

**Contribution of the Republic of Slovenia**

**to the Questionnaire on the right to privacy in the digital age**

**Thematic report on 'The right to privacy in the digital age' prepared by the Office of the United Nations High Commissioner for Human Rights**

28 May 2021

|  |
| --- |
| **Questionnaire of the Office of the United Nations High Commissioner for Human Rights on the impact of the artificial intelligence (AI) on human rights and the right to privacy** **Contribution of the Republic of Slovenia** |

**1. The response of the Ministry of Agriculture, Forestry and Food:**

With regard to “Human Rights Council Resolution 42/15 on the right to privacy in the digital Age”, please find below our response.

The introduction of new technologies, including the AI, represents both an opportunity and a challenge in the field of agriculture. The concept of the digitalisation of agriculture includes everything from the systems of precision farming, robotisation and automation, connectivity, virtual services and digitalisation of supply chains, to systems and tools for decision-making support (artificial intelligence, big data). Their aim is to increase the efficiency of agricultural practices with a potentially reduced or changed workforce and the timeframe of operations and business processes and, at the same time, with reduced environmental impacts and the potential revitalisation of rural areas. In relation to this, there are two important focal points:

– more flexible (agile) and advanced systems need new knowledge and competencies (IT experts, advisors, service providers, social networks and media, the use and supervision of communication channels, etc.) and require a different and complex network of partners and stakeholders. They also require a change in performance/ activities, while constantly introducing new changes,

– taking into account the goal of sustainable development and green transition to digitalisation, with exposed conflict between the goals of the ambitious agricultural and environmental policy, the agricultural sector has not yet developed a fast enough, sufficient and appropriate operational response to the rapid development by introducing new tools and technologies in the new digital age.

In this respect, we note that:

* There are several types of several levels digital platforms and unrelated applications and portals (FAO's Platform for Digital Food and Agriculture, national platform Our Super Food, FoodPlus and other platforms on food waste, Horizon 2020, Smart Villages, the AKIS platform, EIP projects, etc.);
* Rules and obligations in the legislative framework of agricultural, forestry, food and fisheries policy and broader have been amended, changed, adapted and are constantly changing (e.g. the Common Agriculture Policy system (CAP), based on beneficiaries receiving funding from the European Agricultural Guarantee Fund and the European Agricultural Fund for Rural Development, the Common Fisheries Policy system (CFP), where the beneficiaries receiving funds form the European Maritime, Fisheries and Aquaculture Fund). At the same time, the high expectations of institutions and the interested and general public (consumers) following the inclusion of the objectives of agendas and guidelines in the legislative framework of the CAP reform package and the CFP (2030 Agenda for Sustainable Development, European Green Deal, Farm to Fork Strategy, Biodiversity Strategy, CAP Strategic Plan, etc.) are reflected as a strong pressure for transforming the policies and systemic values;
* Different forms of incentives and means for the use of new methods and tools (digitalisation) that encourage the use of e-services (data analysis, data mining tools – Arachne, etc.) are introduced;
* The trend in the age structure of Slovenian population is steadily growing;
* There are white and grey areas in the national plan for the development of broadband networks;
* Interdisciplinary and competent working groups must be included in the implementation of solutions that are based on the use of new mechanisms and tools laid down in the rules for the implementation of policies (e.g. CAP and CFP in the 2021-2027 period), and the interoperability of systems must be guaranteed at the national level;
* It is a fundamental shift from a descriptive to operational model; that is from the compliance model to the performance based model, from strategies to action;
* General knowledge and awareness on AI and its impact is low.

Already in 2020, the Council of Europe called on the Member States to take a precautionary approach to the development and use of algorithmic systems and adopt legislation, policies and practices that fully respect human rights. The Recommendation on the human rights impacts of algorithmic systems includes a set of guidelines calling on governments to ensure that they do not breach human rights through their own use, development or procurement of algorithmic systems. As regulators, they should establish effective and predictable legislative, regulatory and supervisory frameworks that prevent, detect, prohibit and remedy human rights violations, whether stemming from public or private actors.

