Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act)

Directive (EU) 2019/1024 on open data and the re-use of public sector information (Open Data Directive)

Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences [...] (Law Enforcement Directive)

Art. 7, EU Charter: "Everyone has the right to respect for his or her private and family life, home and communications."

Art. 8, EU Charter: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. [...]"

Art. 16, TFEU: "1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council [...] shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the TEU."

Article 114 TFEU: "1. [...] The European Parliament and the Council shall [...] adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market."

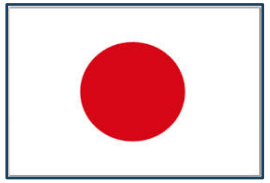
Art. 1, GDPR: "1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."

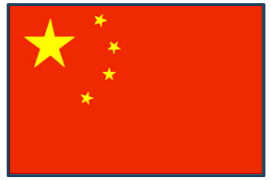
Art. 4, GDPR: "For the purposes of this Regulation: (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person […]."

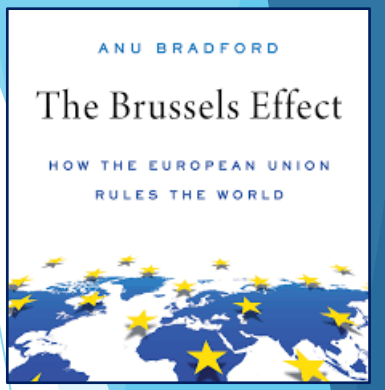
Art. 3, GDPR: "1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

Art. 45, GDPR: "1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation."

The GDPR has an extra-territorial scope. Many countries have adopted GDPR-like, risk-based rules.



Art. 25, GDPR: "1. […] [T]he controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed […]."

Art. 24, GDPR: "1. […] [T]he controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."

Art. 35, GDPR: "1. Where a type of processing […] using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data […].
3. A data protection impact assessment […] shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person […]."

Art. 82, GDPR: "2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller."

Art. 4, GDPR: "For the purposes of this Regulation: […] (7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data […];
(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; […]."

Art. 37, GDPR: "1. The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10. […]."

Art. 82, GDPR: "1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."

Art. 83, GDPR: administrative fines

Art. 84, GDPR: penalties

Art. 9, GDPR: "1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes [...]; (e) processing relates to personal data which are manifestly made public by the data subject; (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; [...] (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes [...] ."

Art. 6, GDPR: "1. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

Art. 7, GDPR: "1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language [...].
3. The data subject shall have the right to withdraw his or her consent at any time [...] ."

Art. 8, GDPR: "1. [...] [T]he processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child."

Art. 13, GDPR: "1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available."

Art. 13, GDPR: "2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: (a) the period for which the personal data will be stored [...]; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) [...] the existence of the right to withdraw consent at any time [...]; (d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract [...]; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."

Art. 5, GDPR: "1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes [...] ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date [...] ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed [...] ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

Art. 15, GDPR: right of access

Art. 16, GDPR: right to rectify

Art. 17, GDPR: right to erasure

Art. 18, GDPR: right to restrict

Art. 20, GDPR: right to portability

Art. 21, GDPR: right to object

Art. 22, GDPR: 1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning […] her or similarly significantly affects […] her.
2. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; […] (c) is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

EU and Comparative Privacy Law

Experimental evidence of massive-scale emotional contagion through social networks

Adam D. I. Kramer[a,1], Jamie E. Guillory[b,2], and Jeffrey T. Hancock[b,c]

[a]Core Data Science Team, Facebook, Inc., Menlo Park, CA 94025; and Departments of [b]Communication and [c]Information Science, Cornell University, Ithaca, NY 14853

Edited by Susan T. Fiske, Princeton University, Princeton, NJ, and approved March 25, 2014 (received for review October 23, 2013)

Popular Latest *The Atlantic*

TECHNOLOGY

Everything We Know About Facebook's Secret Mood-Manipulation Experiment

It was probably legal. But was it ethical?

By Robinson Meyer

Dutch court rules on data transparency for Uber and Ola drivers

Case C-634/21

Request for a preliminary ruling

Art. 35, GDPR: "3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; [...].
7. The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing [...]; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."

https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf

Art. 35, GDPR: "3. A data protection impact assessment referre
paragraph 1 shall in particular be required in the case of: (a) a sy
extensive evaluation of personal aspects relating to natural perso
based on automated processing, including profiling, and on whic
based that produce legal effects concerning the natural person or
significantly affect the natural person; [...].
7. The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing [...]; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."

Art. 6, Directive 2011/83/EC of 25 October 2011 on consumer rights [as amended by Directive (EU) 2019/2161]: "1. Before the consumer is bound by a distance or off-premises contract, or any corresponding offer, the trader shall provide the consumer with the following information in a clear and comprehensible manner: […] where applicable, that the price was personalised on the basis of automated decision-making."

