ECtHR JUDGMENT OF 13 SEPTEMBER 2018, *BIG BROTHER WATCH AND OTHERS V. THE UNITED KINGDOM*

Power Point

Francesca Tassinari Becaria FPU Dpto. DIPu y RRII UGR

In *Big Brother Watch and others v. The United Kingdom*, the European Court of Human Rights (hereinafter ECtHR) revisited[1] the compatibility of the United Kingdom's surveillance program on communication with the European Convention of Human Rights (also ECHR) following the denounces submitted by three groups of Non-Governmental Organisations against the Regulation of Investigatory Power Act 2000 (RIPA). In their opinion, RIPA would breach: the right to privacy and to a family life (Article 8); the freedom of expression (Article 10)[2]; the right to a fair trial (Article 6)[3], and the prohibition of discrimination (Article 14[4]). Waiting for a final answer form the Great Chamber, in this post I propose to go through the main points objected in the controversy in order to point out the necessity of an evolution of the ECtHR's jurisprudence on strategic surveillance programs in the light of the technological advances reached in the last twenty years. The reader will forgive my focusing on the ECtHR's analysis on the British domestic law with regard only to Article 8 ECHR, the right to a private and family life.

THE JUDGEMENT: THE REGULATION OF INVESTIGATORY POWER ACT *versus* ARTICLE 8 ECHR

The ECtHR analysis on the compatibility of RIPA with regard to Article 8 ECHR focuses on three different provisions: firstly, section 8(4) allowing the Government Communications Headquarter of the United Kingdom to intercept external communications; secondly, the possibility of the same Government to receive information by third countries – with especial emphasis on the United States of America PRISM and UPSTREAM programs – according to the revised Interception of Communications Code of Practice (ICP Code); and, finally, Chapter II RIPA enabling the Government Communications Headquarter to ask for data from the Telecommunications Service Providers.

SECTION 8(4) OF THE REGULATION OF INVESTIGATORY POWER ACT: THE UNTARGETED WARRANT REGIME

The British regime of strategic interception of communication regulates two types of programs: firstly, the Targeted Warrant (section 8(1)); and, secondly, the Untargeted Warrant (section 8(4)). Targeted Warrant (section 8(1)) is an investigative tool used in case a subject has already been identified and pursuits interception purposes, whereas Untargeted Warrant (section 8(4)) allows to intercept "external communication in the course of their transmission by means of telecommunication system", following a certification issued by the Secretary of State[5]. Only the latter mechanism is provided with the enhanced safeguards set forth in Article 16 RIPA that protects individuals known to be in the British Islands when the material contained in the communication sent by or intended for these individuals shall be identified [6].

The ECtHR maintains that national security by means of secret surveillance measures pursuits a legitimate interest in the light of Article 8(2) ECHR (§ 308). In order to elucidate the respect of the principle of legality, formally and substantially, the ECtHR applies the so called "Weber criteria" that consist of the analysis of: 1. the nature of the offences that may give rise to an interception order; 2. a definition of the categories of persons whose communications may be

intercepted; 3. a limit to the duration of the interception; 4. the procedure to be followed to examine, use and store the data obtained; 5. the precautions to be taken when data are communicated to third parties, and 6. the circumstances in which intercepted data may or must be destroyed (§ 307).

The ECtHR points out that any review and supervision upon secret surveillance measures can be implemented at three stages: when the surveillance is ordered; while it is ongoing, and when it is over. The ECtHR establishes that the issuing of an interception warrant by the Secretary of State provides for sufficient safeguards thanks to the introduction of the Investigatory Power Act 2016 (IPA) for which a Judicial Commissioner would be set up so as to approve the executive act. As far as the "ongoing" safeguards are concerned, the ECtHR detects two infringements: firstly, the certificate issued by the Secretary of State should have strictly defined the scope of the interceptions was well as the parameters of the searches; secondly, ECtHR maintains that the whole selection process, as well as the parameters used by the analysts to select the relevant material, should have been controlled by an independent authority. Besides, the safeguards offered under Article 16 RIPA should be equally applied to "communication content" data as well as to "metadata", for which the Court maintains that: "In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with" (§ 356). Finally, the ECtHR establishes that the guarantees foreseen in the *ex post* surveillance phase are satisfied since the Investigatory Power Tribunal (IPT) provides for effective remedies to individuals[7].