According to a rough analysis of the impact of AI on human rights and the right to privacy, with a focus on agriculture, forestry, food and fisheries, we stress:

* That states should carry out a comprehensive risk assessment for human rights in the digital age, including the review and assessment of the existing legislation (GDPR, the ePrivacy Directive, the Open Data Directive, etc.) and establish a common fundamental denominator. EU framework for a horizontal integration of AI that would have to complement a horizontal act on AI and other sectoral legislation. That a synchronised interpretation of rules and initiatives that will be implemented at the national and EU level and beyond is of utmost importance;
* The absence of the high-risk level with the definition of critical processes, procedures and applications that include AI and its potential risks. Since standard approaches on the basis of analyses and risk assessments do not fully cover the dimensions of all ethical implications and consequences, it is necessary to establish/upgrade the system for managing the constant changes and monitoring the effects of corrections;
* The need for an interdisciplinary cooperation between experts with a contextualisation (taking into account the policy and geographical area, cultural and other specifics) and developing information models of policy aspects that would take into account the needs of the digital age;
* That since data management addresses a huge potential that will affect the lives of all of us – from the point of view of technology drivers, defined by progress and use –, Europe needs to be prepared and take advantage of all competitive benefits. There is a strong need for raising awareness and strengthening the knowledge of the general public (the understanding of the concept, the functioning and the consequences of the introduction of AI into our lives);
* A need for standardisation: the availability and transparency of data and the use of sources and processes will be key factors for an appropriate use, management and supervision of AI;
* Building the trust of users in the system based on ensuring the security in the exchange and re-use of data, also taking into account the privacy policy (based on the consent of a user to create certain profiles – biometric data, preserving the rights and freedoms...), and a positive experience of users, contrary to creating the standard of the »Social credit System« (that calls for the establishments of unified record system for individuals, businesses and the government to be tracked and evaluated for trustworthiness and that seeks complete control of individuals/citizens);
* the obligation of the state to establish healthy management and a regulatory environment for facilitating the use of data and digital technologies for the creation of policies and mechanisms for their implementation as well as for other purposes (taking into account the risks);
* The integration of new knowledge in education process and the data literacy of citizens, aiming for better understanding of the impact of AI and data practices and their consequences.

The creation of “red lines” in connection with human rights and the rights to privacy depends primarily on the level of development and profile of the state, which defines and enforces the rights, and its citizens. The basis for the protection of human rights are clearly defined competences and the responsibility for preventing the violations of (current?) human rights as consequences of violations throughout the entire chain. These are the obligations of states in relation to the protection and promotion of human rights and fundamental freedoms as the responsibilities of actors from the private sector in relation to human rights and fundamental freedoms in the framework of algorithmic systems.

**2. The response of the Institute of Criminology at the Faculty of Law Ljubljana:**

In the excerpts below, you can find our insight regarding the issues addressed for the preparation of the thematic report, which mainly focuses on our **particular areas of interest**. In or research, we predominantly focus on how **judicial systems** change on a national and international level with the increased use of information and communication technology (ICT), including artificial intelligence (AI), in order to analyze how automation could be beneficial to the decision-making process on the one hand and what risks it poses to human rights and other fundamental values on the other.

The potential uses and benefits of new and emerging digital technologies contain threats to human rights and demand the change of regulatory regime. The developments in AI must therefore take place in an appropriate legal and ethical framework, which will reinforce the existing levels of respect for human rights (this proves to be particularly important for the prevention of violations of the right to privacy) and fundamental freedoms of every individual and vulnerable social group and consolidate legitimate democratic processes. Our answer concentrates on the uses of new tools in the **crime and security domain** and ways to mitigate the accompanying risks since this is the main field of research of our institution, explored in the following **research projects**:

* Automated Justice: Social, Ethical and Legal Implications (Slovenian Research Agency, 2018 -2021),
* Law in the Age of Big Data (Slovenian Research Agency, 2014 -2017),
* Human Rights and Regulation of Trustworthy Artificial Intelligence (Slovenian Research Agency, 2019 -2021).

