THINK [TECH]

Protecting fundamental rights and promoting competition in the Artificial Intelligence Act

5 August 2021

TABLE OF CONTENTS

Executive summary II

Introduction 1

Issue 1: Ambiguity and legal uncertainty 2

Problem: The compliance assessment scheme would threaten human rights and undermine innovation 2

Ambiguous language creates legal uncertainty 2
Programming should not be policy-making 2
Self-assessed compliance exacerbates legal uncertainty 3
Harmonised standards and common specifications would create more problems than they would solve 4
Legal uncertainty and burdensome compliance requirements hinder innovation 5

Solution: More legal, technical, and logistical compliance support 6

Specifications and standards 6
Expanded access to notified bodies 7
Effective compliance tools and guidance 8
Member State communication channels 8
Virtual compliance tool 8
Eliminate redundant compliance requirements 8
Definitions 9

Issue 2: Biometric surveillance and human rights 10

Problems: Permissiveness, insufficient safeguards, and inherent incompatibility with human rights 10

Permissiveness 10
Human rights risks 10
Insufficient legal safeguards 13

Solutions: Absolute ban or strict purpose limitations 13

Stricter purpose limitations 13
Stronger legal safeguards 14
Absolute ban 14

Conclusion 15

Executive summary

The European Commission's proposal for a regulation on artificial intelligence is motivated by two worthy goals: promoting technological innovation and protecting fundamental rights. However, elements of the proposal undermine these goals. Ambiguous key terms would result in legal uncertainty, which in turn would undermine investment and innovation, while creating opportunities for human rights violations. Hypothetically, harmonised standards would offer legal certainty by defining these terms technically and providing presumptive compliance for systems that implement them. However, the proposal does not ensure that standard-setting bodies will be sufficiently responsive, democratic, or rights-protective. Also, the legal safeguards outlined for biometric surveillance methods fall short of what is needed to prevent human rights violations, and unrealistically assume Member States and companies will exercise sufficient self-restraint to make up the difference.

More compliance support for providers would ensure greater legal certainty and less room for human rights violations. Amendments to this proposal and related legislation should ensure that harmonised standards and common specifications are issued speedily, designed with stakeholders representing a more complete range of affected interests, and, in particular, stakeholder groups with human rights legal expertise. In place of, or in addition to, harmonised standards, providers of all high-risk systems should have access to third-party conformity assessment, rapid and complete Member State compliance advice, and a user-friendly virtual compliance tool.

Also, large-scale biometric identification, categorisation, and emotion recognition systems should generally be prohibited for state and business uses, or at least limited to combating serious violent crimes.

Introduction

Two broad goals underlie the European Commission's proposal[1] for a regulation of artificial intelligence (AI). First, the Commission aims to protect fundamental rights, health, and public safety in order to increase public trust in and uptake of AI products in the European Union (EU).[2] Second, the Commission aims to promote technological innovation in the EU, in part by providing legal certainty and support to small- and medium-sized enterprises (SMEs).[3] These goals flow from the Commission's higher-order visions of digital sovereignty and strategic autonomy.[4] This proposal could promote digital sovereignty, in part, by ensuring AI technologies and business practices conform to European values, such as the protection of fundamental rights.[5] By boosting innovation in the EU, it could help to achieve strategic autonomy, which requires a competitive and influential endogenous digital technology sector to preclude geopolitical vulnerabilities arising from dependence on outside digital technologies.[6] But would the proposal achieve these goals?

In its current form, the proposal would create major obstacles to these goals. Highly ambiguous terminology would create an unworkable level of legal uncertainty. This legal uncertainty would both endanger fundamental rights by giving providers inordinate discretion, and also deter investment and innovation by creating confusion about how to avoid large fines for noncompliance. Both legal uncertainty and complex compliance documentation requirements would disproportionately burden SMEs. The availability of harmonised standards would do little to mitigate these problems if – as is currently the case – standard-setting bodies are not necessarily required to engage a broad range of human rights legal experts or respond to requests within a brief time frame. Also, provisions concerning biometric surveillance would provide insufficient human rights protections. This means that the proposal carries the onerous compliance costs of overly prescriptive legislation without the potential benefits of stringent human rights protections.

ThinkTech, e.V., a Munich-based nonprofit organisation composed of technologists, social scientists, philosophers, and attorneys, aims to provide interdisciplinary advice that will enable the Commission to achieve its goals. These include more legal, technical, and logistical support for high-risk conformity assessments, as well as an absolute ban or stricter purpose limitations on large-scale biometric surveillance.

---

[1] *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM/2021/206 final*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206. [Accessed 21 April 2021].

[2] Proposal, Explanatory Memorandum, § 1.1.

[3] Ibid.

[4] Ibid., §§ 1.3 and 2.2; *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2030 Digital Compass: the European way for the Digital Decade, COM/2021/118 final*, § 1 and footnote 3. Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118. [Accessed 27 June 2021]; Madiega, T. (2020, July). *Digital sovereignty for Europe*, p. 1. Available from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf; Michel, C. (2021, February 3). *Digital sovereignty is central to European strategic autonomy* [speech]. Masters of digital 2021, online. Available from: https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/. [Accessed 27 June 2021].

[5] Communication 118, §§ 1, 2, and 6; Madiega, p. 1.

[6] Communication 118, § 3.2; European Political Strategy Centre. (2019, July). *Rethinking Strategic Autonomy in the Digital Age*, pp. 3-4 and 15. Available from: https://op.europa.eu/en/publication-detail/-/publication/889dd7b7-0cde-11ea-8c1f-01aa75ed71a1.

Issue 1: Ambiguity and legal uncertainty

This proposal would shift important policy decisions from politically accountable EU institutions to providers and standard-setting bodies. Providers, the people or entities that make AI systems available in the EU, would be required to answer highly contested legal and ethical questions in order to comply with provisions governing high-risk systems, due to terminological ambiguity and self-assessed compliance. This would be an ineffective way to protect human rights, and the privatisation of such consequential policy-making would be undemocratic. Despite being highly burdensome, providers' documentation requirements would offer little value due to the absence of concrete and stringent human rights protections in the compliance process. This uncertainty would also expose providers to higher risks of unintentional noncompliance and large fines. Despite offering legal certainty to providers, an alternative scheme for harmonised standards would replicate many of these problems. Solutions to these problems include a harmonised standard scheme that incorporates representatives of the broad range of affected stakeholders and business-friendly response times, an expanded third-party conformity assessment process, and effective compliance tools.

