North American Academic Research

Contents lists available at : www.twasp.info
Journal homepage: http://twasp.info/journal/home

Research

Data Protection Rights & National Security Objectives: Critical Analysis of ECtHR and CJEU Case Law

Hassan Syed[1*]
[1]*Graduate Law Studies, BPP Law School, UK*

[*]**Corresponding Author :**
H Syed
Email: h.syed2@my.bpp.com

Published online : ***19 March, 2019***

Abstract: *The present heightened environment of the so-called 'global war on terrorism' has pushed the national security and public safety to forefront of strategic policy and legislative agendas. The human rights in general and data protection rights in particular have paled in contrast to the state security agencies intrusions in available digital data of the citizens. It is then left up to the Courts such as the European Court of Justice ('**CJEU/ECJ'**) Luxembourg and the European Court of Human Rights ('**ECtHR**') Strasbourg to avail opportunities presented to them in their justiciability of data protection rights interferences. Both the Courts apply the European Charter for Fundamental Rights ('**the Charter**') and the European Convention on Human Rights ('**the Convention'**) respectively to carry their analysis of rights interferences with the legitimate objectives of national security and public safety. Our critical analysis of the data protection case law of both the Courts confirms that the Courts have struck a balance in protecting the individual data protection rights and the legitimate aims of national security and public safety. Our analysis shows that it was ECtHR that laid the foundation of applying the principles of necessity and proportionality consistently in its analysis of interferences with Article 8 Convention rights in pursuing the aims of fighting serious crime and terrorism[1]. ECJ has followed ECtHR's reasoning of necessity and proportionality in its landmark judgments of Digital Ireland[2], Schrems[3] and Watson[4]. The ECJ was confronted with the questions of blanket coverage allowing mass surveillance and access to users' data by the state security agencies under the EU Directives. ECJ declared such measures invalid ,failing the necessity and proportionality tests in the absence of legal measures that could protect those who did not fall into the category of suspects defined under the law. ECJ accepted such interferences with Article 7 (right to*

[1] ECtHR Klass v. Germany, (App no. 5029/71, Judgment Sep 6, 1978
[2] ECJ Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238 ("Digital Ireland")
[3] ECJ Schrems v Data Protection Commissioner C-362/14 ("Schrems")
[4] ECJ Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others ECLI:EU:C:2016:970 ("Watson")

privacy) and 8 (right to data protection) Charter rights necessary in pursuits of aims to fight serious crime and terrorism. The requirement of a robust legal framework that justifies ECHR Art 8 Privacy rights interferences[5] with data protection, has been accepted by the Court as necessary in the face of security challenges such as fighting terrorism and prevention serious transnational crimes. ECtHR also considers the availability of national legal remedies for interferences through independent bodies in its analysis of necessary and proportional in a democratic society. ECJ has also laid emphasis on availability of legal remedies[6] in cases of interferences with data protection rights while interpreting EU Legislations in the light of rights under Art 8 CFR. While ECJ protects data rights under CFR Art 8 Data Protection Right, ECtHR extends ECHR Art 8 Right to Privacy to protect data rights. Both the Courts readily acknowledge the society's needs to fight serious crimes and terrorism in their case law. It is the balance that both the Courts strike while relying on the principles of necessity and proportionality that ensures the protection of data rights of those who abide by the rule of law in a democratic society.

***Keywords**: Data Protection, EU Law, National Security, European Courts, Data Protection Rights*

I- Introduction

The fundamental rights interferences pertaining to mass data collection, retention and access that have taken place under the shield of various national legislations that were enacted in Europe and North America as a consequence to the so-called '*global war on terror'* post 9/11 are slowly surfacing. Extra-judicial killings using Drone technology[7], illegal rendition of suspects by the state agencies with the complicit cooperation of EU member states are some of the extreme examples of such rights violations involving users data (All through the paper we will use the terms 'user data', 'data subject' and 'users' interchangeably). Revelations by NSA ex security contractor Edward Snowden[8], Wikileaks[9], Ex FBI Agent Sibel Edmond's Boiling Frog Posts[10] are all examples that elucidate fundamental rights interferences through mass retention of user's data, its access and exchange between intelligence agencies as the central theme. Artificial Intelligence based data application for almost every sphere of human life is now the norm[11]. At the core of all this technological advancement is user data. Scenarios have been depicted in war game rooms across nations about the impact of a global

