**HUMAN RIGHTS COUNCIL**

**REPORT A/HRC/51/17. THE RIGHT TO PRIVACY IN THE DIGITAL AGE**

*Heliona Miço (Bellani), Federica Cristani\**

# 1. Introduction and a short overview of the instrument

The Office of the UN High Commissioner for Human Rights (OHCHR) released its latest report on ‘The right to privacy in the digital age in 2022, following the previous ones issued in 2014, 2018, and 2021, respectively.[[1]](#footnote-1)

The 2022 report discusses the recent trends and challenges concerning the right to privacy in the digital sphere, with a focus on the abuse of ‘intrusive hacking tools’, the importance of encryption, and the monitoring of public spaces. Especially when it comes to encryption, the report has been welcomed in particular by the Global Encryption Coalition for being "perhaps the strongest endorsement of encryption ever issued by the world body, and, as well, the strongest indictment it has issued against governmental attacks on encryption".[[2]](#footnote-2)

The report is structured as the following:

I. Introduction

II. Surveillance of personal devices and communications

A. Hacking

B. Restrictions on encryption

III. Surveillance of the public

A. Surveillance of public places

B. Online monitoring

C. Human rights impacts

D. Human rights requirements

IV. Conclusions and recommendations

# 2. Human rights addressed

The report overviews the most recent trends and challenges concerning the **right to privacy** in the digital sphere. In particular, the report focuses on three areas: (a) the widespread abuse of intrusive hacking tools; (b) the key role of robust encryption in ensuring the enjoyment of the right to privacy and other rights; and (c) the widespread monitoring of public spaces.

The following list includes the main findings of the report on the human rights affected concerning each area of analysis:

Surveillance of personal devices and communications

*A. Hacking*: This section overviews the most recent cases related to hacking, like the abuse of Pegasus software, which has highlighted the proliferation and abuse of "hacking tools for the targeted and covert surveillance of digital devices" that have also been used „ʻfor illegitimate reasons, including to clamp down on critical or dissenting views and on those who express them, including journalists, opposition political figures and human rights defenders" (p. 2 of the report). This is one instance where the right to privacy is closely interlinked with other human rights, like **freedom of expression and information**.

Hacking operations come in various forms, from full control of devices to access to emails, connected devices, and service providers' infrastructure. Such intrusions seriously infringe on the right to privacy and can lead to violations of other rights, including freedom of opinion and thought. Moreover, as the report highlights, "[…h]acking operations can be deeply traumatic experiences, affecting the mental health of the victims and their families" (p. 4 of the report), thus affecting also the **right to life** and the **right to be free from torture or cruel, inhuman or degrading treatment or punishment**. Furthermore, "[h]acking may also have a negative impact on the **rights to due process and fair trial**" (p. 4 of the report), to the extent that hacking tools may manipulate evidence that can be used in a trial.

As the report well recalls "[w]hile, in certain circumstances, intrusive surveillance measures may be permissible under articles 17 and 19 of the International Covenant on Civil and Political Rights on grounds of the protection of national security or public order, hacking can never be justified for political or business reasons, which is often the case when human rights defenders or journalists are targeted" (p. 5 of the report).

Spyware's capabilities raise serious concerns about privacy invasion and the manipulation of evidence. Hacking not only impacts the targets but also everyone in communication with them. Many governments lack proper legal frameworks to govern hacking operations and human rights bodies emphasize the need for stringent safeguards and independent oversight. The use of spyware should be limited to cases of preventing or investigating serious crimes or threats to national security, with strict adherence to necessity and proportionality. Calls are made for a moratorium on the sale and use of hacking tools until human rights-based safeguards are established.

*B. Restrictions on encryption*: the reports highlight how in some instances, actions of governments may "risk undermining the security and confidentiality of encrypted communications. This has concerning implications for the enjoyment of the right to privacy and other human rights" (p. 6 of the report). In particular, "[e]ncryption is a key enabler of privacy and security online and is essential for safeguarding rights, including the rights to freedom of opinion and expression, freedom of association and peaceful assembly, security, health, and non-discrimination" (p. 6 of the report).