Problem: The compliance assessment scheme would threaten human rights and undermine innovation

Ambiguous language creates legal uncertainty

Parts of the legislation crucial to human rights protections contain highly ambiguous terminology. For example, a high-risk system must have "appropriate" levels of accuracy and traceability.[7] Programmers must use "appropriate" data governance and management practices.[8] Training, validation, and testing data must be "relevant" and have "appropriate statistical properties."[9] Levels of risk remaining after a risk assessment and control process must be "acceptable."[10] The Commission sees this as "flexibility," allowing programmers to determine the "precise technical solutions" for a set of "minimum requirements" for the protection of human rights and other public interests.[11]

However, this is misleading. Mandating an "appropriate" level of accuracy is not a minimum requirement, if a requirement is understood as a rule or legal standard. This neither prescribes a specific action nor is a legal term of art that can be interpreted objectively in different circumstances by referencing other sources of law, such as court judgments.[12] It is not a technical term of art, despite the Commission's apparent belief that it can be interpreted with reference to the state of the art. Nonbinding parts of the legislation recommend that providers "tak[e] into account the state-of-the-art and technological and scientific progress in [the] field" and that accuracy "should . . . [be] in accordance with the generally acknowledged state of the art."[13] In risk assessment and management more broadly, providers must "take into account the generally acknowledged state of the art."[14] However, a requirement to consider something is not a requirement to do that thing. What if the provider chooses to read about and then ignore the state of the art because implementation would be expensive? Or what if the state-of-the-art accuracy level is low or provides no clear guidance?

Programming should not be policy-making

Though the Commission presents these as technical details best left to technologists, they actually concern substantive public policy issues with significant impacts on human rights.[15] Consider accuracy. What is an appropriate minimum accuracy level for a recidivism risk assessment program?[16] In other words, how many people should a state put at risk of unfair criminal punishments due to an AI system's inaccuracy? Four out of ten? 0.0001 out of ten? No more than a human? No more than an experienced

[7] Proposal, Articles 12(2) and 15(1).
[8] Proposal, Article 10(2).
[9] Proposal, Article 10(3).
[10] Proposal, Article 9(4).
[11] Proposal, Explanatory Memorandum, § 5.2.3.
[12] Citron, D. (2008). Technological Due Process. *Washington University Law Review, 85*(6), pp 1249-1313 (see pp. 1301-1302). https://openscholarship.wustl.edu/law_lawreview/vol85/iss6/2.
[13] Proposal, Recital 49 and Explanatory Memorandum, § 5.2.3.
[14] Proposal, Article 9(3).
[15] Citron, pp. 1261-1263.
[16] Proposal, Annex III(6)(a).

human judge? And what level of efficiency gain or other benefit would justify each additional person put at risk?

The answer could depend on policy considerations a programmer may not foresee. For example, if a justice ministry's goal is simply to replace human judges to save money, then it could be appropriate to replicate the relatively low human accuracy rate of about 62%.[17] However, if the goal is to improve the fairness and effectiveness of a justice system by increasing the degree of accuracy, then this level would be inappropriately low. The appropriate level may also depend upon the availability of additional resources to house and treat offenders or identify erroneous algorithmic determinations.[18]

Moreover, the draft legislation lacks requirements for acceptable levels of racial, gender, and other biases in accuracy levels and other features. This is despite the well documented potential for automated decision-making systems to produce discriminatory results against historically disadvantaged or marginalised groups.[19] Certain provisions obligate programmers to consider potential bias, such as requirements for datasets to be examined for biases and have "appropriate statistical properties."[20] These are complemented by obligations to identify and mitigate human rights risks to the extent that residual risks are deemed acceptably small, and also notify users about potential human rights risks.[21] However, when considered as a whole, this multiplicity of imprecise and insubstantial provisions does not compensate for the absence of a single precise and concrete rule. For programmers, they require guesswork or create room for endless fudging.

Similarly, the proposal omits rules about *how* to measure bias in accuracy and other features. Yet the choice of metrics can reflect different policy goals and outcomes, such as procedural versus substantive equality, and can also determine whether bias is detected at all.[22]

Many if not most programmers would be unable to predict which of these choices policy-makers and oversight bodies would consider compliant. They may lack the relevant policy expertise or not know how a relevant government agency weighs competing concerns in decision-making.[23] They may be unfamiliar with the constitutional or other legal constraints on the actors who will use their programs. Or human language may simply not translate into programming language or practices.[24] For example, datasets used in training, validation, and testing must be "free of errors."[25] However, this incorrectly assumes it is always possible to objectively identify errors. Textual datasets may be coded by multiple researchers for constructs like toxicity. Given the impossibility of perfectly eliminating subjectivity from these assessments, and given that coders typically disagree on how to categorise some data points and resolve disagreements with predetermined decision-making rules, how can these programmers guarantee that the coded data is "free of errors?" Even if programmers could answer all these questions, it would nonetheless be inappropriate and unfair to burden them with what are essentially philosophical and political conundrums at huge financial risk.

Self-assessed compliance exacerbates legal uncertainty

A programmers' difficulty deciphering this language would not pose a major problem if each high-risk system was assessed by a public body before release. However, most high-risk systems would be subject to internal control, meaning providers would assess their own compliance in the conformity assessment process.[26] In other words, providers would effectively write their own rules, and then judge whether they have complied with these rules. This is little more than self-regulation, but is complemented by heavy penalties for noncompliance.[27] Or providers may purposefully skew their interpretation of the rules for their own benefit, to the detriment of those affected by the output. Does the Commission trust

[17] Dressel, J. and Farid, H. (2018, January 17). The accuracy, fairness, and limits of predicting recidivism. *Science Advances*, 17(1). DOI: 10.1126/sciadv.aao5580.
[18] See, e.g., Pearce, A. (2020, May). *Measuring Fairness*. Google Research. Available from: https://pair.withgoogle.com/explorables/measuring-fairness/.
[19] Gupta, D. and Krishnan, T. S. (2020, November 17). *Algorithmic Bias: Why Bother?* California Management: Insight. Available from: https://cmr.berkeley.edu/2020/11/algorithmic-bias/.
[20] Proposal, Article 10(2-3).
[21] Proposal, Articles 9 and 13(3)(b)(iii).
[22] Mayson, S. (2019). Bias In, Bias Out. *The Yale Law Journal, 128*, pp. 2218-2300 (see pp. 2240-2249). https://www.yalelawjournal.org/article/bias-in-bias-out; Stevenson, M. (2018). Assessing Risk Assessment in Action. *Minnesota Law Review, 58*, 303-366 (see pp. 27-28). https://scholarship.law.umn.edu/mlr/58/.
[23] Citron, Technological Due Process, p. 1296.
[24] Citron, pp. 1261-1262.
[25] Proposal, Article 10(3).
[26] Proposal, Article 43(2).
[27] Proposal, Article 71.

Alphabet, which recently fired multiple AI ethicists and a high-level human rights policy expert for raising ethical concerns, to mark its own work?[28] Does it trust Facebook, which politicised its internal ethics research by essentially redefining algorithmic bias to help one political party, while deprioritising other more significant ethical concerns, to mark its own work?[29]

Based on the Commission's own experiences, the answer should be no. Consider how much of its workload consists of remedying problems that have arisen from weak or self-regulation by large online platforms.[30] Also, as with online platforms, much of the normative underpinning of this effective self-regulation will come from non-EU countries, which often have relatively weak or nonexistent human rights legal standards.[31] This undermines the goal of promoting digital sovereignty, which refers in part to embedding European values in technical design decisions and business practices that affect EU citizens.[32] Why repeat these foreseeable mistakes?