[5] ECtHR Centrum For Rattvisa v Sweden App no. 35252/08

[6] ECJ Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238 para 68

[7] Telecoms share users data used in Drone Attacks and Rendition: Source https://reprieve.org.uk/press/2014_11_05_BT_OECD_intelligence_sharing_drones/

[8] Edward Snowden: 'The 29-year-old source behind the biggest intelligence leak in the NSA's history explains his motives, his uncertain future and why he never intended on hiding in the shadows'. Source: The Guardian https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

[9] Wikileaks: Spy Files https://www.wikileaks.org/spyfiles/russia/releases/

[10] Boiling Frog: Data Retention https://boilingfrog.com.au/new-data-retention-law-seriously-invades-privacy-time-took-action/

[11] McKinsey Institute: https://www.mckinsey.com/featured-insights/digital-disruption/whats-now-and-next-in-analytics-ai-and-automation

crashing of data servers[12]. It is a catastrophic scenario for which there are limited solutions. From travel to healthcare and from personal choices to strategic warfare decisions, the entire services and their decision-making matrix depends upon the ability of the applications to timely analyse the patterns within the users' data[13].

In the midst of such extreme competing interests, it is no easy task advocating the protection of individual's fundamental rights pertaining to his/her data. The task becomes even more difficult when in some cases the *Legislature* supports and empowers the *Executive* to wage unlimited wars on unknown enemies. It is then up to the *Judiciary* to ensure the *Rule of Law* under the *Principles of Natural Justice*. The results of on-going conflicts in Afghanistan, Iraq, Syria, Libya, Yemen and Palestine are a case in point[14]. US, UK, Canada and EU citizens with dual nationalities from these war zones are some of the worst victims of the mass data surveillance, retention, and access by security agencies[15].

The International Courts such as the European Court of Human Rights (ECtHR), Strasbourg and the European Union Court of Justice (ECJ) Luxembourg ('the Courts') are faced with the challenges to protect the data rights of individuals against the state machinery with its vast apparatus of security agencies working under legislative protection or executive orders. The Courts have to strike a balance between protecting the fundamental rights of the individuals and the legitimate national security and public safety objectives of the state.

The central theme of the essay is that through our critical analysis of ECtHR and ECJ case law on mass data retention and its access by state security agencies, we argue, that both the Courts have indeed struck the right balance in protecting the data subject's right with the objectives of public safety and national security based on the Principles of the Rule of Law and Natural Justice. The balance has been a difficult one in this heightened environment of the so-called 'global war on terrorism'. In striking that balance, the Courts have at times drawn criticism for 'competence creep[16]' in annulling legislations that are incompatible with

[12] Global Crashing of Data Servers: Source: https://www.knoxnews.com/story/news/politics/2018/05/11/global-cyberassault-caused-knox-county-election-night-server-crash/602009002/

[13] 'Why Data is a Big Deal': Article Source https://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal

[14] Human Rights Watch Report- "'According to the Syrian Center for Policy Research, an independent Syrian research organization, **the death toll from the conflict as of February 2016 was 470,000**. The spread and intensification of fighting has led to a dire humanitarian crisis, with **6.1 million internally displaced people and 4.8 million seeking refuge abroad'**, according to the UN Office for the Coordination of Humanitarian Affairs'". Source: https://www.hrw.org/world-report/2017/country-chapters/syria

[15] Mass Data Retention Impacts: Source https://www.eiuperspectives.economist.com/technology-innovation/digital-identity-%E2%80%93-precarious-balancing-act

[16] PhD Thesis- 'Competence Creep': 'With the growing awareness in EU external relations that the existence of Member States' competence does not necessarily allow them to freely exercise such competence, the duty of

the European Convention on Human Rights ('ECHR') or European Union Charter of Fundamental Rights('CFREU, CFR'). Our critical analysis also shows that since the adoption of CFR within the EU, the ECJ judgments have shown a progressive and inclusive analysis of data rights protection while interpreting *both* CFR and ECHR. While Snowden and other revelations may have shed light for the general public, on the covert surveillance of users' communication data and its access, our analysis reveals that ECtHR especially in not new[17] to this topic. In our analysis, these revelations have added *another* dimension to '*how*' this massive body of user's data is being handled within the realm of national security.

