Insights into ERA Seminar on Privacy and Data Protection with a Specific Focus on "Balance between Data Retention for Law Enforcement Purposes and Right to Privacy" (Conference Report)

This report has been prepared by Priyanka Jain*, a researcher at the Max Planck Institute Luxembourg for International, European and Regulatory Procedural Law, and Ph.D. candidate at the University of Luxembourg.*

Introduction:

On 9-11 December 2020, ERA – the Academy of European Law – organized an online seminar on "Privacy and Data Protection: Recent ECtHR & CJEU Case Law". The core of the seminar was to provide an update on the case law developed by the European Court of Human Rights (ECtHR) and by the Court of Justice of the European Union (CJEU) with relevance for privacy and data protection law since 2019. The key issues discussed were the distinction between the right to privacy and data protection in the jurisprudence of the ECtHR and CJEU, the impact of the jurisprudence on international data transfers, notions of 'essence of fundamental rights' 'personal data processing', 'valid consent' and so on.

Day 1: Personal Data Protection and right to privacy

Gloria González Fuster (Research Professor, Vrije Universiteit Brussel (VUB), Brussels) presented on the essence of the fundamental rights to privacy and data protection in the existing legal framework with a specific focus on the European Convention on Human Rights (Art. 8 of ECHR) and the Charter of Fundamental Rights of the EU (Art. 7, Art. 8)

Article 8 of the Convention (ECHR) guarantees the right to respect private and family life. In contrast, Art 52(1) EU Charter recognizes the respect for the essence of the rights and freedoms guaranteed by the Charter. Both are similar, but not identical. This can be validated from the following points:

- As per Art 8 (2) ECHR – there shall be no interference with the exercise of this right except such as in accordance with the law, whereas Art 52 (1) states that any limitation to the exercise of right and freedoms recognized by the Charter must be provided for by law.
- The Art 8 (2) ECHR stresses the necessity in a democratic society to exercise such an interference, whereas Art 52(1) of the EU Charter is subject to the principle of proportionality.
- Respect for the essence of rights and freedoms is mentioned in Art 52 (1) but not mentioned in Art 8 (2).
- Also, Art 8 (2) states that the interference to the right must be only allowed in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or the protection of the rights and freedoms of others. At the same time, Article 52 (1) states that any limitations to rights must meet objectives of general interest recognized by the Union or the need to protect others' rights and freedoms.

In the Joined Cases C?293/12 and C?594/12, *Digital Rights Ireland*; the Court addressed the interferences to the rights guaranteed under Articles 7 and 8 caused by the Data Retention Directive. An assessment was carried out as to whether the interferences to the Charter rights were justified as per Article 52(1) of the Charter. In order to be justified, three conditions under Article 52(1) must be fulfilled. The interference must be provided for by law, and there must be

respect for the essence of the rights, and it must be subject to the principle of proportionality. Certain limitations to the exercise of such interference/ infringement must be genuinely necessary to meet objectives of general interest. The Directive does not permit the acquisition of data and requires the Member States to ensure that 'appropriate technical and organizational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of data' and thus, respects the essence of the right to privacy and data protection. The Directive also satisfied the objective of general interest as the main aim of the Directive was to fight against serious crime, and it was also proportional to its aim of need for data retention to fight against serious crimes. However, even though the Directive satisfied these three criteria, it did not set out clear safeguards for protecting the retained data, and therefore it was held to be invalid.

It is pertinent to note here that the ECHR does not contain any express requirement to protect the 'essence' of fundamental rights, whereas the Charter does. However, with regard to Art 8 of the ECHR, it aims to prohibit interference or destruction of any rights or freedoms with respect for private and family life. This can be possibly interpreted so as to protect the essence of the fundamental right of private and family life. This is because a prohibition of the destruction of any right would mean affecting the core of the right or compromising the essence of the right.

Gloria, also examined Article 7 of the Charter, which guarantees a right to respect for private and family life, home and communications, and Article 8, which not only distinguishes data protection from privacy but also lays down some specific guarantees in paragraphs 2 and 3, namely that personal data must be processed fairly for specified purposes. She analyzed these Charter provisions concerning the Regulation (EU) 2016/679 (GDPR). GDPR creates three-fold provisions by imposing obligations on the data controllers, providing rights to data subjects, and creating provision for supervision by data protection authorities.