Harmonised standards and common specifications would create more problems than they would solve

The Commission might also argue that most or all legal uncertainty emanating from ambiguous terminology could be neutralised by harmonised standards and common specifications. Harmonised standards are technical standards issued by European Standards Organisations (ESO), which could be adopted in exchange for presumptive compliance.[33] They are already issued pursuant to laws concerning manufactured goods, such as medical devices and elevators.[34] Common specifications are issued by the Commission when existing European standards are incomplete or nonexistent, and would be accompanied by presumptive compliance.[35] The Commission apparently thinks most ambiguities would be resolved with harmonised standards or common specifications.[36] However, the current wording of the proposal does not guarantee that this is an effective or even a desirable solution. The scheme lacks sufficient democratic legitimacy, human rights protections, and responsiveness.

If reliance on harmonised standards to answer highly contested policy conundrums becomes the norm, ESOs would effectively become shadow legislatures. Yet these bodies are insufficiently democratic to play this role. While ESOs must accept opinions from outside stakeholders, the legal basis for European standard setting emphasises only certain classes of outside stakeholders, including environmentalists, consumer rights advocates, and labour rights advocates.[37] These narrow priorities are reflected in the fact that the few semi-permanent stakeholder groups represented in European standard setting are a consumer rights group, an environmentalist group, and a trade union group.[38] Although the consumer

[28] Dickey, M. (2021, February 19). *Google fires top AI ethics researcher Margaret Mitchell*, TechCrunch. Available from: https://techcrunch.com/2021/02/19/google-fires-top-ai-ethics-researcher-margaret-mitchell/; Hao, K. (2020, December 4). *We read the paper that forced Timnit Gebru out of Google. Here's what it says*. MIT Technology Review. Available from: https://www.technologyreview.com/2020/12/04/1013294/google-ai-ethics-research-paper-forced-out-timnit-gebru/; Tiku, N. (2020, January 2). *A top Google exec pushed the company to commit to human rights. Then Google pushed him out, he says*. Washington Post. Available from: https://www.washingtonpost.com/technology/2020/01/02/top-google-exec-pushed-company-commit-human-rights-then-google-pushed-him-out-he-says/.

[29] Hao, K. (2021, March 11). *How Facebook got addicted to spreading misinformation*. MIT Technology Review. Available from: https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/.

[30] See. e.g., European Commission. (2021, March 8). *Fifth set of reports – Fighting COVID-19 disinformation Monitoring Programme*. Available from: https://digital-strategy.ec.europa.eu/en/library/fifth-set-reports-fighting-covid-19-disinformation-monitoring-programme; European Commission. (undated). *The EU Code of conduct on countering illegal hate speech online: Monitoring rounds*. Available from: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en#monitoringrounds. [Accessed 27 June 2021].

[31] See, e.g., Manancourt, V. and Scott, M. (2021, May 28). *In Europe, a coronavirus boom for foreign surveillance firms*. Politico Europe. Available from: https://www.politico.eu/article/europe-surveillance-china-israel-united-states/.

[32] Madiega, Digital sovereignty for Europe, p. 1; Michel, Digital sovereignty is central to European strategic autonomy.

[33] European Commission. (undated). *Harmonised Standards*. Available from: https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_en. [Accessed 27 June 2021]; Proposal, Article 40.

[34] Ibid.

[35] European Commission, Harmonised Standards; Proposal, Article 41.

[36] Gross, K. (2021, May 18). *Towards a European AI Regulation: Presentation of the AI Regulation of the European Commission*. In AI4Belgium Webinar; Proposal, Recital 61 (stating that harmonised standards would play a "key role").

[37] *Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance* (Regulation on European standardisation), Articles 5 and 11. Available from: http://data.europa.eu/eli/reg/2012/1025/oj. [Accessed 2 July 2021].

[38] European Commission. (undated). *Key Players in European Standardisation*. Available from: https://ec.europa.eu/growth/single-market/european-standards/key-players_en. [Accessed 27 June 2021].

group focuses partially on privacy and data protection, none specialise in human rights law generally.[39] They also lack voting rights.[40]

Furthermore, standard-setting bodies would not likely be responsive enough to meet demand from providers. For harmonised standards to facilitate innovation, all providers in need of new standards must receive them in a timely manner. The legal basis for European standard setting requires only annual standardisation priorities from the Commission to guide ESOs.[41] While the Commission recognises the need for speedier standardisation, measures to that end have not been successful.[42] Also, requests for new standards may only be initiated directly by the Commission, or indirectly by a Member State request to the Commission, but apparently not by providers who need them.[43]

Legal uncertainty and burdensome compliance requirements hinder innovation

The Commission might argue that, despite these shortcomings, flexible, less prescriptive legislation is necessary to promote innovation.[44] The Commission posits that its approach avoids "unduly constraining or hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market," while the legal certainty provided will "facilitate investment and innovation."[45] By avoiding prescriptiveness, the Commission aims to accommodate the wide variety and unexpected future uses of programs within the legislation's scope, while reducing compliance costs.[46]

However, the ambiguity of key terms discussed above reduces legal certainty. Providers' decisions about appropriate accuracy levels and acceptable risk levels would likely be highly speculative without additional instructions. According to the CEO of a German company providing AI-based services, so-called flexibility in legal interpretations is "toxic" due to the resulting legal uncertainty.[47] Programmers would spend an inordinate amount of time trying to answer questions outside of their areas of expertise, detracting from their technical work, while the looming threat of large fines would likely deter investment. Despite making best efforts, providers may fall short of an oversight body's interpretation of the law and be fined up to € 30,000,000 or 6% of total worldwide annual turnover.[48] It would also sow distrust among consumers for whom a CE mark would not necessarily represent stringent safety and human rights protections in AI systems, thereby undermining uptake.

Furthermore, despite the flexibility or ambiguity of language affecting human rights, the proposed high-risk compliance process would be onerous. Although industry complaints about compliance burdens may be so common as to sound like white noise, it is important for lawmakers to pause and seriously consider the weight of this burden in the proposal. Article 17's quality management system, one part of the Annex VI conformity assessment process, would require documentation of policies, procedures, and instructions describing:

- A strategy for regulatory compliance
- Techniques, procedures, and systematic actions used in design, verification, development, quality control, and quality assurance
- Procedures for examination, testing, and validation done before, during, and after development
- Technical specifications and standards
    - An explanation of how the specifications and standards meet the requirements for high-risk systems, if they are not harmonised standards
- Systems and procedures for data management, such as collection, cleaning, and storage