The focus of our critical study is both the Courts in their analysis highlight the principles of necessity, proportionality and legitimacy of aims pursued to justify interference with data protection rights in a democratic society. Our analysis will also show that both the Courts refer to each other's case law in order to explore the reach of data rights protection. We start our analysis by taking a brief look at the two separate systems of fundamental rights which is the jurisprudence of the ECJ and the ECtHR . Acknowledging the vast body of case law available on the topic, we have mostly relied on landmark cases pertaining to mass collection, retention and access of personal data for national security and public safety from both the courts to support our analysis.

II- *Universal* nature of ECHR and *Supranational* nature of CFR

The European Convention on Human Rights[18] ('the Convention') is a 1950 instrument of the Council of Europe[19] that has been adopted by 47 countries[20] recognized as 'High Contracting Parties'. This includes the 27 members[21] of the European Union ('EU')[22]. The rights defined under the European Convention of Human Rights (ECHR) are recognized as fundamental and common to *all* human beings irrespective of their national, social or legal order to which they may belong. This defines the '*Universal*' nature of the Convention rights. The European Court of the Human Rights (ECtHR) Strasbourg has the sole jurisdiction on all matters related to rights under ECHR. There is no separate data protection right available within

---

sincere cooperation laid down in Article 4 (3) TEU is increasingly becoming the focus of academic attention.': **Citation** : Florence : European University Institute, 2013, **Author** Reuter, Kristin. **Source**: http://hdl.handle.net/1814/28050

[17] ECtHR Klass v. Germany, (App no. 5029/71, Judgment Sep 6, 1978): 'Case of secret surveillance of citizens by state secret police without sufficient judicial oversight.'

[18] 'ECHR 1950' Document: Source- https://www.echr.coe.int/Documents/Convention_ENG.pdf

[19] 'The Council of Europe Strasbourg': Source- https://www.coe.int/en/web/portal/home/

[20] 'ECHR 47 High Contracting Parties List': Source- https://www.coe.int/en/web/portal/47-members-states

[21] The 27 Members of the EU and their years of entry into EU: Source- https://europa.eu/european-union/about-eu/countries_en

[22] 'About the EU': Source- https://europa.eu/european-union/about-eu_en

ECHR because of its drafting in an era when data had limited meaning within the context of technology and personal data. Therefore, data protection emerges as a subset of Article 8 right to privacy in the majority of recent case law related to data protection.

The EU Charter of Human Rights ('the Charter')[23] is uniquely democratic as all member states at the time of its drafting took part in its formulation. The European Charter of Human Rights (CFR) protects right to privacy under Article 7 and the protection of data is recognized as a separate right under Article 8. Article 6(1)[24] Treaty of the European Union ('TEU') states that 'the Charter has the same status as other treaties of the EU and is legally binding on all member states'. The Charter is a 'supranational' instrument that allows the European Court of Justice (ECJ), Luxembourg to guarantee fundamental rights within the EU. ECJ recognises Convention Rights as principally applicable within the body of EU law[25]. Article 6(3)[26] TEU defines Convention Rights as the general principle of EU law.

The 'personal data' in the Strasbourg[27] and Luxembourg[28] has a similar and broad meaning. It is defined as information relating to an identified or identifiable person. What *constitutes* personal data for the purposes of national security and public safety is a non-exhaustive list in the case law of ECtHR and ECJ[29]. Sensitive personal Data has a broad meaning also in the case law of ECJ where it has been shown to include medical records[30] and letter about a work e-mail[31]. ECtHR measures the sensitivity by the relevance in terms of privacy and its impact on a person's private life[32].

---

[23] 'EUCFR Document' : Source- http://www.europarl.europa.eu/charter/pdf/text_en.pdf

[24] Article 6(1)TEU: 'The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted on 12 December 2007, which shall have the same legal value as the Treaties.'

[25] ECJ Nold v Commission (Case 4/73) [1974] ECR 491: 'The Court recognized as the basis for the protection of rights within the EU'. 'Internationale Handelsgesellschaft v Einfuhr und Vorratstelle fur Getreide und Futtermittel (Case 11/70) [1970] ECR 1125:'ECJ declared that fundamental rights were part of the 'general principles' of the EU law'.