UNITED STATES-UNITED KINGDOM INTERNATIONAL DATA TRANSFER: CHAPTER 12 OF THE INTERCEPTION COMMUNICATIONS CODE OF PRACTICE

Big Brother Watch constitutes the first judgment in which the ECtHR faces an intelligence sharing regime. Notably, its attention was brought not to the transfer of data from the United Kingdom to a third country – in this case, the United States – but to the possibility that the Government of Communication Headquarter of the United Kingdom was granted to access to the

[1] Previously, in *Liberty and Others v The United Kingdom*, a British liberal organization and two Irish women alleged that, between 1997 and 1997 their telephone communications data, facsimiles, and emails containing privileged and confidential information, had been intercepted by the Electronic attest Facility of the British Ministry of Defence. The ECtHR stated that the Interception Communication Act – the predecessor of Article 8(4) RIPA – infringed Article 8 ECHR for not being in conformity with the principle of legality. Concretely, the ECtHR found that the domestic law was not sufficiently clear which may have flown into an abuse of power since competent authorities in charge to intercept and examine outside communication were given a too broad discretion. Furthermore, the British law lacks any provision indicating the procedure to be followed by competent authorities in the proceeding of examination, sharing, storage and destruction of the intercepted materials.

[2]Being the applicants NGOs, they alleged that the United Kingdom strategic surveillance program acts as a Watchdog and intercepts also confidential material in case of journalists in breach of the freedom of expression.

[3]Concretely, the applicants complained that the Investigatory Power Tribunal (IPT) lack independence and impartiality.

[4]Section 8(4) RIPA applies to « external relations » for which persons outside the United Kingdom are more likely to be intercepted. Yet, in this case, the safeguards offered by section 16 RIPA does not apply since its scope is limited to the individuals established within the British Islands whose communications' material want to be identified.

[5] It shall be reminded that the ECtHR has been generally called to evaluate the legality of targeted warrant regimes, while the untargeted warrant ones were taken into consideration in Weber and Saravia v Germany and Centrum för rättvisa v Sweden – the latter is now pending the Grand Chamber's final judgment too.

[6] The system automatically registers all correspondences that match with the "simple selectors" while analysts open and read the information to establish what is most valuable for the intelligence services. In doing so, they follow a two-step proceeding for which firstly they discard material that is less likely to be of interest and, secondly, they apply questions to the material pre-selected so as to generate an index to be further analysed.

[7] In the same line see also *Kennedy v The United Kingdom*.

U United States' PRISM and UPSTREAM systems according to the Interception of Communication Code of Practice (ICP Code). In particular, through the latter, the United Kingdom can access not only non- United States citizens data but everyone's data – British nationals too[8], while circumventing the guarantees set forth under the RIPA (§ 423).

The ECtHR notes that the interceptions are materially carried out by the third country so that the United Kingdom's responsibility can be claimed only in case it exercises control over the US government in conducting such an operation. Yet, the United Kingdom's responsibility shall also be assessed on the basis of the receipt of the material and its subsequent storage, examination and use by foreign intelligent services (§ 421). The ECtHR passes to apply the "Weber criteria" but, in doing so, it discards two over the six criteria – namely the nature of the offences that may give rise to an interception order, and the definition of the categories of persons whose communication may be intercepted. Hence, it notices that the data transferred from the United States to the United Kingdom should be searched under the same conditions required for national searches and with the same authorisation allowing the interception of bulk material by the intelligence agency. By doing so, the ECtHR maintains that the obtention of data from the United States government does not circumvent the RIPA safeguards, and that adequate controls and remedies exist in case of abuse of powers (§ 447).

CHAPTER II OF THE OF THE REGULATION OF INVESTIGATORY POWER ACT: THE INTERCEPTION COMMUNICATION DATA REGIME

The last regime analysed with regard to Article 8 ECHR concerns Chapter II RIPA - and the Acquisition and Disclosure of Communications Data Code 2015 (ARD Code) - for which public authorities can acquire communication data from Communication Service Providers (CSP). This is quite a new situation the ECtHR is called to assess since in its previous case-law the access to data concerned historical data and not data captured in real time[9]. Hence, the ECtHR goes back to the Court of Justice of the European Union (hereinafter CJEU) jurisprudence and, concretely, to *Digital Rights Ireland* and to *Watson and Others*. The latter in particular ordered the United Kingdom to adjust its national legislation by 1st November 2018 so as to strictly limit the access of police corps to telecommunication data to fight serious crime. Such access should be subject to a prior review conducted by a judicial authority or an independent administrative body, while forbidding any transfer of data outside the European Union (§ 463). By doing so, the ECtHR condemns the United Kingdom for violating Article 8 of the ECHR, without entering into further analysis (§ 468).

ANALYSIS

In *Big Brother Watch*, the ECtHR shows a certain unpreparedness by relying on its previous jurisprudence on bulk interceptions. As a consequence, it emphasises more and more on the CJEU case-law that, on the contrary, is advancing rapidly.