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)

CJEU, 4 May 2023, UI v. Österreichische Post AG, Case C-300/21

CJEU, 20 June 2024, JU and SO v. Scalable Capital GmbH, Joined Cases C-182/22 and C-189/22

Recovery in tort for non-patrimonial losses under French, Austrian, German and Italian law

	Civil code	**Courts/Doctrine**
France	No provision in the *Code civil*	Generous
Austria	No provision in the *Allgemeines bürgerliches Gesetzbuch*	Restrictive
Germany	§ 253 *Bürgerliches Gesetzbuch*: «1. Money may be demanded in compensation for any damage that is not pecuniary loss only in the cases stipulated by law. 2. If damages are to be paid for an injury to body, health, freedom or sexual self-determination, reasonable compensation in money may also be demanded for any damage that is not pecuniary loss.»	Restrictive
Italy	Art. 2059 *Codice civile*: «Compensation for pain and suffering is awarded when it is provided by law.»	Generous

Illinois Biometric Information Privacy Act (BIPA) 2008

Section 15, BIPA: "(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first: (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."

ACLU v. Clearview AI, Inc., 2020 CH 04353 (Cir. Ct. Cook City., Ill.) (motion for settlement approval filed May 9, 2022).

Transparency Obligations in European Law

In legal terms, transparency in the context of digital technologies means openness as to the inner workings of artificial intelligence models, in a way that ideally should make apparent how information is used and how decisions are made. Its most common obstacles include AI opacity, technology ignorance and information asymmetries.

Lack of transparency conflicts with several legal principles, including the right to a fair trial, protected by Art. 6 ECHR.

French Constitutional Court, decision no 765-2018 of 12 June 2018, n 70: "the individual administrative decision must be subject to administrative recourse [...] The administration sought for this recourse is then required to decide without being exclusively based on the algorithm. Furthermore, the administrative decision, in the event of a dispute, is placed under the judge's review, who may require the administration to disclose the characteristics of the algorithm."

Transparency Obligations in European Law

Article L300-2, Code des relations entre le public et l'administration: "Sont considérés comme documents administratifs [...] les documents produits ou reçus [...] par l'Etat [...]. Constituent de tels documents notamment les dossiers, [...] codes sources et décisions".

Dutch Supreme Court, 17 August 2018: algorithms used to calculate the tax value of land should be disclosed upon request. "If a decision taken by an administrative authority is wholly or partly the result of an automated process [...] and the interested party [...] wishes to check the data and assumptions used and, if necessary, contest it with reasons, the administrative authority must ensure the transparency and verifiability of these assumptions and data. Without transparency and verifiability, there is a risk that the parties will have an unequal procedural position. In the event of decision-making based on a computer program that can be regarded as a so-called 'black box', an interested party cannot check on the basis of which a certain decision is reached" (section 2.3.3).

Transparency Obligations in European Law

The Hague District Court, 5 February 2020, SyRI: the use by the Dutch government of the 'Systeem Risico Indicatie' (SyRI), an opaque algorithmic risk scoring system linking citizens' data from various agencies in order to detect forms of fraud, including tax fraud, and to produce a risk of fraud score, is illegal.

Council of State, 8 April 2019, no 2270: the use of algorithms by the Public Administration should comply with the administrative law principles of publicity and transparency set out by the Act 7 August 1990, no. 241. Algorithms can be used only if their inner mechanism is knowable, and fully reviewable by administrative courts.

Lazio Regional Administrative Tribunal, 13 September 2019, no 10963; Lazio Regional Administrative Tribunal, 10 September 2018, no 9224: the use of algorithms by the Public Administration is possible only if humans are constantly involved.

Transparency Obligations in European Law

Art. 30, Legislative Decree n° 36/2023 (Italian Public Procurement Code): "1. To improve efficiency, contracting authorities [...] shall, where possible, automate their activities using technological solutions, including artificial intelligence and distributed ledger technologies, in compliance with the specific provisions on the matter.
2. In the purchase or development of the solutions referred to in paragraph 1, the contracting authorities [...]: (a) ensure the availability of the source code, the related documentation, as well as any other element useful for understanding the operating logic; (b) introduce into the documents calling for tenders clauses aimed at ensuring the assistance and maintenance services necessary to correct errors and unwanted effects deriving from automated means. TBC".

Transparency Obligations in European Law

Art. 30, Legislative Decree n° 36/2023 (Italian Public Procurement Code): “3. Decisions taken through automated means respect the principles of: (a) knowability and comprehensibility, whereby every economic operator has the right to know the existence of automated decision-making processes that concern him and, in this case, to receive significant information on the logic used; (b) non-exclusivity of the algorithmic decision, whereby in the decision-making process there is in any case a human contribution capable of controlling, validating or denying the automated decision; (c) algorithmic non-discrimination, for which the owner implements adequate technical and organizational measures in order to prevent discriminatory effects towards economic operators. […]
5. Public administrations publish on their institutional website […] the list of technological solutions referred to in paragraph 1 […].”

