

***Committee of experts on
human rights dimensions of automated data processing
and different forms of artificial intelligence
(MSI-AUT)***

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

12 November 2018

MSI-AUT(2018)06

**Draft Recommendation of the Committee of Ministers to member
States on human rights impacts of algorithmic systems**

Preamble

1. Developments in data analytics and machine learning - collectively understood as techniques of algorithmic or automated data processing – increasingly permeate all aspects of contemporary life. Member States of the Council of Europe must therefore evaluate and address the impacts of the application of algorithmic systems in public and private spheres on the effective exercise of human rights and fundamental freedoms, and for state capacity to secure these rights in line with their obligations derived from the European Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5, “the Convention”).
2. Human rights and fundamental freedoms are universal, indivisible, inter-dependent and inter-related. Given the unprecedented rise in the use of digital services as essential tools of modern communication, news consumption, education, and entertainment, public concern has focused mainly on the right to privacy (Article 8 of the Convention), the right to the freedom of expression (Article 10) and the prohibition of discrimination in accessing Convention rights (Article 14). Yet, the use of algorithmic systems have positive and negative effects on the exercise and enjoyment of all human rights and fundamental freedoms.
3. Algorithmic systems principally operate by detecting and reinforcing patterns in large datasets, and offer the potential to rationalise services and deliver enormous efficiency gains in task and systems performance. This has helped achieve immense progress in categorisation and searchability of information, generating major improvements in fields such as medical diagnostics, transportation and logistics. Advanced technologies play a pivotal role in enabling broader and quicker sharing of information and ideas globally, can strengthen individual autonomy and self-determination, and can enhance human flourishing by creating optimal conditions for the exercise of human rights, notably the freedom of expression and access to information
4. Yet, there are also significant challenges attached to the increasing reliance on algorithmic systems in everyday life. Their functionality is often based on the systematic collection, aggregation and analysis of data collected through fine-grained digital tracking of individuals at scale. When used to automate and inform decision-making, data-driven profiling based on inferred interests and anticipated behaviours may have serious consequences for the individual concerned.
5. Content moderation on online platforms for example, is regularly performed by algorithmic rather than human decision-making, thereby directly affecting the freedom of expression and the right to information, including in contexts of political and electoral campaigning. The automation of decision-making processes in sensitive situations that carry profound weight for individual lives can further lead to the social sorting of financially weak groups and to the disruption of housing and labor markets. In addition, it raises significant concerns about fairness, accuracy, transparency and contestability of decisions.
6. Datasets, which are by nature incomplete, retrospective and constructed, often involve personal information and are thus problematic from a data protection and privacy perspective. A key objective of Convention 108 (ETS No. 108), as modernised, and other data protection frameworks is to empower individuals to understand better and to control the processing of their personal data through automated means. This protection is an essential and integral part of an overall enabling framework for the free flow of data and information which, in other important respects, facilitates

the realisation of human rights and fundamental freedoms, stimulates innovation, and fosters social and economic progress.

7. Data-driven algorithmic systems, however, do not only process and generate personal information and data. They are often designed towards achieving optimum solutions within the given parameters specified by their developers. When operating at scale, such optimisation processes prioritise certain values over others, thereby shaping and disrupting the contexts and environments of broader society and producing effects significantly beyond the rights of data subjects. Whether involving unsupervised, supervised, semi-supervised or reinforcement learning processes, while the basic logic of the various machine learning methods such as the input data, the optimisation target, and the learning model are known to the programmer, the effects that may result on broader environments often remain opaque.
8. Throughout the ongoing process of societal transformation that is fuelled by constant technological advancement, member States of the Council of Europe maintain the obligation to refrain from violating human rights and fundamental freedoms enshrined in the Convention, to establish favourable legislative frameworks to protect and promote the exercise of these rights and freedoms, and to ensure their effective enforcement in line with the rule of law. These obligations include, due to the horizontal effects of human rights, the protection of individuals from adverse activities of private actors, by ensuring their compliance with applicable legislative and regulatory frameworks and by guaranteeing procedural safeguards and access to effective remedies vis-à-vis all relevant actors.
9. Ongoing public and private sector initiatives intended to develop ethical guidelines and standards for the design, development and deployment of algorithmic systems are highly welcome. However, they do not substitute the task for States to ensure that human rights obligations are firmly embedded into all steps of their algorithmic operations, and that adequate legislative and regulatory frameworks are in place to promote human rights-respecting technological innovation by all actors.
10. The development and deployment of algorithmic systems engages many actors, including designers, programmers, data sources, proprietors, sellers, users, providers of infrastructure, as well as public and private institutions. Accordingly, mechanisms of cooperative responsibility and accountability must be established, ensuring that responsibility is effectively distributed throughout all stages of the process, from data collection and analysis, to system modeling and design, through to deployment and implementation. Risk management processes should promote the realisation of public interest goals at all levels and include the possibility of refusing deployment of certain systems when possible harms are considered too grave.
11. Against this background and in order to provide guidance to all relevant actors who are obliged to protect and respect human rights in the contemporary, global and technology-driven environment, the Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe (ETS No. 1), recommends that member States:
 - implement the guidelines included in this recommendation when devising and implementing legislative frameworks relating to algorithmic systems in line with their relevant obligations under the European Convention on Human Rights, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as modernised in the Amending Protocol (CETS No. 223, “modernised Convention 108”), the Convention on Cybercrime (ETS No. 185, “the Budapest