The excerpts in the following answer are taken from the undermentioned **articles/chapters**:

1. Mojca Mihelj Plesničar, Aleš Završnik & Pika Šarf. (2020). Fighting impunity with new tools: how big data, algorithms, machine learning and AI shape the new era of criminal justice, in: Luisa Marin, Stefano Montaldo (eds.), The Fight Against Impunity in EU Law. <https://doi.org/10.5040/9781509926909.ch-014>
2. Aleš Završnik. (2019). Criminal Justice, Artificial Intelligence Systems, and Human Rights. *ERA Forum – Journal of the Academy of European Law*, Springer, <https://doi.org/10.1007/s12027-020-00602-0>
3. Aleš Završnik. (2019). Algorithmic justice: Algorithms and big data in criminal justice settings. *European Journal of Criminology*

<https://doi.org/10.1177/1477370819876762>

Given the modern criminal justice system’s incessant stride for objectivity, it is of little surprise that criminal justice begun utilising the emerging technologies in various contexts and various ways. The application of ICT in judicial processes has enabled more effective case management, availability of case-law through online search engines (e. g. HUDOC, E-justice portal), online dispute resolution mechanisms, advanced legal analytic tools as well as faster and easier communication between all parties involved. Above all, the digital environment is producing the data, which is necessary to fuel further development and predictive ability of algorithmic tools.

Several **stakeholders** in the crime and security domain are currently using new tools:

1) intelligence agencies, which have been increasingly focusing on the surveillance of public telecommunications networks (e.g. as revealed by Edward Snowden in 2013);

2) law enforcement agencies, which are increasingly using crime prediction software such as PredPol (Santa Cruz, California), Precobs (Zürich, Munich), and Maprevelation (France);

3) criminal courts and probation commissions predicting recidivism; and

4) administrative agencies and inspectorates, e.g. tax and customs authorities, environmental and food inspection services, which use the new tools to do their work more effectively.

Listing possible actors in the chain of building and employing AI systems may also lead to all-encompassing lists of **state and private sector actors**. The deepening of the digital ecosystem has lead to a situation where responsibilities are becoming increasingly spread to a number of dependant actors. We can map responsibility in several ways:

from the obligations of states to the obligations of the private sector; from data preparation to writing algorithm code (how data is cleaned and prepared, which data is taken in and used, and which data is left out of the calculus, etc.); from algorithmic design and development to implementation processes, etc. With the deepening of the digital ecosystem it becomes much more burdensome to determine who is responsible for certain data intake and algorithmic output. The acts committed might not even reach the existing **thresholds of accountability**. It may even be unjust to hold an actor accountable for the consequences of activities that are generally of great benefit to a society. An actor may be generating a risk our societies are willing to accept as “socially permissible risk”.[[1]](#footnote-1)

Some of the proposed uses for **crime-preventive purposes** are outright outrageous and directly dangerous in terms of fundamental liberties. The controversial software promising to infer criminality from face images,[[2]](#footnote-2) for example, illuminated some of the deep-rooted misconceptions about what crime is, how it is defined, prosecuted and adjudicated. The once ridiculed phrenology from the 19th century hence entered the 21st century in new clothes as “algorithmic phrenology”, which can legitimise and normalise deep-rooted implicit biases about crime.[[3]](#footnote-3) In the near future, further steps along the line of the corporal importance of one’s body for crime control are reasonably to be expected: from analysis of walking patterns, posture and face recognition for identification purposes (e.g. Facebook’s DeepFace program) to analysis of facial expressions for emotion recognition.

The described types of **predictive policing** have incited a considerable level of concern among scholars, who have addressed “the rise of predictive policing” [[4]](#footnote-4) and the “algorithmic patrol”[[5]](#footnote-5)  as the new predominant method of policing that in turn affects other methods of policing. A common concern is the allure of objectivity, as well as the creative role police still have in producing inputs for automated calculations. Country-specific studies on predictive policing exist in Germany[[6]](#footnote-6), France[[7]](#footnote-7), Switzerland[[8]](#footnote-8), and the UK[[9]](#footnote-9).