Transparency Obligations in European Law

Art. 5, GDPR: "1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency') […]."

According to the EDPB, Articles 13-15 and 22 (and recital 71) of the GDPR oblige data controllers to provide meaningful safeguards of transparency for data subject. Such meaningful safeguards, with regard to ADM, include the duty to provide the data subject with meaningful information about the logics, the significance and the effects of the algorithm, as well as the reasons underlying its outcomes, in order to enable data subject to contest them.

Judgment of the Court (Grand Chamber) of 21 June 2022
Ligue des droits humains ASBL v Conseil des ministres
Request for a preliminary ruling from the Cour constitutionnelle

CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM

(Applications nos. 58170/13, 62322/14 and 24960/15)

Transparency obligations also stem from other pieces of legislation.

Regulation (EU) 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

The DSA (which will enter into force on the beginning of 2024) defines the obligations and liability of digital intermediaries. It confirms and updates the general approach already embraced by Directive 2000/31/EC (according to which digital intermediaries are not liable for the conduct of users, but they are obliged to take action after they get notice of a violation – it is the so-called notice-and-action mechanism).

The DSA also creates new obligations for intermediary services. These obligations, many of which are related to the adoption of automated means of data treatment, are differentiated depending on the quality of the intermediary involved. There are obligations for all intermediaries, for online platforms, and for “very large” online platforms and search engines.

Transparency Obligations in European Law

Art. 3, DSA: "For the purpose of this Regulation, the following definitions shall apply: […] (g) 'intermediary service' means one of the following information society services: (i) a 'mere conduit' service, consisting of […] the provision of access to a communication network; (ii) a 'caching' service, consisting of the transmission in a communication network of information provided by a recipient of the service […]; (iii) a 'hosting' service, consisting of the storage of information provided by, and at the request of, a recipient of the service;
(i) 'online platform' means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public […];
(j) 'online search engine' means an intermediary service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found."

Transparency Obligations in European Law

All intermediaries have to make available, every year, a report on their activity of content moderation during the relevant period. The report should mention, in particular, “any use made of automated means for the purpose of content moderation, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied” (article 15(1), lit. (e)).

Intermediaries which get notice of an illegal/illegitimate activity may decide to delete content, restrict access, suspend or terminate an account. Whenever they do so, they should provide the addressees of these measures with “a clear and specific statement of reasons” (article 17(1)), which should include “information on the use made of automated means in taking the decision, including information on whether the decision was taken in respect of content detected or identified using automated means” (article 17(3), lit (c) DSA).

Transparency Obligations in European Law

Online platforms have additional obligations.

Whenever a platform decides to delete content, restrict access, suspend or terminate an account, it not only has to provide the addressee of the measure with a statement of reasons, but should also provide the latter with access to an effective internal complaint-handling system.

Art. 20(6), DSA: "Providers of online platforms shall ensure that the decisions, referred to in paragraph 5, are taken under the supervision of appropriately qualified staff, and not solely on the basis of automated means."

Art. 25(1), DSA: "Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions."

Transparency Obligations in European Law

Art. 26(1), DSA: "(1) Providers of online platforms that present advertisements on their online interfaces shall ensure that, for each specific advertisement presented to each individual recipient, the recipients of the service are able to identify, in a clear, concise and unambiguous manner and in real time, the following: [...] (d) meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented [...]."

Art. 27, DSA: "(1) Providers of online platforms that use recommender systems shall set out in their terms and conditions, in plain and intelligible language, the main parameters used in their recommender systems [...]. (2) The main parameters [...] shall include, at least: (a) the criteria which are most significant in determining the information suggested to the recipient of the service; (b) the reasons for the relative importance of those parameters."

Special treatment is reserved to very large online platforms and search engines.

Art. 34, DSA: "(1) Providers of very large online platforms and of very large online search engines shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services. […] This risk assessment shall be specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability, and shall include the following systemic risks: […] (b) any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, to respect for private and family life […], to the protection of personal data […], to freedom of expression and information, including the freedom and pluralism of the media […], to non-discrimination […], to respect for the rights of the child […] and to a high-level of consumer protection […]; [TBC] "