Various governments have taken actions that risk undermining the security and confidentiality of encrypted communications, raising concerns about the right to privacy and other human rights. Encryption is crucial for safeguarding rights such as freedom of opinion and expression, association, security, health, and non-discrimination. It allows people to share information freely without fear of unauthorized access, censorship, or surveillance. Encryption is particularly important for journalists, human rights defenders, women facing online threats, and civilians in armed conflicts. Its vital role has been widely recognized by states, United Nations bodies, human rights experts, and regional experts. However, some governments impose restrictions on encryption for national security and crime prevention purposes, including bans, criminalization of encryption tools, and mandatory access to encrypted communications. These restrictions can weaken encryption and compromise privacy and human rights.

Governments' attempts to limit encryption often lack evidence of necessity, given alternative law enforcement tools and approaches. Encryption bans, key escrow systems, mandated back doors, and licensing requirements disproportionately affect the general population, not just targeted individuals. Such measures create vulnerabilities and jeopardize privacy and security, exposing users to unlawful interference by both state and non-state actors.

Surveillance of the public

*A. Surveillance of public places*: as the report states, "[s]urveillance cameras, deployed to monitor public streets, car parks, transportation hubs, and other public places, have become common in many countries" (p. 9 of the report), highlighting how "[t]hese developments often occur against a background of new identity systems and expanded biometric databases […]As a consequence, identifying individuals wherever they are located has become easier and easier" (p. 10 of the report).

*B. Online monitoring*: the report also stresses that "monitoring of public online discourse has become widespread. Globally, many authorities are collecting and analyzing social media posts and the private and professional networks built on publicly accessible communications platforms“ (p. 11 of the report).

Governments' access to private company data and the use of surveillance services offered by businesses add to the complexity and potential abuses of surveillance practices. Surveillance mechanisms of such kind impact several human rights, including the right to privacy, **freedom of expression and peaceful assembly, participation, and democracy**.

# 3. Challenges in implementation

Public surveillance poses significant human rights risks and can undermine the right to privacy. States using public surveillance must assess potential human rights impacts and ensure compliance with international human rights law. However, many countries lack adequate legal frameworks for surveillance, and surveillance measures often fail to meet the requirements of legality, legitimate goals, necessity, and proportionality. While public surveillance can serve legitimate aims, it is frequently used for impermissible purposes such as political targeting and profiling.

The report includes a number of final recommendations for states, including compliance with existing instruments of international human rights law; conducting human rights due diligence systematically whenever dealing with surveillance systems; adopting and effectively enforcing, through independent authorities, data privacy legislation for the public and private sectors; promoting public debate of the use of surveillance technologies; and ensuring effective remedies for any violations of human rights (pp. 15-17 of the report).

The report highlights several key areas in which the right to privacy in the digital realm is under threat. It acknowledges that there are additional challenges not covered in the report, such as covert mass surveillance, digital identity systems, biometrics, and pervasive tracking of internet users by various entities. The report emphasizes the need for a deeper exploration of how privacy violations affect marginalized and vulnerable individuals.

The OHCHR´s report is a soft law instrument. As such, the implementation of the recommendations included in it is left to the discretion of states. However, a good sign of the willingness of some states to implement the report´s findings may be found already in the inputs submitted for the preparation of the report:[[3]](#footnote-3) for example, Andorra stressed the need to adopt an international binding instrument on the topic[[4]](#footnote-4)

It is true that at the international level a common glossary on artificial intelligence is still lacking:[[5]](#footnote-5) Until all relevant stakeholders, including the national government, agree on a common vocabulary on the issues at stake, it will be very difficult to build up a common set of rules and regulations.

# 4. Similar initiatives

Other UN reports have highlighted how the digital sphere has challenged the right to privacy. We can recall, among others, the UN General Assembly resolution 75/176, The Right to Privacy in the digital age (28 December 2020), and the Human Rights Council resolution 48/4, the Right to Privacy in the digital age (13 October 2021).

