Not You Again!

Theresa Bosl 2023-09-07T09:00:54

Mass surveillance has been a recurring issue before courts around the globe, including the Court of Justice of the European Union (CJEU). In the last cases brought before the CJEU, e.g., against Germany, one could almost hear the judges' eyes roll while limiting – repeatedly – the states' plans of mass surveilling without proper safeguards. The case of "Hadopi" that is currently before the CJEU might be different, however. It could actually lead to a detrimental change in the Court's jurisprudence on fundamental rights and thus also impact the jurisprudence of other courts, most notably the European Court of Human Rights (ECtHR).

The Hadopi Case

The "Hadopi case" (Case C#470/21), referred to the CJEU for a preliminary ruling by the Conseil d'État of France, concerns a claim by the French data protection authority (CNIL) against Hadopi, the French agency responsible for enforcing copyright infringement laws. The case concerns the legality of Hadopi's use of personal data on a mass scale to identify and sanction internet users who engage in illegal file-sharing and thus tests – once again – the limits of states' mass surveillance laws. The CJEU will have to deal with the compatibility of Hadopi's activities with the EU law on data protection and privacy, especially the General Data Protection Regulation (GDPR) and the e-Privacy Directive. The explosive potential, however, lies not so much within the circumstances of the case but within the opinion delivered by Attorney-General (AG) Szpunar who explicitly demands an adjustment of the CJEU's jurisprudence concerning mass surveillance. His opinion has led to the CJEU sitting as a full court with 27 judges in these proceedings.

How a Case About Copyright Infringement Could Be a Game-Changer for the Right to Privacy

To comprehensively understand the possible implications of the Hadopi case, we need to understand the current legal framework surrounding mass surveillance. Thus, we can turn to the CJEU's jurisprudence. As Article 52 III of the Charter of Fundamental Rights (CFR) stipulates, the meaning and scope of EU fundamental rights shall be the same as those laid down by the ECHR, so the ECtHR's jurisprudence can be taken into account as well. Both courts have acknowledged mass surveillance as a tool that states may use to react to modern threats, such as the dangers of modern terrorism. In *La Quadrature Du Net*, the CJEU found the objective of combatting terrorism to justify interferences with the right to privacy in the form of the real-time collection of traffic and location data (para. 188) and allowed the general and indiscriminate retention of IP addresses (paras. 155-156). Similarly, the ECtHR has proclaimed, most recently in *Big Brother Watch* (para. 365) and *Centrum för rättvisa* (para. 254), that states are permitted to adapt their measures to technological developments that allow criminals to communicate digitally and thus can operate internationally without the need of physically crossing borders.

Both courts have been heavily criticized for what Marko Milanovi# called the “Grand Normalization of Mass Surveillance” and Monika Zalnieriute labelled as the “Fading Anti-Securitisation Stance at the CJEU”.

The Hadopi case could boost this trend in two aspects: AG Szpunar not only calls for a lowered threshold for mass surveillance but also for a weakening of monitoring requirements.

Lowering the Threshold for Mass Surveillance?

While the ECtHR grants the states a wide margin of appreciation and accepts protecting national security, preventing disorder and crime as well as protecting the rights and freedoms of others as legitimate aims when evaluating the legality of bulk interception (ECtHR, Big Brother Watch, para. 365), the CJEU’s requirements for mass retention of data are stricter. The CJEU only accepts the combatting of *serious* crimes as a justifiable aim for serious interferences with Articles 7 and 8 of the CFR (CJEU, La Quadrature Du Net, para. 140). It held that, accordingly, only non-serious interferences could justify prosecuting and preventing general crime (Ibid.). Now, AG Szpunar calls upon the CJEU to also allow such measures for prosecuting copyright infringements. As the term “serious crime” must be interpreted autonomously (AG Szpunar, para. 74), it only covers particularly grave offences (CJEU, Digital Rights, para. 24). Art. 83 of the Treaty on the Functioning of the European Union (TFEU) lists as examples of serious crimes “terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime.” As AG Szpunar rightly admits, copyright infringement is not covered by this term (para. 74). Accordingly, prosecuting copyright infringement could only justify non-serious inferences with fundamental rights to suffice the requirements laid down by the CJEU. However, the French practice of collecting IP addresses and personal data does not constitute such a non-serious interference. Specifically regarding the retention of IP addresses, the CJEU held in *La Quadrature Du Net* that such widespread measures do constitute a serious interference as internet users are generally entitled to expect that their identity will not be disclosed (para. 155).