[39] European Association for the Coordination of Consumer Representation in Standardisation (ANEC). (undated). *Priorities: Digital Society*. Available from: https://www.anec.eu/priorities/digital-society. [Accessed 27 June 2021].
[40] Regulation on European standardisation, Preamble 23.
[41] Regulation on European standardisation, Article 8.
[42] European Commission (2016, April 19). *Press Release*: *Commission sets out path to digitise European industry*. Available from: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_1407. [Accessed 27 June 2021]; European Commission. (undated). *Joint Initiative on Standardisation*. Available indirectly from: https://ec.europa.eu/growth/content/joint-initiative-standardisation-responding-changing-marketplace_en [Direct link is broken]; Dieters, O. (2021, July 20). *Feedback from DERKA on the European Commission's Standardisation Strategy*. Available from: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13099-Standardisation-strategy/F2662668_en. [Accessed 23 July 2021]; Council of the European Union. (2021, May 11). *Joint – CY, CZ, DE, DK, EE, ES, FI, HU, IE, LU, NL, PL, PT, RO, SE, SI, SK – non-paper on harmonised standards*, *8600/21*. Available from: https://data.consilium.europa.eu/doc/document/ST-8600-2021-ADD-1/en/pdf.
[43] Regulation on European standardisation, Articles 10 and 13; European Commission. (undated). *Standardisation requests – mandates*. Available from: https://ec.europa.eu/growth/single-market/european-standards/requests_en. [Accessed 27 June 2021].
[44] Proposal, Recitals 71 and 73, and Explanatory Memorandum, § 1.1.
[45] Proposal, Explanatory Memorandum, § 1.1.
[46] Proposal, Recital 6.
[47] Manthey, T. (2021, May 14). Personal interview.
[48] Proposal, Article 71(4).

- A risk management system (Article 9)
    - Ongoing risk assessments and risk management strategies for reasonably foreseeable uses
    - A determination of whether residual risks are acceptable
    - Information for users about risks
    - Testing to identify the most appropriate risk management practices

This would be in addition to answering the challenging legal questions raised in Articles 8-15, which are requirements for high-risk systems, and the post-market monitoring plan outlined in Article 61. Such extensive documentation is comparable to requirements for operating a nuclear reactor.[49]

Yet without clear and stringent human rights and safety requirements, the resulting mountain of paperwork would serve no purpose. Who benefits from this scenario?

Large, dominant companies – mostly based outside of the EU – would benefit from this scenario. High compliance costs, such as expenditures on legal advice and additional compliance labour, fall disproportionately on SMEs. Such expenditures are insignificant to a company like Alphabet, but could be cost-prohibitive to smaller European companies.[50] General Data Protection Regulation compliance costs have had similar anticompetitive effects, but these are outweighed by the public benefit of specific, concrete, and stringent human rights protections.[51] Here, there is no equivalent public benefit. This would likely undermine the Commission's goal of promoting innovation and SME competitiveness, and with it strategic autonomy and digital sovereignty.

It may also constitute a disproportionate interference with SME owners' freedom to conduct business.[52] The EU Agency for Fundamental Rights (FRA) has identified burdensome and complex regulatory compliance procedures as a practical impediment to the enjoyment of this right, particularly for young entrepreneurs.[53] The principle of proportionality requires the choice of the least burdensome regulatory strategy possible to achieve a legitimate aim.[54] As discussed below, there are far less burdensome regulatory strategies available to protect human rights and promote innovation.

Solution: More legal, technical, and logistical compliance support

We propose several alternative regulatory strategies for high-risk systems that would more effectively protect fundamental rights and promote innovation. Most suggestions build upon concepts in the Commission's proposal. They include improving European standardisation, expanding the availability of third-party conformity assessment, and providing more effective compliance tools and guidance. Ultimately, providers must be able to obtain legal clarifications from at least one source in order to avoid the financial and human rights risks of legally uncertain self-assessment. Greater legal certainty would advance both of the Commission's goals, while justifying the elimination of redundant paperwork. We also suggest some clarifications of ambiguous key terms.

Specifications and standards

Harmonised standards and common specifications could hypothetically provide legal certainty for providers of high-risk systems, but their legal, democratic, and logistical shortcomings must first be remedied.

First, a far wider variety of outside stakeholder groups must be included in European standardisation. Given that ESOs' democratic legitimacy derives from outside stakeholder involvement, a fuller range of

[49] Manthey, T. (2021, May 14). Personal interview.
[50] Johnson, J. (2021, February 8). *Annual net income of Alphabet from 2011 to 2020*. Statista. Available from: https://www.statista.com/statistics/513049/alphabet-annual-global-income/.
[51] See generally, Gal, M. and Aviv, O. (2020). Competitive Effects of the GDPR. *Journal of Competition Law and Economics, 16*(3), pp. 349-391. https://doi.org/10.1093/joclec/nhaa012; Geradin, D. Karanikioti, T., and Katsifis, D. (2021). GDPR Myopia: how a well-intended regulation ended up favouring large online platforms – the case of ad tech. *European Competition Journal, 17*(1), pp. 47-92. https://doi.org/10.1080/17441056.2020.1848059; Prassad, A. (2020, September 2). *Unintended Consequences of GDPR: A Two-Year Lookback*. Available from: https://regulatorystudies.columbian.gwu.edu/unintended-consequences-gdpr. [Accessed 28 June 2021].
[52] *Charter of Fundamental Rights of the European Union* (Charter). (2012, October 26). http://data.europa.eu/eli/treaty/char_2012/oj.
[53] European Union Agency for Fundamental Rights (FRA). (2015). *Freedom to conduct a business: exploring the dimensions of a fundamental right*, pp. 37 and 40. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-freedom-conduct-business_en.pdf.
[54] Judgment of 9 September 2004, *Spain and Finland v. European Parliament and Council of Europe*, Joined cases C-184/02 and C-223/02, EU:C:2004:497, paragraph 57. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62002CJ0184.

affected interests must be represented. Because AI affects nearly every aspect of EU citizens' lives, and the regulation touches upon deeply political issues, the current representation of environmental, labour, and consumer rights groups does not cover the full range of affected interests.

One way to include more stakeholder groups would be to amend Annex III of the regulation on European standardisation, which lists the types of outside stakeholder groups that are eligible for EU funding.[55] The list should be expanded to include, at a minimum, subject matter experts in each right enumerated in the Charter of Fundamental Rights of the European Union (Articles 1-50), with exceptions for seemingly irrelevant provisions, such as the right to diplomatic and consular protection in Article 46. This would enable the iterative dialogue between technologists and legal experts that is necessary to translate abstract legal principles into precise programming instructions, in order to avoid human rights violations. Also, Recital 17 should be deleted or amended such that the interpretation of the term of "social interests" in Annex III(4) is not perceived as coequal to labour rights.[56] In practice, this suggestion leads to an unjustifiably narrow scope of social interest groups eligible for funding.[57] While the representation of labour interests is crucial, it is not sufficient to cover all social interests affected by AI.

Second, providers must be able to obtain new harmonised standards or common specifications quickly. Currently neither the proposal nor the regulation on European standardisation includes time limits for issuing harmonised standards or common specifications. This contributes to the long delays industries already face in obtaining harmonised standards.[58] Article 41 of the proposal should set a time limit (or a set of time limits) for the Commission to issue common specifications, while Article 10(1) of the regulation on European standardisation should be amended to require the Commission to set short deadlines for ESO standardisation deliverables. Different deadlines for different types of high-risk systems could be enumerated in a new annex to the regulation on European standardisation, and determined after a survey that establishes typical time frames for AI development processes. The same time limits should apply for issuing common specifications. This would promote innovation by ensuring providers are not forced to choose between waiting indefinitely for standards and specifications necessary to put products on the market, or the quicker but legally uncertain path of internal control.