[26] Article 6 (3) TEU: 'Fundamental Rights as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedom and as they result from the constitutional traditions common to all the Member States, shall constitute general principles of the Union law'.

[27] Data Protection Convention 108, Strasbourg 1981:
Source:http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

[28] Directive 95/46/EC : 'EU Data Protection Directive for processing of personal data and the free movement of such data'.

[29] **ECtHR & ECJ Cases- GPS Surveillances** ;Uzan v Germany App no 35623/05, IHRL 1838 (ECHR 2010) on **DNA** Storage; S. and Marper v UK (App nos. 30562/04 and 30566/04) on **Mobile Phone Location**; Ben Faiza v France (Appl no. 31446/12) on Secret Phone Surveillances; **Letters** Klass and Others v Germany App no 5029/71 **E-Mails** Monika Esch-Leonhardt, Tillmann Frommhold and Emmanuel Larue v European Central Bank Case No. T-320/02, **Surname** McCullough v Cedefop T-496/13

[30] ECJ Lindquist C -101/01, para 50-51,

[31] ECJ Esch-Leonhardt Case No. T-320/02

[32] ECtHR M.M. v UK App No. 24029/07 para 188: Past criminal record becomes part of person's private life

The ECJ has jurisdiction to give preliminary ruling is under Article 267 TFEU[33] (ex Article 234 TEU). ECJ has limited jurisdiction in matters of national security of its member states under Article 2(4) TFEU[34]. The member states have autonomy in matters of Area of Freedom, Security and Justice ('AFSJ') under Article 72 TFEU[35]. ECtHR has competence in matters of national security of its High Contracting Parties pertaining to Convention Rights[36]. Matters of rights violation can be brought before the ECtHR under Art 34[37] ECHR against the High Contracting Parties. ECtHR gave a precise judgment[38] under Art 35 Admissibility Criteria that clarified individual's ability to access the Court in matters of rights violations.

III- ECJ - Balancing Data Protection Rights under Art 7 & 8 CFR

While ECJ has paid particular attention to fundamental rights protection since 9/11, ECJ seems to have accorded urgency to the matters of data protection and privacy post Snowden revelations (2014-2015 period).The average time to decide rights violations in the cases of data protection and privacy has been less than a year[39].

Art 7 of the Charter protects right to privacy and Art 8 exclusively addresses data protection. However, ECJ has drawn its definition of 'protection of data' from ECHR's right to privacy under Art 8 of the Convention as meaning right to private life includes data protection[40]. It stands to clarify that according to ECJ data protection and privacy are not interchangeable.

In Digital Ireland[41], the ECJ accepted that according to the EU Directive[42], Art 7 and 8 Charter rights are not absolute and accordingly interference with those rights can be justified

[33] Article 267 TFEU: 'The Court of Justice of the European Union shall have jurisdiction to give preliminary rulings concerning: (a) the interpretation of the Treaties (b) the validity and interpretation of acts of the institutions, bodies, offices or agencies of the Union'

[34] Article 2(4) TFEU: Title I Categories and Areas of Union Competence: 'The Union shall have competence in accordance with the provisions of the Treaty on European Union, to define and implement a common foreign and security policy, including the progressive framing of a common defence policy'.

[35] Article 72 TFEU (ex Article 64(1) and ex Article 33 TEU) Title V Area of Freedom, Security and Justice:' This Title shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safe guarding of internal security'.

[36] ECtHR Roman Zakhrov v Russia (App no. 47143/06) Judgment 4 Dec 2015: 'Mobile Operators in Russia were required by law install equipment to allow state security agencies to carry-out operation for the security purposes without any legal oversight'.

[37] Art 34 ECHR: 'The Court may receive applications from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the protocols thereto. The High Contracting Parties undertake not to hinder in any way the effective exercise of this right.

[38] ECtHR Schalk and Kopf v Austria App no. 30141/04**: '**A same-sex couple brought a discrimination application against the Austrian Government under Art 34 ECHR'.