Convention”), the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201, “the Lanzarote Convention”) and the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (CETS No. 210, “the Istanbul Convention”), and promote them in relevant international and regional forums;

- take all necessary measures to ensure that private actors engaged in the design, development and deployment of algorithmic systems fulfill their responsibilities to respect human rights in line with the United Nations Guiding Principles on Business and Human Rights, Recommendation [CM/Rec\(2016\)3](#) of the Committee of Ministers to member States on human rights and business, and Recommendation [CM/Rec\(2018\)2](#) on the roles and responsibilities of internet intermediaries;
- in implementing the guidelines, take due account of Committee of Ministers Recommendation [CM/Rec\(2014\)6](#) on a Guide to human rights for Internet users, Recommendation [CM/Rec\(2012\)3](#) on the protection of human rights with regard to search engines, Recommendation [CM/Rec\(2012\)4](#) on the protection of human rights with regard to social networking services, Recommendation [CM/Rec\(2010\)13](#) on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation [CM/Rec\(2007\)16](#) on measures to promote the public service value of the Internet, and the [2017 Guidelines](#) on the protection of individuals with regard to the processing of personal data in a world of Big Data;
- engage in a regular, inclusive and transparent dialogue with all relevant stakeholders, including from civil society, the private sector, public service media, education establishments, academia, and providers of infrastructure and basic public services with a view to sharing and discussing information and promoting the responsible use of emerging technologies, including different forms of artificial intelligence, that impact the exercise and enjoyment of human rights and related legal and policy issues;
- promote the building of expertise in public and private institutions involved in integrating algorithmic and machine learning systems into lived environments;
- encourage and promote the implementation of effective age- and gender-sensitive media and information literacy programmes to enable all adults, young people and children to enjoy the benefits and minimise the exposure to risks stemming from the use of algorithmic systems in communication networks, in co-operation with all relevant stakeholders, including from the private sector, public service media, civil society, education establishments, academia and technical institutes;
- review regularly the measures taken to implement this recommendation with a view to enhancing their effectiveness.

Appendix to Recommendation CM(x)x

Guidelines for States on actions to be taken vis-à-vis the human rights impacts of algorithmic systems

A – Obligation of states with respect to the protection and promotion of human rights and fundamental freedoms in the context of algorithmic systems