Also, the procedure for requesting new standards or specifications should be more streamlined and better publicised for providers. Article 6 of the regulation on European standardisation could be amended to enable providers to send requests for new standards directly to ESOs or the Commission, rather than through stakeholder bodies that advise the Commission about its annual standardisation priorities. The proposal should also require the Commission to establish an easily found and user-friendly website to submit requests for new harmonised standards or common specifications.

Only with these amendments, or functionally equivalent amendments, can harmonised standards and common specifications play the role the Commission intends.

Expanded access to notified bodies

Another option that could provide legal certainty, though with less democratic legitimacy, is a more widely available ex-ante third-party conformity assessment process. While Article 43 gives providers of biometric surveillance systems the options of self-assessment (internal control) or third-party (notified body) assessment of conformity, it states that providers of other high-risk systems "shall" use self-assessment.[59] To ensure human rights are adequately protected, and to avoid the severe penalties of misinterpreting an ambiguous law, providers of all high-risk systems should be able to verify their conformity assessments with a notified body. Article 43(1) could be reworded as: "For high-risk AI systems listed in Annex III . . .", and the first sentence of Article 43(2) could be deleted.

This strategy would also require a sufficient level of human rights legal expertise in notified bodies. Article 33(10) should be amended such that notified bodies must have an adequate number of staff members with human rights legal expertise, in addition to the required technical and scientific experts, to ensure minimum legal requirements are satisfied. In consultation with staff technologists, these

[55] See footnote 37.
[56] Regulation on European standardisation, Recital 17 (stating: "the representation of social interests and social stakeholders in European standardisation activities refers particularly to the activities of organisations and parties representing employees and workers' basic rights, for instance trade unions").
[57] European Commission. (undated). *Key players in European Standardisation*. Available from: https://ec.europa.eu/growth/single-market/european-standards/key-players_en. [Accessed 26 July 2021].
[58] Council of the European Union, Joint non-paper on harmonised standards, 8600/21.
[59] Proposal, Article 43(2).

human rights legal experts could ensure that each human rights risk is identified and sufficiently mitigated in the program's design.

Effective compliance tools and guidance

We also encourage the Commission to expand upon and actualise its ideas about compliance tools, guidance, and advice for providers of high-risk systems, and particularly those relying upon internal control. Several provisions mention the possibility of guidance and advice for providers. Article 55(1)(c) requires Member States to "establish a dedicated channel for communication . . . to provide guidance and respond to queries about the implementation of this Regulation," but only "where appropriate." Article 59(7) states that competent authorities "may provide guidance and advice" about implementation to providers. Like the standard-setting process, these ideas would promote innovation only if they are sufficiently responsive to providers' needs.

Member State communication channels

In lieu of or in addition to harmonised standards and common specifications at the EU level, the Commission should require Member State authorities to clarify ambiguous terminology and other questions upon request. This could be accomplished through the dedicated communication channel referenced in Article 55(1)(c) of the proposal. Operationalisable answers to questions about specifications for ambiguous terms, such as which accuracy level and metric are appropriate for a given programme or use, should be mandatory, rather than optional. The "where appropriate" qualifier should not be used to restrict this service, at least where smaller providers are concerned.

Virtual compliance tool

We also propose the provision of a user-friendly website that helps technologists create a quality management system and navigate the internal conformity assessment process. It should be structured as a step-by-step process with guidance on what to document and how, and designed with predefined drop-down fields and supplementary text fields where possible. A structured documentation process of this kind would help providers prevent errors, omissions, and misinterpretations of legal terms. The resulting uniformity would also improve auditability. The website could be designed similarly to the European Chemicals Agency's REACH-IT website or ELSTER, a tax compliance website provided by German tax authorities.[60]

This accords with the FRA's recommendation to "adopt e-tools and particularly virtual one-stop-shops" to reduce the administrative burdens that interfere with the freedom to conduct business.[61]

Eliminate redundant compliance requirements

With clear and concrete rules or guidance in place to address risks to human rights, health, and safety issues, much of the proposal's compliance assessment documentation would be redundant. For example, Article 9's risk assessment procedure essentially requires a provider to determine which human rights, health, and safety issues are affected by their system, and how to technically translate applicable rules. Harmonised standards, common specifications, third-party conformity assessments, and, hypothetically, Member State guidance would identify the relevant rules and translate them technically, rendering Article 9 redundant.

Though the absence of black-and-white rules is based on the common assumption that more prescriptive regulations hinder innovation, this assumption is invalid here. Programming is unlike other regulated activities and businesses in that precise specifications are necessary for any successful programming process.[62] Ambiguous and incomplete user specifications lead to unsatisfactory final products.[63] Given

[60] Bundeszentralamt für Steuern. (undated). *ELSTER*. Available from: https://www.elster.de/. [Accessed 28 June 2021]; European Chemicals Agency. (undated). *REACH-IT*. Available from: https://echa.europa.eu/support/dossier-submission-tools/reach-it. [Accessed 28 June 2021]; European Chemical Agency, *Discover REACH-IT*. Available from: https://echa.europa.eu/documents/10162/22308542/discover_reach_it_en.pdf/b0632da6-c7ab-49a5-86c1-761246e75424. [Accessed 28 June 2021].

[61] FRA, Freedom to conduct a business, pp. 37 and 52.

[62] Sommerville, S. (2010) "Chapter 27: Formal Specification," pp. 3-4 and 19. In *Software Engineering* (10th edition). Available from: https://ifs.host.cs.st-andrews.ac.uk/Books/SE9/WebChapters/PDF/Ch_27_Formal_spec.pdf.

[63] Tran, E. (1999, Spring). *Requirements & Specifications*. Available from: https://users.ece.cmu.edu/~koopman/des_s99/requirements_specs/. [Accessed 2 July 2021].

that part of the Commission's "user requirements" in this proposal are sufficient levels of human rights, health, and safety protections, precise compliance specifications are necessary for programmers to correctly implement the law. In addition to ensuring minimum human rights, health, and safety protections, this would also enable public institutions to maintain democratic control over technologies affecting nearly every aspect of EU citizens' lives.

Definitions

Ambiguous terms must be clarified by legally meaningful definitions and operationalisable elaborations. Unlike the word "proportionate," terms like "appropriate," "relevant," "acceptable," and "suitable" lack universally understood legal meanings derived from case law and related sources.[64] Even if these words were legally meaningful, without additional information they would still be too imprecise for the regulation of computer programming that impacts human rights.

For these reasons, the proposal should define terms like "appropriate" with reference to known law. For example, "appropriate" could be defined as "resulting in a degree of interference with fundamental rights that does not exceed what is proportionate to the program's purpose." Though similarly ambiguous, a term of art like proportionality would at least provide an objective starting point for interpreting the legislation. However, as discussed above, what is appropriate or proportionate will vary greatly among AI systems, requiring case-by-case determinations.