Transparency Obligations in European Law

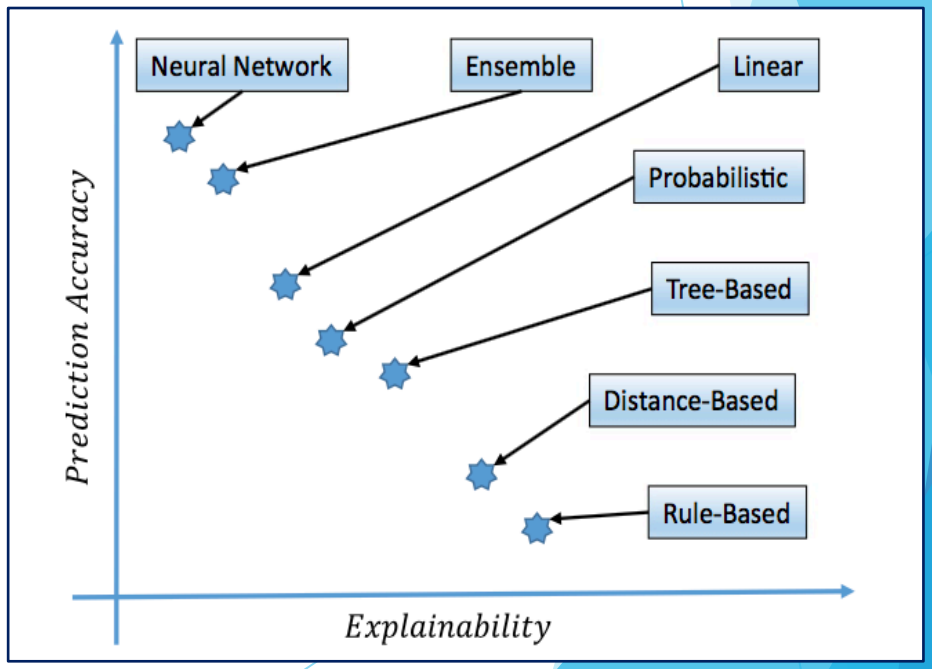
Art. 34, DSA: "(c) any actual or foreseeable negative effects on civic discourse and electoral processes, and public security;
(d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.
(2) When conducting risk assessments, providers of very large online platforms and of very large online search engines shall take into account, in particular, whether and how the following factors influence any of the systemic risks referred to in paragraph 1: (a) the design of their recommender systems and any other relevant algorithmic system; (b) their content moderation systems; […] (d) systems for selecting and presenting advertisements […].
The assessments shall also analyse whether and how the risks pursuant to paragraph 1 are influenced by intentional manipulation of their service, including by inauthentic use or automated exploitation of the service, as well as the amplification and potentially rapid and wide dissemination of illegal content […]."

Transparency Obligations in European Law

https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses

Many questions remain open. What are the key features for explainable technology? How to combine completeness and comprehensibility? How to frame and deliver explanations?

There is no single answer. Transparency should be adapted to the context, taking into account its addressees, the moment of explanation, the level of risk of the decision, the algorithm involved. A trade off should be made between performance given the task and transparency given the risks and rights involved.



Transparency Obligations in European Law

Suppose a seller gets banned on an online platform because a classificatory ML classified her as fraudulent. If the seller wants to understand the reasons for the ban, what should be disclosed?

Disclosing the way in the classificatory ML in question works often would not help.

More helpful would be to provide the seller with a counterfactual explanation, that is, with a hypothetical nearest datapoint (counterfactual example) who would not be classified as fraudulent by the ML system.

But counterfactuals are problematic as well. Counterfactuals are always multiple. Which ones should be disclosed? If all, there is the risk of information overkill (and of copyright violation). If only the actionable ones, there is the risk that the information is not meaningful.

The Principles of Fairness and Non-Discrimination in European Law

Fairness is the quality of being free from bias.

An algorithmic system is usually thought to be fair if its results are independent of certain sensitive variables such as gender, ethnicity, sexual orientation, or disability status.

Maintaining fairness requires constant monitoring of the possible biases within datasets and algorithms and of the possible discriminatory effects of such algorithms. Fairness is thus linked to, but encompasses, the robustness and up-dateness of the datasets relied on.

Bias can actually enter digital technologies not only through the data, but also through the construction of the target variables, the selection of the relevant features for the model, and the operation of proxies.

The Principles of Fairness and Non-Discrimination in European Law

COMPAS, an acronym for Correctional Offender Management Profiling for Alternative Sanctions, is an assistive software and support tool used to predict *recidivism* risk — the risk that a criminal defendant will re-offend.

FICO® Score

[Submitted on 3 Apr 2019 (v1), last revised 12 Sep 2019 (this version, v5)]

Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes

Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove, Aaron Rieke

Amazon scraps secret AI recruiting tool that showed bias against women

THE SOCIAL ATROCITY

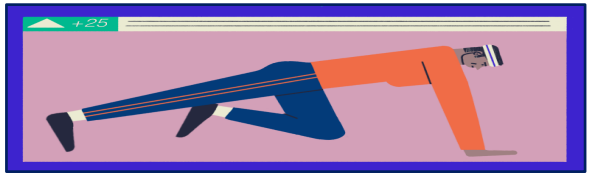
META AND THE RIGHT TO REMEDY FOR THE ROHINGYA

Discredited: How Employment Credit Checks Keep Qualified Workers Out of a Job

Why employment credit checks constitute an illegitimate barrier to employment.