[39] European Papers Vol 1, 2016, ISSN 2499-8249, pp369-373

[40]ECJ Joint cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR-I-11063, para 52

[41]ECJ Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238

[42] Directive 2006/24/EC, ("The Data Retention Directive" (OJ 2006 L 105/54))

to pursue legitimate aims to fight serious crime and international terrorism[43]. However, the Court clarified that those interference must follow the principles of proportionality in pursuing the legitimate objectives[44]. In applying the proportionality reasoning to analyse the legitimate aims of public safety ECJ referred to ECtHR's proportionality rationale as its basis, in which the undefined period of DNA retention[45] by the public authorities was found to be disproportionate and an interference with their Art 8 Convention rights. ECtHR had defined proportionality within the context of the harm of *stigmatization* of a person in cases of a '*blanket policy*' to retain DNA or finger prints in cases of criminal investigation by the police. ECJ applied a strict test for proportionality[46] to assess the data retention under the EU Directive 2006/24[47]. The first limb of the test applied the 'suitability' of the interference under the Directive 2006/24 pursing the public safety objectives. The second limb applied the proportionality analysis to establish the 'necessity' of the Directives interference within the interpretation of Art 8 Charter rights. The court found the interference 'suitable' as the objective was to fight serious crime under the Directive . However, the measures laid down for the 'mass retention of data' with no defined limits were found to be inadequate and thus failing the proportionality analysis of the necessity criteria[48]. In courts view inadequacy of having no defined limits as who's data could be retained and on what grounds amounted to an interference with the rights of the entire population of Europe[49]. The court declared the Directive 2006/24 invalid because of its failure to meet the proportionality under Art 7 and 8 CFR.

In PNR[50], the EU Parliament sought annulment of Council's decision[51] to share every EU passengers' data flying to and from the US in compliance with a US legislation. The Councils decision allowed the US Customs and Immigration to have full access to the passenger data.

[43]ECJ Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238 paras 41-44

[44]ECJ Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238 para 46

[45]ECtHR Joint cases S v United Kingdom App no. 30562/04 and Marper v United Kingdom App no. 30566/04 ,'In both cases the Police continued to hold the DNA data even after the proceedings were either discontinued or resulted in the acquittal of the data subject'.

[46]ECJ Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238 para 46-49

[47] Directive 2006/24/EC, ("the Data Retention Directive" (OJ 2006 L 105/54)) Article 1(1)

[48]ECJ Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238 para 48

[49]ECJ Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238 para 34

[50] ECJ Parliament v Council C-317 and C-318/04 ("PNR")

[51] Council Decision 2004/496/EC adopted on the basis of Directive 95/46 on the adequacy decision to transfer EU Passengers Name Records (PNR) for all flights from EU to the USA following a US statute enacted in Nov 2001 following 9/11 to fight global terrorism

ECJ recognized that the data was initially collected by private air carriers carrying out a commercial activity. However, the purpose of 'transfer' of that collected data to the US under the EU Regulation was to fight terrorism and transnational crime[52]. The Court carefully pointed out that the collection of commercial data by a private entity and its subsequent transfer to a third party for the purposes of fighting terrorism was excluded from the scope of the activities provided by the Directive[53]. This reasoning applied by the court annulled the 'adequacy decision'[54] of the council and the agreement itself. The ECJ without mentioning specifically mentioning the data protection rights carefully balanced the right to retain and transfer mass data to third parties for the purposes of fighting serious crime and terrorism.

In Schrems[55] the ECJ was asked that the Commission's decision to declare mass data transfer to the US *invalid* as the data was suspected to be accessed by the NSA covertly. ECJ carefully considered the powers of the Data Protection Authority ('DPA') under Article 8(3)[56] CFR. The Court first established its sole jurisdiction to declare the Commission's decision invalid[57]. The Court then declared the decision of the Commission invalid for trying to eliminate or reduce the powers of the DPA under Article 8(3) of the CFR and preventing the DPA to comply with Article 25(1) (Adequate level of Protection)[58] of the Directive 95/46. The Commissions 'Adequacy Decision' to prevent DPA from considering a claim from a data subject under Article 28(4)[59] of the Directive was found to be interfering with the fundamental right to protection of privacy and freedom. The Court then proceeded to examine 'Adequacy' requirements of level of data protection in the US under Article 25(6)[60]

[52] ECJ Parliament v Council C-317 and C-318/04 ("PNR") para 55-56

[53]EU Directive 95/46, Article 3(2) 'This Directive shall not apply to the processing of personal data: in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law; by a natural person in the course of a purely personal or household activity.'