She also addressed the balance between the right to privacy and the processing

of personal data of an individual on one hand and the right to information of the public on the other. Concerning this, she highlighted the interesting decision in C-131/12, *Google Spain*, wherein it was stated that an interference with a right guaranteed under Article 7 and 8 of the Charter could be justified depending on the nature and sensitivity of the information at issue and with regard to the potential interest of the internet users in having access to that information. A fair balance must be sought between the two rights. This may also depend on the role played by the data subject in public.

It was also discussed in the judgments C-507/17, *Google v CNIL*; and Case C-136/17 that a data subject should have a "right to be forgotten" where the retention of such data infringes the Directive 95/46 and the GDPR. However, the further retention of the personal data shall only be lawful where it is necessary for exercising the right of freedom of expression and information. The ruling was on the geographical reach of a right to be forgotten. It was held that it is not applicable beyond the EU, meaning that Google or other search engine operators are not under an obligation to apply the 'right to be forgotten' globally.

In the next half of the day, Roland Klages, Legal Secretary, Chambers of First Advocate General Szpunar, Court of Justice of the European Union, Luxembourg, presented on the topic: "The concept of consent to the processing of personal data". He started with a brief introduction of GDPR and stated that there is no judgment on GDPR alone as it has been introduced and implemented recently, but there are judgments based on the interpretation of Directive 95/46 and the GDPR simultaneously. He commented on the composition of the ECJ, which sits in the panel of 3,5, 15 (Grand Chamber), or 27 (Plenum) judges. The Grand Chamber comprises a President, vice-president, 3 presidents of a 5th chamber, rapporteur, another 9 judges, appointed based on re-established lists (see Article 27 ECJ RP).

He discussed the following cases in detail:

C – 673/17 (*Planet49*): Article 6(1) (a) GDPR states that the processing of data is lawful only if the data subject has given consent to the processing of personal data for one or more specific purposes. "Consent" of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's

wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[1] This clearly indicates that consent is valid only if it comes from the active behavior of the user as it indicates the wishes of the data subjects. A consent given in the form of a pre-selected checkbox on a website does not amount to active behavior. It also does not fulfill the requirement of unambiguity. Another important aspect of the ruling was that it does not matter if the information stored or retrieved consists of personal data or not. Article 5(3) of Directive 2002/58/ EC (Directive on privacy and electronic communications)protects the user from interference with their private sphere, regardless of whether or not that interference involves personal or other data. Hence, in this case, the storage of cookies at issue amounts to the processing of personal data. Further, it is also important that the user is able to determine the consequence of the consent given and is well informed. However, in this case, the question of whether consent is deemed to be freely given if it is agreed to sell data as consideration for participation in a lottery is left unanswered.

Similarly, in case C -61/19 (Orange Romania), it was held that a data subject must, by active behavior, give his or her consent to the processing of his or her personal data, and it is upto the data controller, i.e., Orange România to prove this. The case concerns contracts containing a clause stating that the data subject has been informed about the collection and storage of a copy of his or her identification document with the identification function and has consented thereto. He also discussed other cases such as case C-496/17, Deutsche Post, and C- 507/17, Google (discussed earlier), demonstrating that consent is a central concept to GDPR.

Day 2: "Retention of personal data for law enforcement purposes."

On the next day, Kirill Belogubets, Magister Juris (Oxford University), case lawyer at the Registry of the European Court of Human Rights (ECtHR), started with a

presentation on the topic**:**

“Retention of personal data for combating crime.”

Kirill Belogubets discussed the case of *PN v. Germany*. No. 74440/17 regarding the processing of personal identification of data in the context of criminal proceedings. In this case, a German citizen was suspected of buying a stolen bicycle. Authorities collected an extensive amount of data such as photographs, fingerprints, palm prints, and suspect descriptions. It must be noted here that with regard to the right to respect for private life under Article 8 of the ECHR, the interference must be justified and fulfill the test of proportionality, legitimacy, and necessity. The authorities expounded on the likelihood that the offender may offend again. Therefore, in the interest of national security, public security, and prevention of disorder and criminal offenses, it is essential to collect and store data to enable tracing of future offenses and protect the rights of future potential victims. Thus, the collection and storage of data in the present case struck a fair balance between the competing public and private interests and therefore fell within the respondent State’s margin of appreciation.

