Comments to the COVI committee draft report on the COVID-19 pandemic: lessons learned and recommendations for the future (2022/2076(INI))

The European Center for Not-for-Profit Law (ECNL), the International Network of Civil Liberties Organisations (INCLO) and Privacy International (PI) welcome the initiative of the European Parliament's COVI committee to reflect on the three years of the COVID-19 pandemic and assess the response to the pandemic of EU institutions and Member States.

In the months following the beginning of the COVID-19 pandemic, more than half the world's countries enacted emergency measures. Within this broader context, we have seen a rapid scaling up of governments' use of technologies to enable widespread surveillance. In 2022, ECNL, INCLO and PI conducted a global study[1] tracking negative impacts of surveillance technology and measures deployed during the COVID-19 pandemic on activist movements and organisations. Karolina Iwańska, Digital Civic Space Advisor at ECNL, shared our key findings during the COVI committee hearing on fundamental rights and COVID-19 organised in Brussels on 31 January 2023.

These key findings can be summarized as follows:

1. The development and adoption of digital solutions was very hasty and often **lacked any assessment of legality, necessity and proportionality.** Despite scant evidence of their effectiveness, digital solutions were often perceived as an easy fix and their intrinsic limitations were rarely explicitly recognised. This was particularly the case for contact tracing and quarantine monitoring apps which, in most cases, were developed and deployed in a non-transparent manner, without meaningful engagement of civil society, appropriate accountability and oversight mechanisms, and without clear sunset clauses stipulating when these tools would be phased out.
2. We have seen instances of **unlawful and disproportionate limitations to fundamental rights safeguards under the pretext of "emergency".** In Hungary, for example, the government suspended or limited the application of a number

[1] https://ecnl.org/publications/under-surveillance-misuse-technologies-emergency-responses

of GDPR rights under the pretext of emergency, which was criticised as unjustified and disproportionate by civil society and the European Data Protection Board. In France, surveillance drones were unlawfully used by the police to monitor public spaces, including demonstrations in October 2020.

3. We have noted cases involving the **repurposing of surveillance technologies and the risk of their normalization beyond the pandemic**. While we have not seen the repurposing of contact tracing apps for general health interests in the EU, these apps were not officially phased out and deleted from app stores. One concerning case of repurposing data collected for pandemic reasons comes from Hungary where a government official unlawfully used email addresses entered to register for vaccines for political marketing before the 2022 general elections.
4. During the pandemic, the use of surveillance tools was largely ad-hoc and uncoordinated. We should learn from this experience and **develop common standards and mechanisms across the EU**, including measures introducing clear time limits for the use of digital surveillance which would ensure that exceptional measures remain the exception, and not become the norm. In particular, we recommend an urgent **review of adopted digital solutions** to consider how, or if, they respected the essence of fundamental rights; their efficiency; and how, or if, they respected the principles of necessity and proportionality in a democratic society. Such a review should result in a better understanding of which measures are justified and which are not. It would also pave the way for evidence-based responses to future crises. Measures that are no longer, or have never been, necessary should be immediately ceased. This process should be conducted in public and in dialogue with relevant stakeholders, including civil society.

Some of these observations and recommendations have also been included in reports published by the Fundamental Rights Agency[2] and by the Council of Europe[3].

Regrettably, the draft report of the COVI committee[4] does not recognize any of these important lessons. Therefore, we suggest the following amendments to the report:

Proposals for amendments (in bold)	Justification
41. Supports adapting existing EU regulatory frameworks and soft law and developing and implementing new frameworks in order to allow national	We recommend adding an explicit reference to the protection of fundamental rights, next to safety and respectful treatment of patients. The EU