[54] ECJ Parliament v Council C-317 and C-318/04 (PNR) para 57-61

[55] ECJ Schrems v Data Protection Commissioner C-362/14 ("Schrems")

[56]CFREU Article 8(3) Protection of Personal Data:' Compliance with these rules shall be subject to control by an independent authority'

[57] ECJ Schrems v Data Protection Commissioner C-362/14 ("Schrems") para 51-64

[58] Article 25(1) Directive 95/46:' The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an **adequate level of protection'.**

[59] Art 28(4) Directive 95/46:' Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim'.

[60] Art 25(6) Directive 95/46:' The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon

of Directive 95/46. The Court applied the principle of *necessity* and *proportionality* to analyse the US law in its ability to define limits of interference to pursue the legitimate aim of national security. The Court found the US Federal Telecommunication Commissions ('FTC') rules for interference with mass data exempting actions undertaken by the State. The inadequacies in US legislation failing the Courts necessity and proportionality analysis was found to be an interference with Art 8 CFR.

In Watson[61], the ECJ was confronted with the questions about the degree of effectiveness for data protection between CFR and ECHR. The Court was also asked about the legality of mass collection of metadata under national legislations following the EU's E-Directive[62] read in conjunction with CFR. The ECJ declared mass collection of metadata through national legislation following the Directive in breach of CFR. The Court defined mass collection of metadata as a '*serious interference'* with the privacy of data subjects. The Court recognized the importance of pursuing legitimate aims of fighting terrorism and serious crime to justify such interference. The Court then qualified the interference criteria by first subjecting such retention and access of data to have strict prior review by a Court or an Independent Authority. The second requirement laid down for such interference was to store all such data within the EU. The requirement of storage of data within the EU is in line with Courts decision in Digital Ireland[63]. The Court also established the standing of CFR as the most comprehensive authority on the matters of data protection and privacy while comparing CFR and ECHR[64]. The ECJ's decision in Watson[65] follows adherence to the principles of natural justice and rule of law in Digital Ireland[66], Schrems[67] and PNR[68].

---

conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals'

[61]ECJ Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others ECLI:EU:C:2016:970 ("Watson").

[62]EU Directive 2002/58 ("the e-Privacy Directive" (OJ 2002 L 201/37)) concerning the processing of personal data and the protection of privacy in the electronic communications sector.
Source- https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_en.pdf

[63]ECJ Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238 para 68

[64] ECJ Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others ECLI:EU:C:2016:970 ("Watson") ,paras 130-131 "The CJEU observed that Article 7 of the CFR 'has no equivalent in the ECHR' and that Union law is not precluded from 'providing protection that is more extensive than the ECHR'".

[65]ECJ Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others ECLI:EU:C:2016:970 ("Watson")

[66]ECJ Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238

[67] ECJ Schrems v Data Protection Commissioner C-362/14 ("Schrems")

[68] ECJ Parliament v Council C-317 and C-318/04 (PNR)

The ECJ was asked its opinion[69] on a draft Passenger Name Record (PNR) data transfer agreement between EU and Canada. The draft agreement is similar to the 2004 PNR agreement between EU and USA in compliance of a Nov 2001 US national security legislation requiring all international carriers flying in and out US to share their PNR data records with US Customs and Border Security Agency. The EU-Canada PNR agreement's scope was to 'regulate' exchange and processing of PNR data. The agreement also relied on Article 25 of Directive 95/46/EC after fulfilling the 'adequacy decision' of the third country's standards of data protection compatibility with EU standards. The standards can be testified by European Commission. The ECJ found mass transfer of PNR tolerable in the context of being a necessary tool to fight terrorism, but qualified necessary with a very strict implementation of rules to supervise such surveillance. In the absence of such provisions, the draft agreement was found to be incompatible with Art 7 and 8 read in conjunction with Art 52(1)[70] (Proportionality) of the CFR. ECJ in its reasoning relied on Schrems and Watson to point out that the draft agreement lacked a clear data retention framework. In Schrems and Watson ECJ had established that for personal data to be retained, there had to be a clear connection between the retained data and the objectives pursued for its retention. The Court also questioned the reason to transfer sensitive data such as ethnic background to Canada under the draft agreement under the general purpose to fight terrorism. Such data processing was prohibited under EU PNR Directive 216/681. ECJ quoting Watson clarified that disclosure of mass PNR data to Canada in not limited to the strict necessity principle. The obligation to disclose such data according to Watson is allowed under exceptional circumstances by a court or a Data Processing Authority. In case of third countries EU safeguards can be circumvented thus will be in breach of Art 8 CFR. This critical analysis by the ECJ in this recent mass data retention and transfer agreement with an objective to fight terrorism reflects the courts insistence on upholding the Charter rights with an objective review of the evolving security needs.