1 General principles

- 1.1 Any law, regulation or policy applicable to the design, development or deployment of algorithmic systems should effectively safeguard human rights and fundamental freedoms as enshrined in the Convention. States should provide a positive environment for the exercise of human rights and fundamental freedoms, and should ensure that the use of algorithmic systems does not impair the protection and enforcement of rights under the Convention and modernised Convention 108.
- 1.2 In their design, development and deployment of algorithmic systems, States should be mindful that their human rights obligations remain unaltered. All processes or decisions taken or aided by algorithmic systems and significantly affecting access to or exercise of human rights, should be identifiable as such, and should remain explainable and their deployment and substance contestable to an informed human reviewer. This commitment extends to all stages of algorithmic processing, from data collection to training, developing, selling, and applying an algorithmic processing system. Relevant technology developed by public funds should be open source.
- 1.3 States should ensure that all design, development and deployment of algorithmic systems provides an effective possibility for individuals to exercise the right to abstain from computational experimentation - either through their action or inaction.
- 1.4 States should ensure that all design, development and deployment of algorithmic systems provides an avenue for individuals to exercise a right to obfuscation (the deliberate addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection projects), recognising that this is a valid form of expression and that there is no obligation on humans to make themselves legible to automation.
- 1.5 All production and deployment processes should embed safety and security concerns, and implement measures to internalise possible externalities and other unintended effects that may adversely impact the exercise of human rights by directly and indirectly affected individuals, as well as negative externalities or other adverse impacts on lived environments.
- 1.6 The process of enacting legislation or regulation applicable to the design, development and deployment of algorithmic systems should be transparent, accountable and inclusive. States should regularly consult with all relevant stakeholders with a view to safeguarding the interests of individuals and affected parties, and to ensuring that potential negative effects on the exercise of human rights are prevented or mitigated. Legislative frameworks should help build trust in order to drive innovation and prevent damage being caused by “free-riding” of harmful actors.
- 1.7 States should identify appropriate institutional, regulatory and standards frameworks which may include independent offices of technical expertise that set benchmarks and safeguards to oversee

the design, development and deployment of algorithmic systems in the public sphere. These efforts should ensure that possible direct or indirect human rights risks can be promptly identified and adequate remedial action initiated, including review processes, repair and possible abandonment of measures. States should invest in adequate expertise to be available in relevant regulatory authorities, as well as in guaranteeing close co-operation and inclusive dialogue with universities and non-governmental organisations of diverse backgrounds (e.g., geographical, size, focus). Such frameworks may be informed by models from other sectors, including pharmaceutical development, sales of mechanical engineering products, and foodstuffs.

2 Data quality

- 2.1. States should ensure that all data that are used by them in the design, development and deployment of algorithmic systems are effectively and regularly tested against state of the art standards related to bias, completeness, relevance and the possibility of privacy leakages. Standards should be designed and applied for labelling provenance and quality assessment of datasets.
- 2.2. States should carefully assess what human rights may be affected as a result of the nature of the data, which may stand in as a proxy for classifiers such as gender, class, race or ethnicity. The shortcomings of the dataset, the possibility of its inappropriate use, and the externalities resulting from these shortcomings and inappropriate uses, should equally be assessed carefully. Based on these assessments, States should take appropriate action to effectively minimise adverse effects.
- 2.3. Data controllers and, where applicable, processors, should carefully curb the design of their data processing to what is strictly necessary for the purpose for which it is being processed, and minimise the presence of redundant or unreliable data, with a view to avoiding negative impacts on human rights and fundamental freedoms.
- 2.4. Bias and potential discrimination in datasets and algorithmic processing should be regularly evaluated and responded to, ensuring that efforts to combat bias and discrimination do not compromise the human right to privacy and freedom from unwanted surveillance. This concern applies in particular to technologies such as facial recognition and other biometric applications that may be used for the purposes of identification.

3 Data analysis and modelling

- 3.1 States should thrive to ensure that all their data analysis and modelling of algorithmic systems that may profoundly affect the exercise of human rights is designed towards minimising negative impacts and maximising benefits for individuals and society. Evaluation before and after deployment should be part and parcel of these efforts and should include an evaluation of the desirability and legitimacy of the goal that the system intends to achieve or optimise.
- 3.2 States should ensure that the adequacy of algorithmic systems is tested and evaluated on a limited amount of data, before being deployed on a larger scale. These tests should be informed through a diverse stakeholder process and take due account of the externalities of the proposed system (e.g., distribution of errors in terms of both false positives and false negatives) before and after deployment.

3.3 The evaluation and testing of algorithmic systems should be performed with diverse sample populations and not draw on or discriminate against any particular demographic group. Development of algorithmic systems should be discontinued if testing or deployment involves externalising risks on to individuals, groups, populations and their environments.

4 Transparency and contestability

4.1 States should be transparent regarding all aspects of their use of algorithmic systems in the delivery of public services, following the principle of ‘public money, public code’. States should ensure that when decisions are taken or aided by an algorithmic system, the existence of the system, the criteria that were applied in the collection, analysis, and modelling of relevant data, and the system’s optimisation goals are visible to affected individuals, groups, populations and institutions.