At the regional level, we can also recall some key regulations of the European Union, like the ePrivacy Directive[[6]](#footnote-6) and the General Data Protection Regulation,[[7]](#footnote-7) which help ensure digital privacy for EU citizens.

Moreover, following two years of the application of the GDPR, the European Commission noted that further progress was needed to make the handling of cross-border cases more efficient and harmonized across the EU[[8]](#footnote-8), laying down additional procedural rules relating to the enforcement of the General Data Protection Regulation[[9]](#footnote-9).

# 5. Recommendations

The OHCHR´s report offers a general overview of the challenges of the right to privacy in the digital sphere. It also includes the main recommendations that states should follow to address all the relevant challenges. Specific recommendations are provided regarding hacking, encryption, surveillance of public spaces, and export control of surveillance technology.

However, the report is a soft law instrument, leaving it to the discretion of the national governments how to address the issues at stake; states should be encouraged to include the report´s recommendations in their national instruments. The work of the EU, which is already trying to harmonize the relevant rules at the regional level in Europe, already goes in the right direction for ensuring uniform rules among countries.

1. \* Heliona Miço (Bellani) is a lecturer of public and constitutional law at the Law Department of Epoka University, Tirana, Albania. Her research is concentrated in the fields of human rights, the right to education, social inclusion, and quality in higher education institutions. E-mail: hmico@epoka.edu.al;

Federica Cristani is Head of the Centre for International Law, Institute of International Relations, Prague, and Visiting Senior Researcher at the Arctic Centre of the University of Lapland. E-mail: cristani@iir.cz.

The Human Rights Council mandated a Special Rapporteur on the right to privacy in July 2015. the previous year, the High Commissioner issued the first report on the right to privacy in the digital age (A/HRC/27/37). a second report was issued on 3 August 2018, A/HRC/39/29. In the following year, on 26 September 2019, the Human Rights Council adopted resolution 42/15 on “The right to privacy in the digital age”, where it requested OHCHR to organize an expert meeting to discuss "how artificial intelligence, including profiling, automated decision-making, and machine-learning technologies may, without proper safeguards, affect the enjoyment of the right to privacy [and] to prepare a thematic report on the issue” (paragraph 10 of HRC resolution 42/15). The expert seminar on the right to privacy took place on 27-28 May 2020 (please see the following link for details: https://www.ohchr.org/en/privacy-in-the-digital-age/expert-seminar-artificial-intelligence-and-right-privacy-27-28-may-2020). After that, OHCHR invited all relevant stakeholders to provide inputs for the preparation of a thematic report on the right to privacy in the digital age, which resulted in the report issued on 15 September 2021, A/HRC/48/31. [↑](#footnote-ref-1)
2. Greg Nojeim, Mallory Knodel, "Global Encryption Coalition Steering Committee Statement on the OHCHR Report on the Right to Privacy in the Digital Age" (16 September 2022), <https://cdt.org/insights/global-encryption-coalition-steering-committee-statement-on-the-ohchr-report-on-the-right-to-privacy-in-the-digital-age>. [↑](#footnote-ref-2)
3. All are available at the following link for public consultations: <https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021>. [↑](#footnote-ref-3)
4. See the input by Andorra, available at the following link: <https://www.ohchr.org/Documents/Issues/DigitalAge/Submissions/States/Andorra.docx>. [↑](#footnote-ref-4)
5. See for example the submission of Germany, available at the following link: https://www.ohchr.org/Documents/Issues/DigitalAge/Submissions/States/Germany.pdf. [↑](#footnote-ref-5)
6. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

 [↑](#footnote-ref-6)
7. 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). [↑](#footnote-ref-7)
8. Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation (COM/2020/264 final). [↑](#footnote-ref-8)
9. Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679. <https://eur-lex.europa.eu/resource.html?uri=cellar:d02eb625-1a4d-11ee-806b-01aa75ed71a1.0001.02/DOC_1&format=PDF> [↑](#footnote-ref-9)