IV- ECtHR- Fundamental Right to Privacy Article 8 ECHR & Security Objectives

ECtHR accepts the state's obligation to fight serious crime and terrorism as an acceptable interference with Article 8 Convention right in cases of mass collection, retention and access

[69] ECJ Opinion 1/15 dated July 26, 2017 on 'the Draft Agreement between Canada and EU dealing with the transfer of Passenger Name Records (PNR) data from EU to Canada'. The draft agreement was referred by the European Parliament on January 30, 2015 to ECJ for Opinion.

[70] CFREU Art 52(1): 'Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the **principle of proportionality,** limitations may be made only if they are **necessary** and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.'

to users' data. ECtHR's adherence to the principles of necessity, proportionality in cases of data retention and access have been consistent for EU member states[71] operating under the EU Directives on data retention and non-EU[72] high contracting parties operating under ECHR. ECtHR also relied on reasons of inadequate legal measures for oversight and the non-availability of remedies for interference within the national laws as a reason for rights violations[73]. The reasoning of the lack of inadequate legal measures for oversight within the national law in cases of interference with data protection rights has a common thread with the reasoning given by ECJ in Digital Ireland and Watson.

ECtHR is currently reviewing important cases on Article 8 Convention rights[74] pertaining to mass collection, retention and access to personal data . The cases focus on mass data interceptions by the US and UK intelligence agencies following the Snowden revelations. Similar cases from France[75] on mass surveillance are under review. The Notices[76] issued by the Court raised questions of necessity and proportionality of such interferences in a democratic society.

ECtHR stresses the protection of 'privacy' in cases[77] of interference for public safety and national security. ECtHR has also linked person's information pertaining to past public safety records to be 'private'[78] and *protected* as part of 'privacy' under Art 8 convention rights. What is necessary in a democratic society is in the wording of Art 8(2)[79] of the Convention. The ECtHR in Handyside[80] clarified that "'necessary' was not synonymous with indispensable neither has it the flexibility of such expressions as "admissible", "ordinary",

[71] 'ECHR EU Members, ECtHR Cases on interventions with Art 8 Data Protection rights for Public Safety and National Security': Uzun v. Germany, Ben Faiza v. France, Malone v. the UK, Kruslin v. France, Amann v. Switzerland, Taylor-Sabori v United Kingdom

[72] 'ECHR Non-EU Members, ECtHR Cases on interventions with Art 8 Data Protection rights for Public Safety and National Security' :Roman Zakharov v. Russia , Khelili v. Switzerland, Mustafa Sezgin Tanrıkulu v. Turkey

[73] Roman Zakharov v Russia App no. 47143/06, Szabo and Vissy v Hungry App no. 37138/14, Mustafa Sezigin Tanrikulu v Turkey App no. 27473/06

[74] ECtHR Joint Cases Big Brother Watch and Others v UK App no 58170/13, Bureau of Investigative Journalism and Alice Ross v UK App no 62322/14 and Human Rights Organizations and Others v UK App no 24960/15

[75] ECtHR Assocation confranternelle de la presse judiciaire v France App no 49526/15

[76] ECtHR - On 7th Nov 2017 a Chamber hearing was held on the Notices issued by the Court to the UK in 58170/13, 62322/14 and 24960/15 on 9th Jan 2014, 5th Jan 2015 and 24th Nov 2015. Notice to the French Government for 49526/15 was made on 26 April 2017.

[77] ECtHR Amann v Switzerland App no 27798/95 and Rotaru v Romania App no 28341/95

[78] ECtHR MM v UK App no 24029/07

[79] Article 8(2) ECHR: 'There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country….'

[80] ECtHR Handyside v United Kingdom Appl. No. 5493/72

"useful", "reasonable" or "desirable"'[81]. ECtHR has recognized the evolving nature of fundamental rights under the Convention[82] and declared the Convention as a 'living instrument' to protect fundamental rights according to standards '*necessary*' in a democratic society'[83]. ECtHR considers data protection while applying Art 8 Convention right to privacy giving rise to data protection in its case law[84] as both the cases illustrate the Courts broad interpretation of the convention rights pertaining to privacy. This is perhaps because the Court's interpretation of data privacy follows the Convention 108[85] and that the Convention unlike the Charter has no fundamental rights for data protection.

