Dear Ms. Adamowicz,

Would you be comfortable with the thought that all your letters are being opened on the off chance that they might contain suspicious material? If not, please transfer this conviction to the digital sphere and vote against the abolishment of digital privacy for correspondence as part of the ePrivacy Derogation!

The so-called “e-Privacy Interim Regulation” (2020/0259(COD)) would require online messenger and email service providers to automatically scan private message content in real time for suspicious text and image content using error-prone artificial intelligence. All suspicious cases identified by AI would be automatically disclosed to investigative authorities in the EU – without the individuals concerned knowing about it. This is intended to counter the spread of child pornography on the internet.

We, of course, share the sentiment behind the initiative: children’s rights are a serious matter for which we as a foundation have been campaigning for years. But however well-intentioned it might be, this should not obscure the fatal impacts of the planned remedy:

• **The digital privacy of correspondence would effectively be abolished.** All communication content would be indiscriminately captured and searched on a massive scale. Self-censorship would immediately become the norm. Legal opinions have shown that such a mass and suspicion-independent screening of private communication content is not compatible with the Charter of Fundamental Rights of the European Union.

• **Baseless suspicions would become the rule.** According to the Swiss Federal Office of Police (fedpol), the error rate for automatic message screening is around 86%! For example, harmless holiday snaps or intimate selfies made by young people would lead to private message content being automatically disclosed and the launch of police investigations. More than one third of criminal investigations are already directed against minors.

• **Criminals are already finding ways to circumvent surveillance.** When privacy is a crime, only criminals have privacy.

• **A surveillance infrastructure would be created, which – as we know all too well from experience – would eventually be extended to other areas (”mission creep”).** Sooner or later, under the pretext of fighting terror, crime or even the threat of losing power, governments would be tempted to use this tool in other ways.

• **Experience has shown: Leaks, hacks, fails and abuse are inevitable.** Collections of potential blackmail material would be created. In the past, cases have come to light where employees from investigative authorities and NGOs have themselves been secretly spreading child pornography. This would therefore often achieve the very opposite of what is wanted – the protection of children and fundamental rights.
• Most acts of violence against children happen in secret and are not documented electronically. Prevention is what’s needed. A false “sense of security” helps no one. Targeted and effective law enforcement methods should not be cut back, but expanded.

• Many victims of child abuse and leading providers are strongly opposed to universal search measures – as are 72% of EU citizens. Scanning all private messages is no substitute for solid police work and concrete help for victims of sexual violence. A representative survey in ten EU Member States has shown that 72% of respondents are clearly opposed to automated searches of private messages.

Please, don’t get us wrong here: crimes against children are terrible and demand decisive action! But warrantless surveillance of our communications is totally inappropriate and creates a climate of mistrust in Europe.

We therefore urge you to oppose the bill when it comes before Parliament on July 7 and 8!

Kind regards,

Dr. phil. Dr. h.c. Michael Schmidt-Salomon
Spokesman of the board of the gbs

Peder Iblher
gbs Rapporteur on digital basic rights

PS: For more background information please visit our website www.digitalhumanrights.blog