**Criminal justice systems** are fragile environments based on several fundamental principles under attack from many different sources. While promising and potentially beneficial to the system, new technology is definitely one of such potential threats as well. Important considerations about fundamental human rights – such as the right to privacy – may and should arise when we discuss its use and implications in criminal justice system. Before introducing algorithms in any decision-making process, let alone in criminal procedures, it is therefore essential to ensure compliance with fundamental human rights enshrined in the European Convention on Human Rights (ECHR)[[10]](#footnote-10) and the Charter of Fundamental Rights of the European Union (the Charter),[[11]](#footnote-11) as well as with the relevant data protection law.

In the EU General Data Protection Regulation (henceforth GDPR)[[12]](#footnote-12) and Law Enforcement Directive set a high standard for data protection which builds on principles of data minimization, purpose limitation, legality, fairness and transparency. In cases of automated processing, the data controller must implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, for instance by ensuring him or her the right to obtain human intervention, to express his or her point of view, and to contest the decision (Art. 22, para. 3 of the GDPR). GDPR includes the right of the data subject to receive ‘meaningful information about the logic involved’ in automated processing. (See Arts. 13, 14, and 15.).

The increase in the use of **face recognition technologies**, such as the tool offered by a start-up Clearview, is a pressing issue, especially in terms of the protection of the right to privacy and data protection. The use of face recognition technologies in law enforcement can only be permissible when in compliance with the principle of proportionality, while considering that the objective pursued by its use is appropriate, meaning that the use of such applications to prosecute petty crime is unlikely to be justified. A very important aspect to consider in this case is a need for increased transparency, which would contribute to better and fairer decisions, and cause the general public to see the use of artificial intelligence as legitimate and trustworthy.

Finally, we should ask ourselves **what we want** to achieve with the AI applications: the minimisation of crime is an important, but not the only goal in criminal justice - the fairness of the procedure is equally significant.

1. *Gless*, *Silverman*, *Weigend*. [↑](#footnote-ref-1)
2. Wu, Zhang, ‘Automated inference on criminality using face images’ (2016). [↑](#footnote-ref-2)
3. Agüera y Arcas et al., ‘Physiognomy’s New Clothes’ (2017). <https://medium.com/@blaisea/physiognomys-new-clothes-f2d4b59fdd6a>. [↑](#footnote-ref-3)
4. AG Ferguson, ‘*The Rise of Big Data Policing*’. [↑](#footnote-ref-4)
5. D Wilson, ‘Algorithmic patrol’. [↑](#footnote-ref-5)
6. S Egbert, ‘About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany’ (2018) 3 *European Journal for Security Research* 95. [↑](#footnote-ref-6)
7. C Polloni, ‘Police prédictive : la tentation de « dire quel sera le crime de demain’ (2015) *Rue89 <* https://www.nouvelobs.com/rue89/rue89-police-justice/20150527.RUE9213/police-predictive-la-tentation-de-dire-quel-sera-le-crime-de-demain.html>. [↑](#footnote-ref-7)
8. C Aebi, *Evaluation du Systeme de Prediction de Cambriolages Residentiels PRECOBS*. MA Thesis, École des Sciences Criminelles, Université de Lausanne (Lausanne, 2015). [↑](#footnote-ref-8)
9. I Stanier, ‘Enhancing Intelligence-Led Policing: Law Enforcement’s Big Data revolution’ in A Bunnik, A Cawley, M Mulqueen and A Zwitter (eds), *Big Data Challenges: Society, Security, Innovation and Ethics* (Palgrave Macmillan UK, 2016). [↑](#footnote-ref-9)
10. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention

on Human Rights, as amended) (ECHR). [↑](#footnote-ref-10)
11. Charter of Fundamental Rights of the European Union [2012] OJ C326/391. [↑](#footnote-ref-11)
12. 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) [2016] OJ L119/89. [↑](#footnote-ref-12)