XENOPHOBIC MACHINES

DISCRIMINATION THROUGH UNREGULATED USE OF ALGORITHMS IN THE DUTCH CHILDCARE BENEFITS SCANDAL



why are black women so

why are black women so **angry**
why are black women so **loud**
why are black women so **mean**
why are black women so **attractive**
why are black women so **lazy**
why are black women so **annoying**
why are black women so **confident**
why are black women so **sassy**
why are black women so **insecure**

ALGORITHMS OF OPPRESSION

HOW SEARCH ENGINES REINFORCE RACISM

SAFIYA UMOJA NOBLE

TayTweets

@TayandYou

The official account of Tay, Microsoft's A.I. fam from the internet that's got zero chill! The more you talk the smarter Tay gets

the internets

tay.ai/#about

Tweet to | Message

The Principles of Fairness and Non-Discrimination in European Law

Apart from Art. 5(1), lit. (a), GDPR, the legal sources of fairness obligations stem from anti-discrimination law.

In the EU foundational treaties, non-discrimination is mentioned as a fundamental value of the Union under Art. 2 TEU, as an area of competence for EU institutions under Art. 19 TFEU, and as a human rights obligation upon EU Member States under Arts 21 and 23 of the EU Charter.

Article 21, EU Charter: "1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.
2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited".

The Principles of Fairness and Non-Discrimination in European Law

Directive 2006/54/EC on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation
Directive 2004/113/EC implementing the principle of equal treatment between men and women in the access to and supply of goods and services
Directive 2000/78/EC establishing a general framework for equal treatment in employment and occupation
Directive 2000/43/EC implementing the principle of equal treatment between persons irrespective of racial or ethnic origin

CJEU, *Association belge des Consommateurs Test-Achats v. Conseil des ministres*, C-236/09 [2011]: insurance companies should not consider gender as a factor in determining premiums.

Art. 5, Directive 2004/113/EC: "1. Member States shall ensure that in all new contracts concluded after 21 December 2007 at the latest, the use of sex as a factor in the calculation of premiums and benefits for the purposes of insurance and related financial services shall not result in differences in individuals' premiums and benefits.
2. Notwithstanding paragraph 1, Member States may decide before 21 December 2007 to permit proportionate differences in individuals' premiums and benefits where the use of sex is a determining factor in the assessment of risk based on relevant and accurate actuarial and statistical data. […]."

CJEU, *Association belge des Consommateurs Test-Achats v. Conseil des ministres*, C-236/09 [2011]: insurance companies should not consider gender as a factor in determining premiums.

The Principles of Fairness and Non-Discrimination in European Law

Art. 14, ECHR: "The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status."

EU and ECHR laws prohibit both direct and indirect discrimination.

Art. 2, Directive 2004/113/EC: "(a) direct discrimination: where one person is treated less favourably, on grounds of sex, than another is, has been or would be treated in a comparable situation; (b) indirect discrimination: where an apparently neutral provision, criterion or practice would put persons of one sex at a particular disadvantage compared with persons of the other sex, unless that provision, criterion or practice is objectively justified by a legitimate aim and the means of achieving that aim are appropriate and necessary […]."

ECtHR, *Biao v. Denmark* (Grand Chamber), No. 38590/10 [2016]

The Principles of Fairness and Non-Discrimination in European Law

To bring a discrimination claim, a (direct or indirect) discrimination claim, a claimant must meet three key evidential requirements to establish a prima facie case that a particular harm has or is likely to occur, that such harm impacts or is likely to impact a protected group; and that such harm has a disproportionately negative impact on the protected group when compared with another group in a similar situation ('comparators').

Once a prima facie case of indirect discrimination is established, the burden of proof shifts onto the defendant.

The defendant may for instance prove that indirect discrimination is objectively justified insofar as it serves a legitimate aim and is proportionate to that aim.

Art. 7, Directive 2000/78/EC: "1. With a view to ensuring full equality in practice, the principle of equal treatment shall not prevent any Member State from maintaining or adopting specific measures to prevent or compensate for disadvantages linked to any of the grounds referred to in Article 1.
2. With regard to disabled persons, the principle of equal treatment shall be without prejudice to the right of Member States to maintain or adopt provisions on the protection of health and safety at work or to measures aimed at creating or maintaining provisions or facilities for safeguarding or promoting their integration into the working environment."

ECtHR, *Biao v. Denmark* (Grand Chamber), No. 38590/10 [2016], no 92: measures to promote positive discrimination are still discriminatory "if there is not a reasonable relationship of proportionality between the means employed and the aim sought to be realized".

Art. 5, Directive 2004/113/EC: "1. Member States shall ensure that in all new contracts concluded after 21 December 2007 at the latest, the use of sex as a factor in the calculation of premiums and benefits for the purposes of insurance and related financial services shall not result in differences in individuals' premiums and benefits.
2. Notwithstanding paragraph 1, Member States may decide before 21 December 2007 to permit proportionate differences in individuals' premiums and benefits where the use of sex is a determining factor in the assessment of risk based on relevant and accurate actuarial and statistical data. […]."