With respect to margin of appreciation, the case of *Gaughran v. The United Kingdom*, no. 45245/15was also discussed. This case pertains to the period of retention of DNA profiles, fingerprints, and photographs for use in pending proceedings. The Court considered storing important data such as DNA samples only of those convicted of recordable offences, namely an offense that is punishable by a term of imprisonment. Having said that, there was a need for the State to ensure that certain safeguards were present and effective, especially in the nature of judicial review for the convicted person whose biometric data and photographs were retained indefinitely.

However, it has been highlighted that the legal framework on the retention of DNA material was not very precise. It does not specifically relate to data

regarding DNA profiles and there is no specific time limit for the retention of DNA data. Similarly, the applicant has no avenue to seek deletion because of the absence of continued necessity, age, personality, or time elapsed. This has been laid down in the case of *Trajkovski and Chipovski v. North Macedonia*, nos. 53205/13 and 63320/13.

Mass Collection and Retention of Communications data

In the next half, Anna Buchta, Head of Unit "Policy & Consultation", European Data Protection Supervisor, Brussels brought the discussion on Article 7 and 8 of the Charter and Article 8 of the Convention along with the concept of 'essence' of fundamental rights, back to the table. With regard to this discussion, she described the case C-362/14 *Maximilian Schrems v DPC*, which highlights that 'any legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.' In this context, EU member states must recognize the confidentiality of communication as a distinct legal right. In this case, it was the first time where a Directive was invalidated due to non-confirmation with the ECHR. It was laid down that the safe harbor principles issued under the Commission Decision 2000/520, **pursuant to** Directive 95/46/EC does not comply with its Article 25(6), which ensures a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order. The Decision 2000/520 does not state that the United States, infact, 'ensures' an adequate level of protection by reason of its domestic law or its international commitments.

Traffic and Location data

She also commented on the indefinite retention of data, which might lead to a feeling of constant surveillance leading to interference with freedom of expression in light of CJEU cases C-203/15 and C-698/15 *Sverige and Watson*. In these cases, the Court agreed that under Article 15(1) of the Directive 2002/58 / EC, data retention could be justified to combat serious crime, national security, protecting the constitutional, social, economic, or political situation of the country

and preventing terrorism. However, this must only be done if it is limited to what is strictly necessary, regarding categories of data, means of communication affected, persons concerned, and retention period. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the transmission of a communication without prejudice to paragraphs 2, 3, and 5 of this Article 6 and Article 15(1) of the Directive. This was reiterated in C-623/17 *Privacy International.* It must be noted here that these data can be retained only if there is evidence that these data constitute an identifiable link, at least an indirect one, to criminal activities. Data with regard to the geographical location again requires objective factors. It must be retained if there exists a risk of criminal activities in such areas. These locations may correspond to places that are vulnerable to the commission of serious offenses, for instance, areas that receive a large number of people, such as airports, train stations, toll-booth areas, etc.

The Court differentiated between generalized and targeted retention of data. Real-time collection and indeterminate storage of **electronic communications surveillance involving** traffic and location data of specific individuals constitute targeted retention. In this context, the case of C?511/18, C?512/18 and C?520/18, *La Quadrature du Net and Others* were also relied upon, with a focus on the following findings:

Targeted real-time collection of traffic and location data by electronic communication providers that concerns exclusively one or more persons constitutes a serious interference that is allowed where:

- Real-time collection of traffic and location data is limited to persons in respect of whom there is a valid reason to suspect that they are directly or indirectly involved in terrorist activities. With regard to persons falling outside of that category, they may only be the subject of non-real-time access.
- A court or an administrative authority must pass an order after prior review, allowing such real-time collection. This must be authorized only within the limits of what is strictly necessary. In cases of duly justified

urgency, the review must take place within a short time.