4.2 The right to contest relevant determinations and decisions before a competent authority should be afforded to individuals and groups that are impacted directly or indirectly by algorithmic systems and should include the right to have determinations and decisions reconsidered, remade, and justified through reasoning that does not rely on algorithmic systems. The right to contest may not be waived.

4.3 As a necessary precondition of contestability, the existence, operation, and possible outcomes (or reasoning) of algorithmic systems should be explained in neutral terms to individuals whose rights are affected, as well as to relevant public authorities. This information might usefully be provided by means of an interface that simulates data inputs and their potential impact on the individual, in a learn-from-experience approach. In addition to these sources of explanation, those that develop and apply algorithmic systems should provide publicly-accessible evidence of actions taken to identify, document, and mitigate adverse human rights effects.

4.4 States should ensure that adequate oversight is maintained over the number and type of contests made by affected individuals or groups against certain algorithmic systems with a view to ensure that the results do not only lead to remedial action in the specific case but are also fed into the systems themselves so as to avoid repetitions, seek improvement, and possibly discontinue the introduction or ongoing deployment of certain systems due to their human rights risks.

4.5 States should ensure that processes to meaningfully contest algorithmic systems are accessible, affordable, effective, and available before, during and after deployment, including through the provision of contact points and hotlines.

5 Effective remedies

5.1 States should guarantee accessible and effective judicial and non-judicial procedures that ensure the impartial review, in compliance with Articles 6 and 13 of the Convention, of all claims of direct and indirect violations of Convention rights through the use of algorithmic data processing, decision-making or optimisation systems.

5.2 States should guarantee an effective remedy for all violations of human rights and fundamental freedoms set forth in the Convention by private actors engaged in the design, development and deployment of algorithmic systems, in compliance with Article 13 of the Convention. Through their legislative frameworks, they should ensure that individuals and groups are afforded with access to

prompt, transparent, functional and effective remedies with respect to their grievances, including apology, rectification or compensation for damages. Judicial review should remain available, when internal and alternative dispute settlement mechanisms prove insufficient or when the affected parties opt for judicial redress or appeal.

- 5.3 States should proactively seek to reduce all legal, practical or other relevant barriers that could lead to directly or indirectly affected individuals and groups being denied an effective remedy to their grievances. This includes the necessity to ensure that adequately trained staff is available to competently review the case and take appropriate action.
- 5.4 States should consider digital and information literacy as an essential citizen skill. All curricula and modules in formal and non-formal education systems should promote, in an age and gender-sensitive manner, basic understanding of the functioning of algorithmic systems and of the human rights risks stemming from their use in everyday life, ensuring that all users are effectively made aware of their rights and freedoms. Particular attention should be paid to their right to an effective remedy vis-à-vis both State authorities and private actors engaged in the design, development and deployment of algorithmic systems.

6 Precautionary measures

- 6.1 States should utilise the mechanism of procurement or engagement of private services in public service delivery to maintain relevant oversight, ownership, and control over the use of algorithmic systems, and should publicly account for their efforts in this regard. In all their actions, they should seek to ensure that the design, development or deployment of algorithmic systems does not have direct or indirect discriminatory effects or harmful impacts on individuals or particular groups, including on those who have special needs or disabilities or may face structural inequalities in their access to human rights.
- 6.2. States, as well as any private actors engaged to work with States, should conduct regular publicly accessible and expert-informed human rights impact assessments prior to public procurement, during development, at regular milestones, and throughout the use of algorithmic systems in the contexts in which they are deployed, to identify risks of rights-adverse outcomes. Since algorithmic systems can fundamentally transform the quality and governance of lived environments as well as societal institutions, impact assessments should include an evaluation of the transformations that algorithmic systems may bring upon these environments and institutions and their structural impact on the exercise of human rights.
- 6.3. States should adopt appropriate measures to avoid and mitigate human rights risks identified through impact assessments and should conduct dynamic testing methods and pre-release trials, ensuring that potentially affected groups as well as relevant field experts are included as actors with decision-making power in the design, testing, and review phases. States should ensure that private actors who seek to deploy algorithmic systems that may profoundly affect the exercise of human rights, are mandated to conduct such impact assessments prior to and during deployment. Algorithmic systems should be submitted for independent expert review, and create tiered processes for independent oversight, including by judicial authorities when necessary.
- 6.4. With a view to enhancing compliance, States should ensure that the legal and regulatory framework in place to address and mitigate the human rights risks related to the design, development and

deployment of algorithmic systems are effectively enforced in line with rule of law standards. Legislation in place to allocate responsibility for harm caused by algorithmic systems should be non-derogable and may not be averted by invoking the co-responsibility of others.