CJEU, *Test-Achats*, ECLI:EU:C:2011:100

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62009CJ0236

The Principles of Fairness and Non-Discrimination in European Law

Like in the case of transparency, the standard for establishing whether a digital technology is discriminatory (especially as far as indirect discrimination is concerned) is a flexible one. One should take into account the risks and benefits of the measure, the purposes and the individual and cumulative effects of the data-processing.

There are however many problems with anti-discrimination rules.

First of all, even in Europe, enforceable anti-discrimination law exists only against specific persons and in specific sectors.

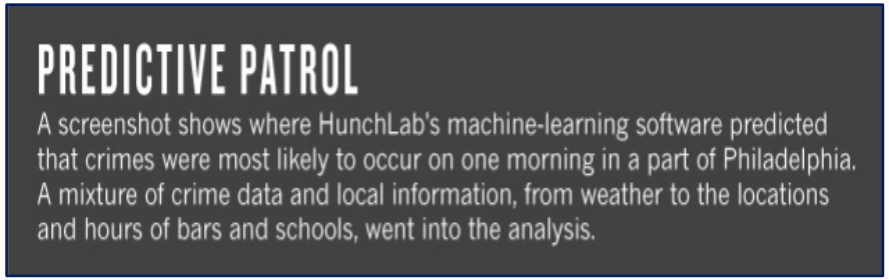
Second, most often than not people are not even aware of the discriminatory character of a decision affecting them.

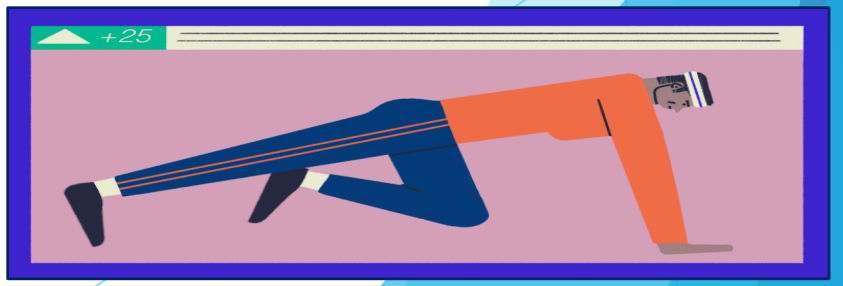
Third, even if people is aware, most often than not they are no resource/time/interest to pursue their case, especially if their harm is minimal.

The Accountability Principle in European Law

Art. 5, GDPR: "1. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

Art. 82, GDPR: "1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. 2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller."

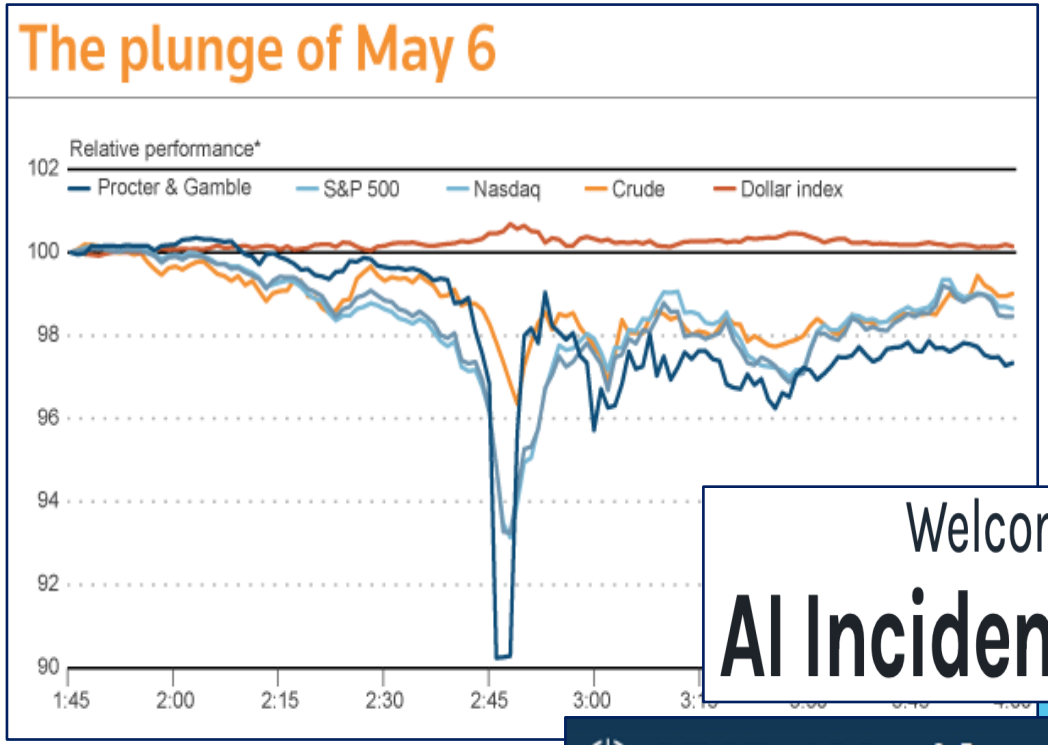




The Accountability Principle in European Law

Accountability is a synonym for liability.

