independent ex post facto review[26]. Conversely, access to data on a generalised and indiscriminate basis ("mass surveillance"), without limitations and safeguards, is unlawful[27]. In addition, specific safeguards must apply to the use of data collected in bulk. For example, to share data collected in bulk with foreign intelligence services, it must be ensured that the receiving State has safeguards in place to prevent abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure. In addition, the transfer of data to foreign intelligence service should be subject to independent control[28].

Third, any government access for national security purposes must be subject to independent oversight, normally by the judiciary[29] and, in any event, by an authority that is independent from the executive[30] and vested with sufficient powers to exercise effective and continuous control[31]. In principle, there should be prior authorisation of surveillance measures or, in the absence thereof (e.g. in cases of urgency), effective "post factum" oversight and review[32].

There is some diversity in the way relevant oversight systems are structured at national level. Competent supervisory bodies in this area include a range of actors such as judicial bodies, data protection authorities, independent specialised bodies and parliamentary committees. These bodies fulfil often complementary (and mutually reinforcing) oversight functions. They are vested with different powers, such as authorising surveillance measures, conducting investigations on the basis of complaints or on their own initiative (and, in that context, accessing relevant information), adjudicating complaints lodged by individuals and ordering remedial measures, providing advice to governmental authorities on draft legislation and issuing recommendations on the implementation of relevant legal rules and policies.

Fourth, effective redress must be available to anyone who suspects that their data has been accessed, including the possibility to obtain access to, or rectification or erasure of the data[33]. In particular, a person affected by measures taken for national security reasons, such as surveillance measures, must be able to have the measure in question reviewed by an independent[34] and impartial

---

[26] See e.g., ECtHR, Big Brother Watch and Others v. the United Kingdom, § 356, "Each stage of the bulk interception process – including the initial authorisation and any subsequent renewals, the selection of bearers, the choice and application of selectors and query terms, and the use, storage, onward transmission and deletion of the intercept material – should also be subject to supervision by an independent authority and that supervision should be sufficiently robust to keep the "interference" to what is "necessary in a democratic society".

[27] CJEU, C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, § 94.

[28] ECtHR, Big Brother Watch and Others v. the United Kingdom, § 362.

[29] ECtHR, Klass and Others v. Germany, § 55.

[30] ECtHR, Szabó and Vissy v. Hungary, § 77 and the case law cited. As regards the criteria for independence, the ECtHR has highlighted, among others, "the manner of appointment and the legal status of the members of the supervisory body" (Roman Zakharov v. Russia, § 278), the absence of conflicts of interest (id. § 280), the powers of the supervisory body, both in terms of "access to all relevant documents, including closed materials" (id. § 281) and remedial powers (id. § 282), and that its "activities are open to public scrutiny" (id. § 283).

[31] ECtHR, Klass and Others v. Germany, § 56. As regards the remedial power, the ECtHR has highlighted, among others, the power to "stop or remedy the detected breaches of law", to hold those responsible accountable and to destroy unlawfully obtained intercept material (see ECtHR, Roman Zakharov v. Russia, § 282 and the case law cited). With respect to investigatory powers, the ECtHR has emphasised "that it is essential that the supervisory body has access to all relevant documents, including closed materials and that all those involved in interception activities have a duty to disclose to it any material it required" (see id. §281 and the case law cited).

[32] ECtHR, Szabó and Vissy v. Hungary, §§ 77, 81; Big Brother Watch and others v. United Kingdom, § 350. See also CJEU, La Quadrature du Net, § 189.

[33] Article 13 ECHR and Article 47 Charter of Fundamental Rights of the EU. See also ECtHR, Klass and Others v. Germany, §§ 55-56; CJEU, La Quadrature du Net, § 190.

[34] Regarding independence, the ECtHR has held that the following criteria must be taken into account: (i) the manner of appointment of its members, (ii) the duration of their term of office, (iii) the existence of guarantees against outside pressures; (iv) whether the body presents an appearance of independence (see Kleyn and Others v. the Netherlands, Applicationsnos. 39343/98, 39651/98, 43147/98 and 46664/99, § 190; Langborger v. Sweden, Application no. 11179/84, § 32).

In any case, any individual, regardless of nationality or place of residence, may, after exhausting such domestic remedies[46], bring a claim concerning a violation of the ECHR before the ECtHR[47]. Therefore, a U.S. individual can bring a claim before the ECtHR. Cases can be brought before the ECtHR claiming either that specific national surveillance measures violate the ECHR, or claiming that the national legal framework governing access to data for national security purposes violates the ECHR[48].

Finally, it is worth noting that the EU, along with the United States, endorsed on 14 December 2022 the Organisation for Economic Co-operation and Development (OECD) "Declaration on Government Access to Personal Data Held by Private Sector Entities", which, for the first time at international level, describes a set of core principles for public authorities' access to personal data in the area of law enforcement and national security that are common to OECD member countries. The Declaration reflects the type of privacy safeguards that the EU, its Member States, and the United States share in this area.

(e-signed)

Didier REYNDERS

[46] Irrespective of whether such remedies would fail on substantive or procedural grounds (e.g. admissibility).

[47] Articles 34 and 35(1) ECHR.

[48] See e.g. ECtHR, Klass and Others v. Germany, §§ 33-38; Weber and Saravia v. Germany, § 78; Roman Zakharov v. Russia, §§ 167-168.