[8] The ECtHR stand out three types of United States-United Kingdom data exchanges: material which the National Security Agency (NSA) had provided to the United Kingdom intelligence services unsolicited, and which on its face derived from intercept; communications which the United Kingdom intelligence services had either asked the NSA to intercept, or to make available to them as intercept; and material obtained by the NSA other than by the interception of communications (§ 417). Considering the former "implausible and rare", the ECtHR focused its attention on the last two options.

[9] As it was analysed in *Malone v the United Kingdom* and *Ben Faiza v France*.

Firstly, and as for the analysis of section 8(4) RIPA, it is regrettable that the ECtHR rejects the applicants' petition to add two further criteria to the "Weber criteria", namely: the evidence of reasonable suspicion in relation to the persons for whom the data has been viewed; a prior and independent judicial authorization to issue the interception orders, and a subsequent notification at the end of the monitoring activity (§ 316-320). While the former and the latter are deemed to be incompatible with bulk interception regime for its own nature – i.e., being by definition untargeted –, the ECtHR admits that, although a judicial authorisation would not be *per se* incompatible, it is not necessary (§ 320) in case an administrative independent body exists. Nevertheless, these allegations are not out of place. Already in *Digital Rights Ireland* the CJEU found disproportionate the fact that the collection of data was directed even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime[10]. Furthermore, in *Watson and Others* it maintained that the necessity of a subsequent notification shall be granted unless it undermines the investigations conducted by the national authority[11]. What the ECtHR and the CJEU have in common is that none of them has so far affirmed, the necessity that a judicial authority shall monitor *ex ante* a surveillance order, being an independent administrative body sufficient[12].

Secondly, the position assumed by the ECtHR is regrettable in the light of the international data transfer regime between the United States and the United Kingdom. Transposed to the EU regime, the CJEU would benefit of an important advantage compared to the limited jurisdiction exercised by the ECtHR since the General Data Protection Regulation (GDPR) clearly extends its scope to the processing of activities conducted by controllers or processors established outside the European Union concerns "the monitoring of their behaviour as far as their behaviour takes place within the Union"[13]. This implies the possibility to outsource the European Union parameters overseas – as the *Schrems I* and *Schrems II* echo – which is not feasible under the ECHR. In this sense, the ECtHR remains more respectful of third countries' sovereignty, but lacks appropriate guarantees that may lastly legitimise the circumvention of European protective standards.

Finally, I shall point out that real-time collection of data – traffic data and the location of terminal equipment – has been only recently addressed by the CJEU. In *La Quadrature du Net* the CJEU has differentiated it from a non real-time access because of its major degree of intrusiveness while stating that such measures can only be taken in case of persons toward whom there is a valid reason for suspecting any kind of involvement in terrorist activities and, in any case, may be questioned in the light of current Article 79 GDPR. Yet, another crucial judgment was held behind the doors of the CJEU soon after *Big Brother Watch*: *Privacy International*. In this judgment, the CJEU rejected the lawfulness of the British Telecommunications Act 1984 on the ground that a generalised and undifferentiated disclosure to security and intelligence services of traffic and located data concerning the totality of the persons that use electronic communication systems, without even an indirect or remote link with the purpose of safeguarding national security, shall be considered disproportionated.

CONCLUSION

The ECtHR jurisprudence on strategic surveillance is progressively approaching the CJEU case-law. The dialogue between the two Courts allows the ECtHR to blindly rely on the CJEU e.g. on the interception communication regime of Chapter II RIPA that was already reappealed by the

[10] *Digital Rights Ireland*, para. 58.

[11] *Watson and Others*, para. 114.

[12] *La Quadrature du Net*, paras. 138 and 139.

[13] Article 3(2)(b) GDPR.

CJEU in *Watson and Others*. Nevertheless, the two courts rely on different protection standards for which the ECtHR comes to different outcomes especially in the light of the data transfer regime from the USA to the United Kingdom. Judges Pardalos and Eicke argue in their dissenting opinion that the role of the ECHR is to set minimum standards and cannot fully rely on the CJEU jurisprudence. To this statement I shall add that the United Kingdom has a special position in the data protection era – see Protocol 21 to the Lisbon Treaty and the reservation to the Charter. Despite this, Judges Koskelo and Turković complain a lack of control conducted by a judicial body authorising the issuing of a surveillance order, which shall also be extended to the United States-United Kingdom data sharing regime. All in all, *Big Brother Watch and others v. The United Kingdom* is offering the ECtHR the great opportunity to revise its jurisprudence in the light of the "sea change" of technological developments that turned our reality into the new digital age we are living in. The long-awaited final judgment of the Great Chamber may still mark a turning point in this regard.