This is why providers must always be able to obtain pre-approved specifications that translate ambiguous policy terms into precise programming instructions, or a way to verify their own interpretations. This could take the form of harmonised standards, common specifications, ex-ante third-party conformity assessment, advice from Member State communication channels, a virtual compliance tool, or some other method.

In particular, the phrase "appropriate level of accuracy" in Article 15(1) should be amended to reflect how differing levels of accuracy in use with different demographic groups can result in bias and discrimination.[65] This could be rephrased as: "A high-risk system must have a sufficiently high level of accuracy in each demographic group subjected to the system to avoid violations of any EU Charter right; the variation in accuracy levels when applied to different demographic groups must be low enough to avoid unlawful discrimination." Again, this provision would only be meaningful if a democratically legitimate body with sufficient technical and human rights legal expertise translated it into precise specifications for providers.

Additionally, we ask the Commission to confirm that Article 5(1)(a), which prohibits "subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm," would not expand intermediary liability for platforms hosting harmful but lawful user-generated content. Intermediary liability can severely threaten the freedoms of expression, opinion, and access to information.[66] It thus requires a strong justification, which is absent from the proposal. If the goal is to prohibit targeted advertising and algorithmic prioritisation of sensational or emotive content on social media platforms in order to limit the spread of disinformation, then the Commission should defend this position explicitly in a transparent debate about the Digital Services Act.[67] Whatever its purpose, this provision should be deleted if additional clarification is not provided, given that apparently no one outside the Commission understands what it means.

[64] Proposal, Articles 9(2)(d), 9(4), and 15(1-2).
[65] Mayson, Bias In, Bias Out, pp. 2233-2248.
[66] Council of Europe Commissioner for Human Rights. (2014). *The rule of law on the Internet and in the wider digital world*, pp. 23, 84, and 118. https://rm.coe.int/16806da51c; Electronic Frontier Foundation et al. (2015, March 30). *The Manila Principles on Intermediary Liability Background Paper*. https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf; HRC. (2011, May 16). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, para. 38-43 and 74-75. A/HRC/17/27. https://undocs.org/A/HRC/17/27.
[67] See, e.g., Breyer, P. (2021, May 19). *Draft opinion of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on the Internal Market and Consumer Protection on the proposal for a regulation of the European Parliament and of the Council Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.* 2020/0361, Amendments 32 and 104. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/PA/2021/07-14/1232458EN.pdf.

Issue 2: Biometric surveillance and human rights

While any form of surveillance may endanger human rights, biometric surveillance poses heightened risks due to its potential invasiveness and pervasiveness. Though biometric surveillance appears in Article 5's list of prohibited practices, the prohibition is narrow and its exceptions are wide, leaving only a thin sliver of prohibited uses. While proposed legal safeguards may prevent trivial use and abuse, similar legal requirements have been ineffective in the context of national security surveillance. Additionally, the infeasibility of implementing large-scale biometric surveillance methods in a manner that meets necessity and proportionality requirements may render them inherently incompatible with human rights. Thus, we recommend an absolute ban on large-scale biometric identification, categorisation, and emotion recognition for purposes within the scope of this legislation, or a combination of stronger purpose limitations and stricter legal safeguards.

Problems: Permissiveness, insufficient safeguards, and inherent incompatibility with human rights

Permissiveness

The legislation prohibits biometric surveillance only when it is conducted for law enforcement purposes, operated remotely and in real time, and aimed at the identification of individuals in publicly accessible spaces.[68] It does not prohibit after-the-fact biometric identification by law enforcement. It does not prohibit biometric categorisation, which uses biometric data to assign an individual to categories such as hair colour, ethnic origin, and political orientation.[69] It does not prohibit emotion recognition. It does not prohibit other uses by the state, such as public health surveillance. It does not prohibit biometric surveillance in the workplace, educational institutions, or other semi-private settings in which people spend much of their time.[70]

Even this narrow prohibition is hollowed out by its exceptions. In addition to searches for a specific potential victim of a crime or the prevention of a substantial and imminent threat to human life or a terrorist attack, real-time remote biometric identification by law enforcement is permitted in public spaces to detect, locate, investigate, or prosecute a perpetrator of any crime that justifies a European Arrest Warrant.[71] These crimes include such quotidian offenses as "swindling," computer-related crime, piracy of products, and stolen car trafficking, as long as they may result in a sentence of three years in custody or detention.[72] With the exception of the word "imminent," there are no explicit temporal or geographic limitations. If a missing person remains missing for years or forever, surveillance could hypothetically continue indefinitely.

With such a wide range and scope of permissible uses, a person could be subjected to nearly continuous biometric surveillance throughout their daily life. This poses a significant risk to human rights.

Human rights risks

Biometric surveillance poses a unique set of risks to privacy and other human rights that demand the most stringent legal protections.

---

[68] Proposal, Articles 3(36) and 5(d).
[69] Proposal, Article 3(35).
[70] See, e.g., Organisation for Economic Co-operation and Development (OECD). (2021). *OECD Digital Education Outlook 2021: Pushing the Frontiers with Artificial Intelligence, Blockchain and Robots*, pp. 84-94 and 110. https://doi.org/10.1787/589b283f-en; Samek Lodovici, M. et al. (2021, April). *The impact of teleworking and digital work on workers and society: Special focus on surveillance and monitoring, as well as on mental health of workers*, pp. 55-57. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662904/IPOL_STU(2021)662904_EN.pdf.
[71] Proposal, Article 5(1)(d)(i-iii); *Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States* (2002/584/JHA), Article 2(2). Available from: http://data.europa.eu/eli/dec_framw/2002/584/2009-03-28. [Accessed 2 July 2021].
[72] Decision on the European arrest warrant, Article 2(2).

First, categorisation often involves the processing of, or inferences about, sensitive categories of personal data, such as ethnic origin, which can serve as the basis for discrimination against disadvantaged groups.[73] This is why such processing normally demands heightened legal protections.[74]

Second, the identification of a person in a public space would typically reveal their locations. Location data can be used to infer much about a person, such as political opinions reflected in the protests and meetings they attend, medical conditions based on the medical offices they visit, or social relationships based on the homes they visit. If exploited, this can result in direct violations of a range of human rights, such as the freedom of assembly, as they are exercised.[75] It can also inhibit the exercise of rights by undermining anonymity, which is a precondition to the exercise of multiple human rights.[76]

Third, biometric surveillance allows for more invasive surveillance of psychological and physiological states than other forms of electronic surveillance, thereby dramatically increasing the degree of interference with privacy and other human rights. For example, some employers now attempt to track their employees' psychological states through facial emotion recognition, heart rate monitoring, and other techniques.[77]

This may be incompatible with the right to hold an opinion, for which no interference is permitted by the International Covenant on Civil and Political Rights (ICCPR).[78] The ICCPR prohibits a state from punishing an individual for holding a certain opinion, or coercing an individual into holding an opinion.[79] Positive legal obligations may require states to prevent similar dynamics between employers and employees.[80] UN special rapporteurs and the Human Rights Committee have found that "coercive 'inducements of preferential treatment' may rise to a level of persuasion that interferes with the right to form and hold opinions," without differentiating between public and private actors.[81] This may require states to prohibit the use of emotion recognition software by employers to punish, reward, or make other consequential decisions about employees. At a minimum, AI-based emotion recognition is "highly undesirable," according to the European Data Protection Supervisor (EDPS) and European Data Protection Board (EDPB).[82] They recommend a prohibition, except in narrow circumstances where emotion recognition is important for health or research purposes.[83]

---

[73] See generally, Buolamwini, J. and Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research, 81*, pp. 1-15. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; FRA. (2020). *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, p. 27. Available from: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf; Rhue, L. (2018). *Racial Influence on Automated Perceptions of Emotions.* https://doi.org/10.2139/ssrn.3281765; Burgess. M. (2021, July 7). *Europe makes the case to ban biometric surveillance*. Wired. Available from: https://www.wired.co.uk/article/europe-ai-biometrics. [Accessed 10 July 2021].