- 6.5. States should adopt diverse hiring practices and engage in consultations to assure diverse perspectives that are not limited to technical expertise so that those involved in the design, implementation, and review of algorithmic systems represent a range of backgrounds and identities and are able to engage with the technologies effectively, critically, and with consideration of the broader context.
- 6.6. States should engage in inclusive, inter-disciplinary, informed and public debates to define what areas of public services profoundly affecting access to or exercise of human rights may not be appropriately determined, decided or optimised through algorithmic systems.
- 6.7. States should ensure that all staff involved in the procurement, development, application, and review of algorithmic systems are adequately trained with respect to applicable human rights norms and are aware of their duty to ensure not only a thorough technical review but also human rights compliance.

7 Empowerment through research and public awareness

- 7.1. States should promote the development of algorithmic systems and technologies that enhance the equal access to and enjoyment of human rights and fundamental freedoms through the use of tax, procurement, or other incentives. This may include the development of algorithmic systems to address the needs of disadvantaged and underrepresented populations.
- 7.2. States should engage in and support independent research aimed at assessing, testing and advancing the potential of algorithmic systems for creating positive human rights effects and for advancing public benefit. This may require the anticipation and possible counteracting of market forces that may exclusively favour commercially most viable optimisation systems.
- 7.3. States should promote innovative design and development of algorithmic systems in line with existing human rights norms, in particular with respect to social rights and internationally recognised labour and employment standards.
- 7.4. States should promote technological development and innovation to enhance internationally agreed sustainable development goals and address existing environmental challenges, such as through initiatives towards 'fair and aware innovation'.
- 7.5. States should encourage independent research into the development of effective accountability mechanisms and solutions to existing responsibility gaps related to opacity, inexplicability and related incontestability of algorithmic systems.
- 7.6. States should investigate strategies to protect and decentralise data assets, as well as to invest in data processing infrastructure. This endeavour is essential to ensure the independence and vitality of the public and private sector, to promote the design and development of algorithmic systems in the public interest, to prevent dependencies, and to curb concentration of market power.

7.7. States should support the independence of institutions in education, healthcare, the media, and other relevant domains, as well as of civil society and rights organisations as an important counterweight to the power of those that own and develop algorithmic processing technologies, and as a crucial element of trust and accountability. States should reward and support those who knowledgeably and intelligently address algorithmic processing, especially in less well-understood domains.

B. Responsibilities for private actors with respect to human rights and fundamental freedoms that member States should aim to ensure

1 General principles

1.1. Private actors engaged in the design, development, sale, deployment and servicing of algorithmic systems, whether in the public or private sphere, have the responsibility to respect internationally recognised human rights and fundamental freedoms of their customers, be they legal entities or individuals, and of other parties who are affected by their activities. This responsibility exists independently of the States' ability or willingness to fulfil their human rights obligations. As part of fulfilling this responsibility, private actors should take on-going, proactive and reactive steps to ensure that they do not cause or contribute to human rights abuses and that their innovation processes are human-rights friendly.

1.2. The responsibility of private actors to respect human rights and to employ adequate measures applies regardless of their size, sector, operational context, ownership structure or nature. The scale and complexity of the means through which they meet their responsibilities may vary, however, taking into account their means and the severity of potential impact on human rights by their services and systems.

1.3. The actions taken by private actors should serve to build their trustworthiness with the individuals that will both use and be subjected to the processes of algorithmic systems. Individuals must be empowered with the choice to give and revoke free and informed consent, to know how their data is being used, to know the personal impact and consequences of algorithmic determination, decision-making and optimisation processes, to know how to contest, and to know that their rights are being safeguarded by the entities in which they place their trust.

2 Data quality

2.1. Private actors should collect data based on reliable and diversified sources and in secure technological environments. All datasets should be regularly tested against bias, completeness, relevance and privacy leakages, and appropriate action taken to effectively minimise adverse effects.