- A decision authorizing the real-time collection of traffic and location data must be based on objective criteria provided for in the national legislation, which must clearly define the circumstances and conditions under which such collection may be authorized.
- The competent national authorities undertaking real-time collection of traffic and location data must notify the persons concerned, in accordance with the applicable national procedures.

Last but not least, the EU Commission as well as the CJEU have started looking at the national laws of data retention and specifically inclined to define national security in manner so as to increase their own role in the area. However, data retention schemes are divergent across the Member States. It is essential to create clearer and more precise rules at the European level to enable the Courts to develop the best ways to strike a balance between the interactions of privacy rights with the need to tackle serious crime. The different legal rules in the area of data retention restricted cooperation between competent authorities in cross-border cases and affected law enforcement efforts. For instance, some Member States have specified retention periods, whereas some do not, a fact from which conflict-of-laws problems may arise. While some Member States for example Luxembourg precisely define 'access to data', there are Member States, which do not. This was pointed out by the EU Council in the conclusion of the data retention reflection process in May 2019, wherein it was emphasized that there is a need for a harmonised framework for data retention at EU level to remedy the fragmentation of national data retention practices.

Day 3: Data Protection in the Global Data Economy

The discussion of the third day started with a presentation by Professor Herwig Hofmann, Professor of European and Transnational Public Law, the University of Luxembourg on the well-known *Schrems*cases namely, C-362/14, *Schrems I*;

C-498/16, *Schrems vs Facebook;* and C-311/18, *Schrems II;*which involves transatlantic data transfer and violation of Article 7 and 8 of the Charter. In the clash between the right to privacy of the EU and surveillance of the US, the CJEU was convinced that *any* privacy agreements could not keep the personal data of EU citizens safe from surveillance in the US, so long as it is processed in the US under the country's current laws. The guidelines in the US for mass surveillance did not fit in the EU. Therefore, privacy shield could not be maintained.

He also highlighted that international trade in today's times involves the operation of standard contractual terms created to transfer data from one point to another. Every company uses a cloud service for the storage of data, which amounts to its processing. It is inevitable to ensure transparency from cloud services. The companies using cloud services must require transparency from cloud services and confirm how the cloud service will use the data, where would the data be stored or transferred.

In the last panel of the seminar Jörg Wimmers, Partner at TaylorWessing, Hamburg, spoke about the balance between **Data protection and copyright.**

The case discussed in detail was C-264/19 *Constantin Film Verleih GmbH***,** which was about the prosecution of the user who unlawfully uploaded a film on YouTube, i.e., without the copyright holder's permission. In this regard, it was held that the operator of the website is bound only to provide information about the postal address of the infringer and not the IP address, email addresses, and telephone numbers. The usual meaning of the term 'address' under the Directive 2004/48 (Directive on the enforcement of Intellectual Property rights) refers only to the postal address, i.e., the place of a given person's permanent address or habitual residence. In this context, he also commented on the extent of the right to information guaranteed under Article 8 of the said Directive 2004/48. This was done by highlighting various cases, namely, C-580/13, *Coty* and C-516/17, *Spiegel Online*, noting that Article 8 does not refer to that user's email address and phone number, or to the IP address used for uploading those files or that used when the user last accessed his account. However, Article 8 seeks to reconcile the right to information of the rightholder/ intellectual property holder and the user's right to privacy.

Conclusion:

To conclude, the online seminar was a total package with regard to providing a compilation of recent cases of the ECtHR and CJEU on data protection and the right to privacy. A plethora of subjects, such as the balance between data protection and intellectual property rights, privacy and data retention, and respect for the essence of fundamental rights to privacy, were discussed in detail. The data retention provision established by the new Directive on Privacy and Electronic Communications may be an exception to the general rule of data protection, but in the current world of Internet Service providers and telecommunication companies, it may not be easy to ensure that these companies store all data of their subscribers. Also, it is important to ensure that data retained for the purpose of crime prevention does not fall into the hands of cybercriminals, thereby making their jobs easier.

[1] Article 4 No.11 GDPR