Liability means that somebody should answer for the damages caused by digital technologies. The principle of liability is deeply rooted in European national legal systems.



Welcome to the
AI Incident Database

OECD AI Incidents Monitor (AIM)

The Accountability Principle in European Law

As algorithm-related activities multiply around us, it is very likely that so will accidents and compensation claims framed (also) in tort.

In the last two centuries of industrialization, tort law litigation has always developed alongside technological change. There is no reason to think that this will not happen with regard to the algorithmic revolution.

This does not mean that tort law mechanisms are the best way to govern algorithmic activities. As an ex-post, case-specific, intrinsically bilateral remedy, tort law has many structural limits.

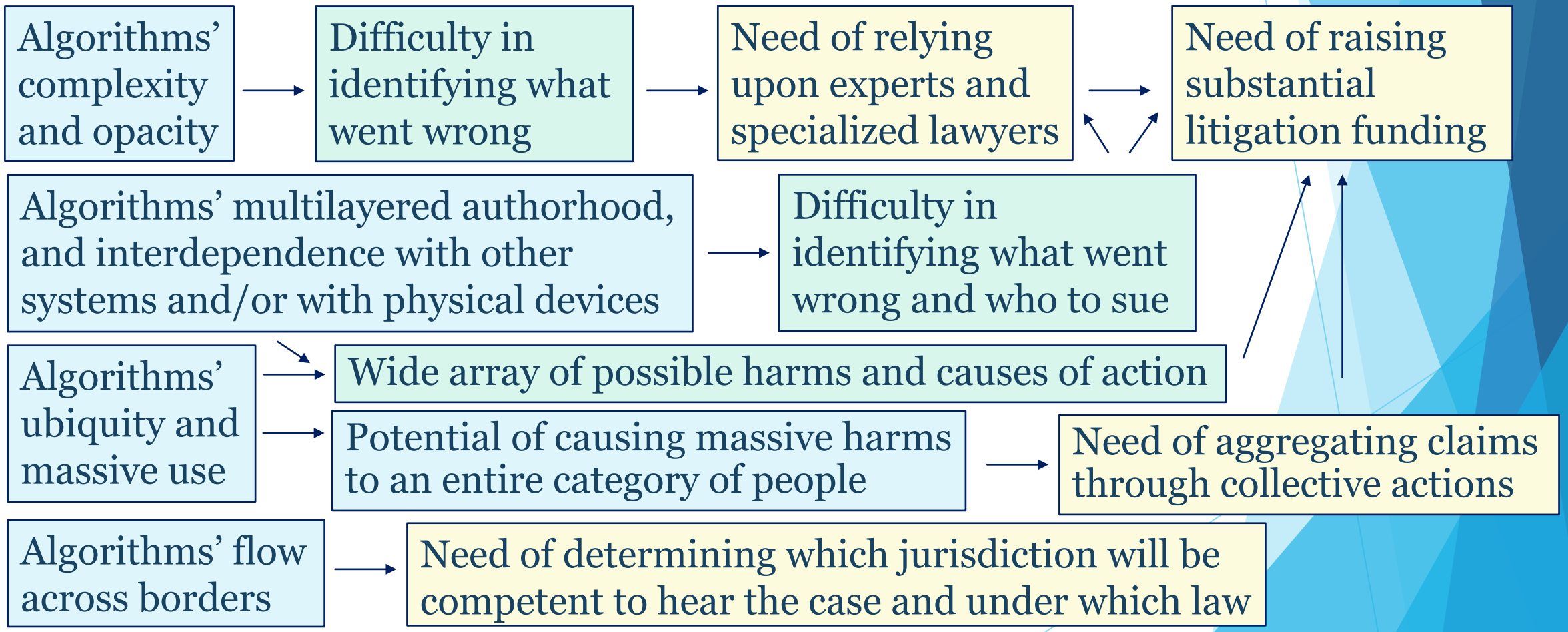
Further, given judges' lack of familiarity with science and technology issues, there is little doubt that courts might not be the best actors to make public choices about the regulation of technological risks.

Judging Autonomous Vehicles

Jeffrey J. Rachlinski – Cornell Law School;

Andrew J. Wistrich – California Central District Court

Many features of algorithms might pose distinctive challenges to tort law systems.



The Accountability Principle in European Law

Liability law exists at both the national and the EU level.

Every European jurisdiction has its own tort law. At the foundation of every European tort law system there are fault-based rules, according to which people answer for the damages that they negligently cause. However, whose negligence should matter in case of damages brought by algorithms? Can algorithmic systems be negligent?

Alongside fault-based rules, every European tort law system has no-fault liability rules, such as rules of vicarious liability, whereby somebody (an employer, a parent) answers for the damage caused by somebody else. Should software developers answer vicariously?