2.2. All processing, including collection, retention, aggregation, storage, adaptation, alteration, linking, sharing or migrating across multiple devices, of personal data, shall be based on the free, specific, informed and unambiguous consent of the data subject, with respect to a specific purpose, or on another legitimate basis laid down by law. Consent rules for the use of tracking, storage and performance measurement tools must be clear, simply phrased, and complete, ensuring that explanations go beyond mere assertion to the effect that "services are being improved".

- 2.3. Private actors should embed “privacy by default” and “privacy by design” principles in all development and deployment of their algorithmic systems. Customers should maintain the right to effectively protect their privacy while maintaining access to services, including through the possibility of choosing from a set of privacy setting options, presented in an easily visible, neutral and intelligible manner, with the default being the most privacy protective. This does not preclude private actors from adjusting their business model to requiring payment for certain services that are otherwise offered free of charge.
- 2.4. Private actors should ensure that all data related rights of their customers, including the right to access their personal data and to obtain correction, deletion or blocking, are clearly and plainly communicated to them in a language they understand. These rights may not be waived or diminished, including not by terms of service conditions.

3 Data analysis and modelling

- 3.1. Private actors should ensure that all their data analysis and modelling activities meet technical checks and auditing for quality assurance, and are regularly tested against their safety and security standards. Testing should be performed not only with respect to the algorithmic output but also the goal which the system is intended to achieve or optimise, the criteria according to which the data are processed, analysed and modelled, and regarding possible standard deviations of the results produced.
- 3.2. Private actors should consider human rights, social and ethical considerations in all design, of algorithmic systems, in line with the concept of ‘human rights by design’. The goals of algorithmic and machine learning systems should not create self-fulfilling markers of success that are based on and therefore reinforce patterns of inequality, arising, for instance, from using non-representative, biased, or outdated datasets.
- 3.3. Private actors should ensure that all staff tasked to oversee human rights, social and ethical compliance in the design, development and deployment of algorithmic systems are adequately trained and aware of their responsibilities with respect to human rights, including but not limited to applicable personal data protection and privacy standards.
- 3.4. Private actors designing or using software that enables the retrieval and presentation of information online should configure the software in such a way that it offers the option of preventing third parties from storing information on the device of the customer.

4 Transparency and contestability

- 4.1. Private actors should ensure that the use of algorithmic systems in the products and services they offer is made visible to all customers, whether individual or legal entities, as well as to the general public. New customers or customers of products and services whose application rules have been amended should be notified of all relevant changes.
- 4.2. Private actors should seek to promote the explainability of all algorithmic systems they use in their products and services towards their customers and towards the general public, thereby enhancing their overall trustworthiness. This entails that all information is made available in easily understandable language and accessible formats. It further implies that information goes beyond

mere “input – output” statements and that it provides relevant insight into the actual processes themselves, as well as their optimisation goals.

- 4.3. Private actors should make publicly available information about the number and type of contests made by affected individuals or groups regarding the products and services they offer, with a view to ensuring that the results do not only lead to remedial action in the specific case but are also fed into the systems themselves to draw lessons from complaints and correct errors before harm occurs at massive scale. Individuals and groups should be allowed not only to contest but also to make suggestions for improvements and provide other useful feedback, including with respect to areas where human review is systematically required.
- 4.4. In order to facilitate meaningful contestability, private actors should ensure that human reviewers remain accessible with respect to all algorithmic systems and that direct contact with a human reviewer is made effectively possible, including through the provision of contact points and hotlines. Customers should be actively encouraged through open and transparent processes to seek explanations and make use of their right to contest in the first place.