[74] *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 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 or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, Article 10(1). Available from: http://data.europa.eu/eli/dir/2016/680/oj. [Accessed 29 June 2021]; *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation), Article 9(1). Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed 29 June 2021]; *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC*, Article 10(1). Available from: http://data.europa.eu/eli/reg/2018/1725/oj. [Accessed 29 June 2021].

[75] FRA. (2020). *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, pp. 29-30. Available from: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

[76] United Nations Human Rights Council (HRC). (2015, May 22). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, para. 16 and 20-21. A/HRC/29/32. Available from: https://undocs.org/A/HRC/29/32.

[77] De Stefano, V. (2020). 'Master and Servers': Collective Labour Rights and Private Government in the Contemporary World of Work. *International Journal of Comparative Labour Law and Industrial Relations, 36*(4), pp. 425-444 (see pp. 34-38). Available from: https://kluwerlawonline.com/journalarticle/International+Journal+of+Comparative+Labour+Law+and+Industrial+Relations/36.4/IJCL2020022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3675082.

[78] *International Covenant on Civil and Political Rights*, Article 19. (1966, December 16). Available from: https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.

[79] HRC. (2011, 12 September). *General comment No. 34*, para. 9-10. CCPR/C/CG/34. https://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf.

[80] Ibid., para. 7.

[81] Kaye, D. et al. (2020, July 7). *Communication, AL CHN 14/2020*, p. 5. Available from: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25374.

[82] European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS). (2020, June 18). *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, para. 35. https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf.

[83] Ibid.

Moreover, given how error-prone and racially biased these programs tend to be, their use to determine whether an employee should be promoted or transferred, for example, could produce unfair or discriminatory results.[84]

Fourth, it is technologically infeasible or impossible to implement large-scale biometric surveillance programs in a way that is proportionate to their purpose and potential human rights harms. In the context of fighting serious crime, the Court of Justice of the European Union (CJEU) found data retention legislation disproportionate when it mandated the retention of all electronic subscriber (identity) and location data of an entire population, without differentiation relating to the purpose of fighting serious crime, without geographic or temporal limitations, and including data pertaining to people not suspected of committing a crime and those who require professional secrecy.[85] Though biometric identification may not involve the retention of data, it features striking parallels in this proposal. Biometric identification can involve the processing of personal data for all people within a given geographic area – perhaps even an entire country – or a given database, including those not suspected of a crime and those requiring professional secrecy, to identify one person.[86] This proposal imposes no specific geographic or temporal limitations on permitted uses, other than general necessity and proportionality standards.[87] Though the legislation envisions Member States sorting out the details of necessity and proportionality, and though Member State surveillance activities are already circumscribed by necessity and proportionality requirements pursuant to the EU Charter, they often ignore or misinterpret the meaning of these standards.[88] Therefore, even if it were technically possible to implement large-scale biometric surveillance in a proportionate manner, it would be unrealistic to expect governments to do so.[89]

Its tendency toward generalised and indiscriminate use, combined with its invasiveness, render large-scale biometric surveillance incompatible with the right to privacy and other human rights. Incompatibility with a right or its essence means a law or practice lacks an element essential to the protection of a right, or it inverts the proper relationship between protection as a rule, and interference as the exception to the rule. According to the Human Rights Committee, an interference with or restriction on a right "may not put in jeopardy the right itself . . . the relation between the right and restriction and between norm and exception must not be reversed."[90] For example, the CJEU has found a surveillance scheme providing an ineffective judicial review mechanism inherently inconsistent with the essence of the right to an effective remedy, irrespective of the scheme's other safeguards.[91] This fundamental flaw was not offset by additional legal protections that did not correct this flaw. A biometric identification system processes the biometric data of all people stored in a dataset or visible to a camera, even if the goal is to identify or locate a specific individual.[92] This arguably makes interference the norm and protection the exception, rendering the practice incompatible with the nature or essence of privacy and data protection rights. This would certainly be true if its use was permitted for nearly unlimited law enforcement purposes. In this situation, the human rights risk assessments in a provider's conformity assessment process would be irrelevant. Just as additional safeguards cannot compensate for ineffective judicial review where the right to a remedy is concerned, no amount of paperwork can compensate for generalised and indiscriminate forms of deeply invasive surveillance where privacy and data protection are concerned.

---

[84] See generally, Murgia, M. (2021, May 12). *Emotion recognition: can AI detect human feelings from a face?* Financial Times. Available from: https://www.ft.com/content/c0b03d1d-f72f-48a8-b342-b4a926109452. [Accessed 3 July 2021]; Purdy, M. et al. (2019, November 18). *The Risks of Using AI to Interpret Human Emotions*. Harvard Business Review. Available from: https://hbr.org/2019/11/the-risks-of-using-ai-to-interpret-human-emotions. [Accessed 3 July 2021]; Rhue, *Racial Influence on Automated Perceptions of Emotions*.

[85] Judgment of 8 April 2014, *Digital Rights Ireland*, Joined Cases C-293/12 and C-594/12, EU:C:2014:238, para. 56-65. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293.

[86] FRA. (2020). *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, pp. 7-8. Available from: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

[87] Proposal, Article 5(2-3).

[88] See generally, Privacy International. (2017, September). *National Data Retention Laws since the CJEU's Tele-2/Watson Judgment*. Available from: https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf; Judgment of 6 October 2020, *Privacy International v. UK*, Case C-623/17, EU:C:2020:790, para. 76-78. https://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=24387800.

[89] Likewise, the EDPS and EDPB find that remote AI-based biometric identification "might present serious proportionality problems, since it might involve the processing of data of an indiscriminate and disproportionate number of data subjects for the identification of only a few individuals," and call for a general ban. EDPB and EDPS, Joint Opinion, para. 30 and 32.

[90] HRC, General Comment 34, para. 21; See also, HRC. (2011, May 16). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, para. 68. A/HRC/17/27. https://undocs.org/A/HRC/17/27 (stating: "the full guarantee of the right to freedom of expression must be the norm, and any limitation considered as an exception . . . this principle should never be reversed").

[91] Judgment of 16 July 2020, *Schrems II*, Case C-311/18, EU:C:2020:559, para. 187. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0311.