AG Szpunar acknowledges the CJEU’s former jurisprudence but argues that it is necessary to adjust EU law to modern technology’s challenges (para. 82). Otherwise, committing offences exclusively online would lead to a systemic impunity of acts below the threshold of serious crime, such as copyright infringement and online defamation (paras 78 et seq.). Therefore, AG Szpunar calls on the CJEU to allow for the retention of and access to IP addresses and corresponding data if they are the only means to effectively prosecute these crimes (paras 79 et seq.).

Weakening Safeguards?

The second point of significance in AG Szpunar’s opinion concerns the safeguards the CJEU – and similarly the ECtHR – have found to be essential for measures of bulk data interception. It is not possible, in the confines of this post, to review the entirety of safeguards both courts have dealt with and what was called “convergence

around procedural fetishism". However, one common requirement that both courts repeatedly relied upon was the guarantee of prior review for the state entities' access to retained data (CJEU, Tele 2 Sverige, para. 120; Prokuratuur para. 51; Commissioner of An Garda Síochána and Others, para. 106; ECtHR, Szabó and Vissy, paras 77 and 88; Roman Zakharov, para. 233; Klass and Others, paras 55-56, Big Brother Watch, para. 336). This prior review must not necessarily be conducted by a court but by a competent body independent from the executive (CJEU, Digital Rights, para. 52, ECtHR: Big Brother Watch, para 351).

Nevertheless, AG Szpunar argues that prior review would not be necessary for the access to IP addresses and corresponding personal data (paras. 98 ff.). According to him, cases in which prior access was required concerned only "particularly serious" interferences (para. 99). The case at hand would not meet that threshold as Hadopi's access was limited to linking civil identity data to the IP address used and to the file (illegally) viewed at a given point in time. Contrary to other measures, this would not allow the authorities to draw a conclusive picture of the users' private life, e.g., by reconstructing their clickstream (paras 100 et seq.). Thus, Szpunar holds that the renunciation of prior review would not constitute a change in the CJEU's jurisprudence.

Between Pragmatism and Pandora's Box

Following AG Szpunar's opinion would have two major implications for the right to privacy in the EU – and, as the ECtHR and CJEU jurisprudence regularly impact each other – possibly beyond. First, states could regulate the access to retained IP addresses and corresponding data also for the general prevention and prosecution of (less serious) crimes. Second, state authorities could access the data without prior review by an independent body.

Naturally, AG Szpunar's concerns of systemic impunity of offences which were committed exclusively online (such as copyright infringements but also hate speech, identity theft, fraud etc.) are as such comprehensible. However, following his opinion also bears immense risks of abuse. Permitting mass surveillance for the fight against general crime means allowing states to use mass surveillance against *any* acts that *they* consider worth penalizing as general crime. It thus depends on the penal code of the individual member states to determine the acts that might be targeted by surveillance measures.

Now, while AG Szpunar certainly has the best of intentions, this consequence seems to lead to a rather dangerous path, especially considering that even within the EU, there are member states that do not hold fundamental rights and democratic values as high as one would hope (yes, I am looking at you, Poland and Hungary). Let us assume (though we do not even have to be that imaginative) that there was a law penalizing homosexuality or abortions, states could potentially use surveillance measures to prosecute also such "offences". Of course, these offences are not exclusively committed online, but states could nevertheless argue that the retention of and access to IP addresses and corresponding data are the only means to effectively prosecute them. Against this backdrop, even if one agrees with

Szpunar on the first point, effective control of access to such data seems even more important.

It can ensure that these measures are, in fact, the only option to prosecute the offences in question and minimize risks of abuse. This also holds true for cases of online defamation as they require a careful balancing act to determine which expression amounts to defamation and which is protected by the freedom of expression. Otherwise, surveillance measures might be abused to hinder the public from voicing valid criticism with the states' representatives and politics.

Considering the CJEU's previous stance on the importance of procedural safeguards, it seems unlikely that the independent review requirement will be abandoned. Moreover, unless the ECtHR also abandons this requirement, EU member states, as they are all parties to the ECtHR, would still have to comply with it. It is hard to imagine that both courts would turn their backs on this requirement, which they have repeatedly and prominently mentioned in their judgments. But if they did, it would certainly change the way the right to privacy is understood in Europe and beyond.

Overall, it is rather surprising that the Hadopi case has not yet received more attention, since it tackles several highly controversial and actual topics. It will be interesting to see if the CJEU manages to strike a balance between pragmatism in dealing with modern technologies on the one hand and effectively protecting fundamental rights from states' abuse of power on the other. This could be achieved by allowing access to IP addresses and corresponding data for the prosecution of general crime but simultaneously sticking to the requirement of efficient safeguards.

The "Bofaxe" series appears as part of a collaboration between the IFHV and Völkerrechtsblog.