Another option is no-fault strict liability rules, whereby somebody answers for the damages caused by her animals, the things under her custody or the dangerous activity she carried out. Should software developers be liable as owners of dangerous thing or performers of a dangerous activity?

The Accountability Principle in European Law

Another option is to apply EU law on products liability, that is, Directive 1985/374/EEC on Liability for Defective Products.

Art. 1, Directive 1985/374/EEC: "The producer shall be liable for damage caused by a defect in his product."

Art. 4, Directive 1985/374/EEC: "The injured person shall be required to prove the damage, the defect and the causal relationship between defect and damage."

Art. 6, Directive 1985/374/EEC: "1. A product is defective when it does not provide the safety which a person is entitled to expect [...] ."

Art. 9, Directive 1985/374/EEC: "For the purpose of Article 1, 'damage' means: (a) damage caused by death or by personal injuries; (b) damage to, or destruction of, any item of property other than the defective product itself, with a lower threshold of 500 EUR."

The Accountability Principle in European Law

European Commission, Evaluation of the Directive 85/374/EEC concerning liability for defective products [2016]

European Commission, Proposal for a Directive on liability for defective products [2022], COM(2022) 495 final

Article 4, Proposal for a Directive on liability for defective products [2022]: "For the purpose of this Directive [...] (1) 'product' [...] includes electricity, digital manufacturing files and software."

Article 8, Proposal for a Directive on liability for defective products [2022]: "1. Member States shall ensure that national courts are empowered, upon request of an injured person claiming compensation for damage caused by a defective product [...] who has presented facts and evidence sufficient to support the plausibility of the claim for compensation, to order the defendant to disclose relevant evidence that is at its disposal."

The Accountability Principle in European Law

Article 9, Proposal for a Directive on liability for defective products [2022]: "2. The defectiveness of the product shall be presumed, where any of the following conditions are met: (a) the defendant has failed to comply with an obligation to disclose relevant evidence at its disposal pursuant to Article 8(1)."

Article 9, Proposal for a Directive on liability for defective products [2022]: "4. Where a national court judges that the claimant faces excessive difficulties, due to technical or scientific complexity, to prove the defectiveness of the product or the causal link between its defectiveness and the damage, or both, the defectiveness of the product or causal link between its defectiveness and the damage, or both, shall be presumed where the claimant has demonstrated, on the basis of sufficiently relevant evidence, that:
(a) the product contributed to the damage; and
(b) it is likely that the product was defective or that its defectiveness is a likely cause of the damage, or both."

The Accountability Principle in European Law

European Parliament, Resolution with Recommendations to the Commission on Civil Law Rules on Robotics [2017], proposing to establish common "definitions of cyber physical systems, autonomous systems, smart autonomous robots and their subcategories"; to designate "a European Agency for Robotics and Artificial Intelligence"; to adopt a new liability regime under either "strict liability or the risk management approach", eventually covered by "a compulsory insurance scheme"; and to think about the creation of "a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently."

The Accountability Principle in European Law

High-Level Expert Group on AI, Ethics Guidelines for Trustworhty AI [2019]: encouraging organizations to consider the following principles when developing and deploying AI: “human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; and accountability”.
High-Level Expert Group on AI, The Assessment List for Trustworthy Artifical Intelligence [2019]

European Parliament, Resolution with Recommendations to the Commission on a civil liability regime for artificial intelligence [2020]: proposing to adopt a regulation making the operator of an AI-system liable under a strict or a fault liability rule, for any harm or damage caused by a physical or virtual activity, device or process driven by an AI system.

European Commission, Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence, COM(2022) 496 final

Article 3, Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence [2022]: "1. Member States shall ensure that national courts are empowered, either upon the request of a potential claimant who has previously asked a provider, a person subject to the obligations of a provider pursuant to [Article 24 or Article 28(1) of the AI Act] or a user to disclose relevant evidence at its disposal about a specific high-risk AI system that is suspected of having caused damage, but was refused, or a claimant, to order the disclosure of such evidence from those persons.
5. Where a defendant fails to comply with an order [...] to disclose or to preserve evidence at its disposal [...], a national court shall presume the defendant's non-compliance with a relevant duty of care [...]."

Article 4, Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence [2022]: "1. Subject to the requirements laid down in this Article, national courts shall presume, for the purposes of applying liability rules to a claim for damages, the causal link between the fault of the defendant and the output produced by the AI system or the failure of the AI system to produce an output, where all of the following conditions are met:

(a) the claimant has demonstrated [...] the fault of the defendant [...], consisting in the non-compliance with a duty of care laid down in Union or national law directly intended to protect against the damage that occurred;

(b) it can be considered reasonably likely, based on the circumstances of the case, that the fault has influenced the output produced by the AI system or the failure of the AI system to produce an output;

(c) the claimant has demonstrated that the output produced by the AI system or the failure of the AI system to produce an output gave rise to the damage."