5 Effective remedies

- 5.1. Private actors should ensure that effective remedies and dispute resolution systems are available both online and offline to customers, both individuals and legal entities, who wish to report a violation of their rights. The scope of available remedies may not be limited, such as to exclude errors that occur during transition periods while changes to the system take effect, or to breaches of the terms of service only. All remedies should allow for an impartial and independent review, should be handled without unwarranted delays and should be conducted in good faith, with respect for due process guarantees. Relevant mechanisms should not negatively impact the opportunities for complainants to seek recourse through independent national, including judicial, review mechanisms.
- 5.2. Private actors should ensure that all customers and other parties affected by their actions have full and easy access to transparent information in clear and easily understandable language about applicable complaint mechanisms, the various stages of the procedure, the exact competencies of the contact points, indicative time frames and expected outcomes.
- 5.3. Private actors may not include in their terms of service waivers of rights or hindrances to the effective access to remedies, such as mandatory jurisdiction elsewhere or non-derogable arbitration clauses.
- 5.4. Private actors should actively engage in participatory processes with consumer associations, human rights advocates and other organisations representing the interests of customers and affected parties, as well as with data protection and other independent administrative or regulatory authorities, for the design, implementation and evaluation of their complaint mechanisms. Business associations should further invest – in cooperation with trade associations – in the establishment of model complaints mechanisms.
- 5.5. All staff involved in the handling of customer complaints should be suitably versed in relevant human rights standards and benefit from regular training opportunities.

6 Precautionary measures

- 6.1. Private actors should develop internal processes to ensure that all design, development and deployment of algorithmic systems is evaluated and tested not only against possible technical errors but also against the potential legal, social and ethical impacts that the systems may carry. Human rights impact assessment should particularly be conducted prior to any deployment, not only at the individual level but also in terms of externalised risks for societal environments, and with the participation of experts from different fields. All staff involved in the review of algorithmic systems should be adequately trained with respect to applicable human rights norms and made aware of their specific responsibilities.
- 6.2. Private actors should ensure appropriate follow-up to their human rights impact assessments by taking adequate action upon the findings with a view to avoiding or mitigating adverse effects on and risks for the exercise of human rights, and by monitoring and evaluating the effectiveness of identified responses.
- 6.3. Human rights impacts assessments should be conducted as openly as possible and encourage active engagement of customers. The results of any risk assessment process, identified techniques for risk mitigation, and relevant monitoring and review processes, should be made publicly available, without prejudice to secrecy safeguarded by law. In the presence of such secrecy, any confidential information should be provided in a separate annex to the assessment report. This annex shall not be public, but should be accessible by relevant supervisory authorities.
- 6.4. When the application of algorithmic systems may profoundly affect the rights and fundamental freedoms of individuals, including in processes of unsupervised machine learning where causality of possible impacts may be difficult to establish, private actors should consult supervisory authorities in all relevant jurisdictions to seek advice and guidance on how to manage these risks. Private actors should submit these algorithmic systems for regular independent expert review, and create tiered processes for independent oversight, including by judicial authorities when necessary.
- 6.5. Private actors should provide their products and services without any discrimination. They should seek to ensure that the design, development or deployment of their algorithmic systems do not have direct or indirect discriminatory effects or harmful impacts on individuals or particular groups, including on those who have special needs or disabilities or may face structural inequalities in their access to human rights.
- 6.6. Private actors engaged in providing algorithmically run services should take reasonable and proportionate measures to ensure that their terms of service agreements are applied and enforced consistently and in compliance with applicable procedural safeguards.
- 6.7. Private actors should track their response to human rights issues that emerge during implementation and over time, including evaluation of the effectiveness of responses. This requires regular and ongoing quality assurances checks and real-time auditing through design, testing, and deployment stages to monitor a system for human rights impacts in context and in situ, and to correct errors and harms as appropriate, including with respect to unintended harms. This is particularly important given the risk of feedback loops that can exacerbate and entrench negative outcomes.

7 Empowerment through research and public awareness

- 7.1. Private actors should engage in and support independent research aimed at assessing, testing and advancing the potential of algorithmic systems for creating positive human rights impacts and for advancing public benefit. This may include the development of algorithmic systems to address the needs of disadvantaged and underrepresented populations.
- 7.2. Private actors should provide relevant individual and meta-datasets as well as access to data that has been classified for deletion to independent researchers and academics engaged in analysing the impacts of algorithmic systems and digitalised services on the exercise of rights, on communication networks, and on democratic systems.
- 7.3. Private actors should promote innovative design and development of algorithmic systems in line with their responsibilities to respect human rights and in particular with respect to social rights and internationally recognised labour and employment standards, including in the context of 'fair and aware innovation' initiatives.
- 7.4. Private actors engaged in the design, development and deployment of algorithmic systems and related services should engage in and promote targeted age- and gender-sensitive efforts to promote public awareness of relevant rights, including in particular, information about applicable complaint mechanisms and procedures.