[92] FRA, Facial recognition technology, pp. 7-8.

Insufficient legal safeguards

One might argue that the proposal's legal safeguards would prevent abuse and use in trivial circumstances. For law enforcement these include prior judicial or otherwise independent authorisation, necessity and proportionality requirements, and more detailed procedural rules incorporated into Member State law.[93] All uses of biometric identification require two-person confirmation of the identification before an action is taken or a decision made.[94] However, these safeguards may be illusory.

Both the law enforcement agency using real-time biometric identification and the authorising body must consider its necessity and proportionality.[95] In part, they must weigh the relative gravity of the harm investigated and potential human rights interferences resulting from use.[96] This analysis informs the geographic and temporal scope, among other things.[97] However, certain permitted uses, such as the investigation of swindling, are arguably inherently disproportionate to the human rights risks posed by biometric surveillance. Given the gravity of the human rights interference, the FRA recommends that real-time biometric identification be used only in "exceptional" circumstances related to serious crime or terrorism, or to detect missing persons or crime victims.[98] The broad scope of potential uses in the proposal, if replicated in Member State law, would put law enforcement agencies and judges in a contradictory situation, potentially leading to approval for the investigation of commonplace and less serious crimes. Moreover, necessity and proportionality requirements derived from the EU Charter and European Convention on Human Rights are already routinely ignored by Member States in their national security surveillance activities.[99] There is no reason to think this would not continue.

These problems could be mitigated by the requirement for prior judicial or independent authorisation, which is a crucial legal safeguard against the abuse of state surveillance powers.[100] However, the wording of the emergency exception may largely sideline the authorising body. Though it is reasonable to forego prior judicial or independent authorisation in emergency situations, the legislation does not seem to require approval or ratification during or after emergency use. Instead, subsequent authorisation "*may* be requested."[101] One would expect a large proportion of uses, such as the search for a suspect of an imminent terrorist attack, to commence immediately on an emergency basis. This would negate the safeguard. Such ineffective supervisory powers can render a surveillance scheme unlawful, though this would depend on the totality of the circumstances.[102]

Solutions: Absolute ban or strict purpose limitations

As discussed above, large-scale or generalised biometric surveillance methods are likely fundamentally or practically incompatible with human rights law. Use should be prohibited by law enforcement and other public authorities, and also for employee management or commercial purposes. Otherwise, to ensure it is used rarely, the Commission should narrow the scope of potential uses and strengthen legal safeguards against abuse.

Stricter purpose limitations

The purposes for which law enforcement agencies can use real-time remote biometric identification should be narrowed. The reference to European Arrest Warrant crimes in Article 5(1)(d)(iii) should be deleted. In its place, the legislation should permit use only for the identification, location, investigation, and prosecution of suspects, perpetrators, and victims or potential victims of serious violent crimes. This would exclude property crimes like car theft and swindling. The narrowed scope should apply to both real-time and after-the-fact surveillance, as a time delay would not mitigate the impacts of processing

[93] Proposal, Article 5(2-4).
[94] Proposal, Article 14(5).
[95] Proposal, Article 5(2-3).
[96] Proposal, Article 5(2-3).
[97] Proposal, Article 5(2).
[98] FRA, Facial recognition technology, p. 34.
[99] Privacy International, National Data Retention Laws since the CJEU's Tele-2/Watson Judgment, p. 4.
[100] Judgment of 4 December 2015, *Zakharov v. Russia*, Case 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, para. 249. http://hudoc.echr.coe.int/eng?i=001-159324.
[101] Proposal, Article 5(3) (emphasis added).
[102] *Zakharov*, para. 282-285.

sensitive categories of data, location data, psychological and physiological states, or generalised and indiscriminate use.

Also, given that the social benefits of large-scale biometric surveillance in the workplace, educational institutions, and similar settings are even less apparent, it should be entirely prohibited in these contexts.

Stronger legal safeguards

To ensure that the emergency exception to prior judicial or independent authorisation is not abused by law enforcement agencies, Article 5(3)'s "may" should be replaced with "must."

Absolute ban

Without, or possibly despite, these amendments, large-scale biometric identification, categorisation, and emotion recognition would be incompatible with the nature or essence of the right to privacy and other human rights. As such, they should be included in Article 5's list of prohibited practices, without exception.

Conclusion

If the Commission wishes to promote innovation and safeguard fundamental rights affected by AI, and also achieve digital sovereignty and strategic autonomy, it cannot take half measures. The harmonised standard scheme *could* enable providers to adapt general rules to specific high-risk programs, only if it is more responsive. The scheme *could* protect fundamental rights, only if it is better informed by human rights legal expertise. It *could* reduce the undemocratic effects of privatised and technocratic rulemaking, only if all interests affected by AI are represented in decision-making. However, a regulation that creates only a hypothetical possibility of reliance upon European standards, but which effectively forces providers to rely upon self-assessment, would undermine innovation by creating legal uncertainty. It would also squander an opportunity to ensure fundamental rights are adequately protected in AI-related technology, and to reassert democratic control over the technological design decisions that profoundly affect people's lives.

To ensure providers and society at large can benefit from European standardisation, the proposal and the regulation on European standardisation should be amended as outlined above. The two laws should also be considered in tandem in the Commission's new standardisation strategy, to ensure they complement one another.[103]

Also, the contradictory treatment of biometric surveillance must be corrected. The proposal acknowledges the dangers biometric surveillance poses to human rights by placing it on the prohibited use list, but defines prohibited use so narrowly as to allow most uses. It unrealistically assumes that – contrary to other forms of electronic surveillance – Member States will use and govern biometric surveillance in accordance with human rights law. To ensure privacy, data protection, and other human rights legal protections are effective, all large-scale biometric surveillance methods should be prohibited, or at least subject to strict purpose limitations and strong legal safeguards.

These are not merely suggestions for improvements, but rather address structural flaws that – if left unaddressed – will exacerbate problems the Commission intends to remedy.

[103] European Commission. (2021, June 28). Standardisation strategy: Initiative details. Available from: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13099-Standardisation-strategy_en. (Accessed 28 July 2021).

Authors: Christine Galvagna, Tom Niklas Pohlmann, and Chiara Ullstein
Contact: christine.galvagna@thinktech.ngo

www.thinktech.ngo

Thanks to: Gabriel Lindner, Alina Leidinger, Gunnar König, and Svenja Breuer

ThinkTech e.V.
c/o Alexander Ladwein
Situlistraße 71b
80939 München
Deutschland

Sitz und Gerichtsstand: München
Registergericht: Amtsgericht München, Nr. VR208542
Als gemeinnützig anerkannt durch das Finanzamt München

www.thinktech.ngo

Aufsichtsrat: Chiara Ullstein, Vorsitzendende; Gunnar König, Dominik Dahlhaus, Louis Longin
Vorstand: Alexander Ladwein, Vorsitzender und Vorstand (einzelvertretungsberechtigt) i.S.d. § 26 BGB; Julius Morandell, Julia Pfeiffer, Gabriel Lindner