[2] https://fra.europa.eu/en/publication/2020/covid19-rights-impact-june-1

[3] https://rm.coe.int/report-dp-2020-en/16809fe49c

[4] https://www.europarl.europa.eu/doceo/document/COVI-PR-739788_EN.pdf

healthcare systems and the scientific community to benefit from artificial intelligence (AI) in the fields of clinical practice, biomedical research, public health and health administration, while ensuring the ***strong protection of fundamental rights***, safety and respectful treatment of patients receiving AI-mediated healthcare ***and other affected individuals or groups***; **Note:** Similar changes have been proposed in **AM 797**	Charter of Fundamental Rights includes a comprehensive list of fundamental rights and binding obligations on EU institutions and Member States to safeguard them also when these rights are impacted by the use of technology. It is also important to note that specifically in the context of AI systems, the proposed Artificial Intelligence Act currently deliberated in the European Parliament[5], which will apply to AI systems in the area of healthcare, explicitly refers to the need to protect fundamental rights when developing and deploying AI systems.
86. Urges the further digitalisation of administrative services and, wherever appropriate and feasible, the use of online healthcare services***, while ensuring the strong protection of fundamental rights through the assessment of impact of these services on fundamental rights, including the right to health care, right to the protection of personal data, right to privacy, the right to non-discrimination and the right to good administration, before they are made operational***;	The use of digital technologies in healthcare services can bring risks to fundamental rights, especially the right to health care, the protection of personal data, non-discrimination and good administration. It is crucial that digitalization of health services safeguards these rights. This is only possible when a robust fundamental rights impact assessment is conducted prior to procuring and deploying digital services or products.
~~**120. Highlights that disinformation campaigns, along with cyberattacks, are part of 'hybrid warfare' strategies by foreign powers; reiterates that security and freedom are inseparably interlinked;**~~	We recommend deleting this paragraph as it is misplaced in the context of the COVID-19 pandemic. In addition, by focusing on foreign interference, it shifts attention away from domestic threats related to disinformation.
122. Reiterates the importance of well-established scrutiny processes, both at national and European level, to ensure that national authorities are held	There is no justification why the accountability of national authorities should only be limited to selected fundamental rights mentioned in this

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

accountable for breaches of ***fundamental rights, including*** freedom of assembly, freedom of speech, ***the right to privacy and protection of personal data,*** the right to private property and patient rights, and to ensure certainty and predictability in changes to rules for businesses; **Note:** Alternatively, we support the proposed **AM 1849.**	paragraph. Therefore, we propose ensuring that the wording encompasses all fundamental rights.
123. Notes that the EU has a strong data protection system with consistent data privacy provisions; highlights that the EU COVID Digital Certificate and its tracing apps ***generally*** respected this system, while allowing the free movement of EU citizens under the ***sanitary*** rules applied during the crisis; ***emphasizes, however, that the adoption of digital tools was rarely preceded by a meaningful assessment of their efficacy, necessity and proportionality as well as their fundamental rights impacts;***	The original version of this paragraph fails to acknowledge concerns about the use of contact tracing apps documented by civil society organisations, researchers[6], as well as by FRA and Council of Europe. It also does not recognize concerns raised by the European Data Protection Board and European Data Protection Supervisor in relation to the EU COVID Digital certificate[7]. Therefore, we recommend including an explicit reference to the shortcomings of the process of introducing digital solutions, especially the lack of assessment of effectiveness, necessity, proportionality and their fundamental rights impacts.
135. Acknowledges that ***because relevant procedures and processes were not in place***, in the middle of the crisis, institutions were confronted with exceptional situations in which urgency ~~***necessarily***~~ prevailed over the timely ***assessment of necessity and***	Urgency does not have to necessarily prevail over timely impact assessment and transparency. In our view, a lesson in the case of the COVID-19 pandemic was that relevant processes were not put in place in advance, which needs to be mitigated for the future.

[6] https://www.awo.agency/blog/covid-19-app-project-phase-2/

[7] https://edps.europa.eu/system/files/2022-03/edpb-edps_1-2022_joint_opinion_extension_of_covid_certification_regulation_en.pdf

proportionality and fundamental rights impacts of different solutions as well as the publication of certain documents; stresses, however, that ***the development of common standards across the EU,*** transparency ***and careful fundamental rights review*** should still be a priority; **Note:** These concerns have also been addressed by **AM 2025, 2026, 2030**.	In line with the previous comment, we suggest an explicit recommendation for an ex-post review of digital solutions that were adopted during the pandemic and an explicit recommendation ensuring meaningful fundamental rights impact assessments during future emergencies.
136. Considers that the COVID-19 crisis was a stress test for the EU's democratic resilience; ***emphasizes that there is a need for further review of the necessity and proportionality of emergency measures, especially digital solutions, and for creating common standards for EU institutions and Member States for ensuring a high level of protection of fundamental rights and democratic principles*** **Note:** These concerns are also addressed by AM 2036, 2051, 2053, 2054, 2056, 2057, 2067.	We recommend including specific recommendations for how to improve emergency response in the future, especially through the review of the necessity and proportionality of the adopted measures and creating European standards for the protection of fundamental rights in emergency responses.
249. Recommends the setting up of instruments and funding programmes to fight cyber threats, terrorism and external state-sponsored propaganda, ***ensuring, through robust transparency and accountability measures, that these instruments do not violate fundamental rights, especially the freedom to expression, assembly and association and the right to privacy and data protection***;	We strongly recommend ensuring that relevant safeguards protecting fundamental rights are in place when countering threats and terrorism. These measures have in the past been used against journalists, human rights defenders, civil society or political opponents, also in EU Member States.