ECtHR considers interference with Article 8 rights proportionate in cases of the state pursuing legitimate aims to prevent serious crime for short period (3 months) affecting only the person of interest[86]. Arbitrary secret surveillance by intelligence agencies[87] with no legal limits on their access to mass data is a serious interference with Art 8 rights according to ECtHR. National legislation to deploy cutting-edge technologies to fight terrorism[88] has been accepted as a legitimate aim by the Court. However, the lack of measures defined in the legislation to prevent blanket data access by the security agencies was found to be an interference with Art 8 Convention rights. The National court's decision[89] allowing interception of anyone's communication in Turkey for period of one and a half month was found in violation of Article 8 (and Article 13) Convention rights. ECtHR's balanced analysis in bulk interception of electronic signals in Sweden[90] for foreign intelligence purposes was found not to be a violation of Art 8 rights. The Courts analysis found that the national legislation had provided for an adequate system of judicial oversight for surveillance orders requiring a court review for renewal of such order and that the legislation also allowed a complaint mechanism that consisted of access to multiple independent entities. ECtHR has found violation of Art 8 rights in France, in instances where the real-time geolocation of

[81] ECtHR Handyside v United Kingdom Appl. No. 5493/72 Judgment 7 Dec 1976 para 48
[82] ECtHR Demir and Baykara v Turkey App no. 34503/97Judgment 12 Nov 2008
[83] ECtHR Demir and Baykara v Turkey (Application no. 34503/97) para.146 'The Convention is a living instrument which must be interpreted in the light of present-day conditions, and in accordance with developments in international law, so as to reflect the increasingly high standard being required in the area of the protection of human rights, thus necessitating greater firmness in assessing breaches of the fundamental values of democratic societies.'
[84] ECtHR Amman v Switzerland App No.27798/95 para 65 also see Rotaru v Romania App No. 28341/95 para43
[85] Council of Europe Data Protection Convention 108, Strasbourg 1981
[86] ECtHR Uzan v Germany App no 35623/05
[87] ECtHR Roman Zakharov v Russia App no. 47143/06
[88] ECtHR Szabo and Vissy v Hungary App no. 37138/14
[89] ECtHR Mustafa Sezgin Tanrıkulu v. Turkey App no. 27473/06
[90] ECtHR Centrum For Rattvisa v Sweden App no. 35252/08

individuals[91] was collected by the law enforcement to fight serious organized crime. The Courts reasoning was based on the absence of any national legislation to afford minimum protection afforded under the law, necessary in a democratic society. The Court further ruled that a court order issued in the same case to obtain the cell phone traffic data of the person was justified on the grounds to fight serious crime as the court issuing the order was in accordance with the law. The Court analysis to balance the interference with the rights for fighting serious drug crime under a legal framework with recourse to legal remedies reflects the Courts application of the principles of proportionality and necessity in a democratic society.

ECtHR's consideration of national security objectives especially terrorism is not a new occurrence. In Klass v Germany[92] the Court found no violations of Art 8 of the Convention. The Court carefully look at the German legislation to consider the interference in the interest of national security and the role of secret police surveillance. The Court did characterize the role of such surveillance as an action in a 'police state'. However, the Court acknowledged that democratic societies are threatened by sophisticated forms of terrorism therefore such interferences are necessary to counter such acts of terrorism. The Court qualified the allowance for such interference under exceptional conditions necessary in a democratic society to prevent acts of terrorism and in the interest of national security. This a controversial yet an important case in which ECtHR went to great lengths to justify intrusive surveillance activities as interferences *necessary* and *proportionate* in a democratic society.

ECtHR found violation of Art 8 of the Convention for the failure of the police to obtain a court order for accessing the Internet Protocol Address ('IP Address') of a suspect[93]. The IP address of the suspect was identified by a third-country's law enforcement while monitoring users of a certain file sharing network. The suspect was identified after sharing files that included child-pornography. The reasoning given by ECtHR identified the lack of legal framework to check any arbitrary interference and absence of any independent supervision of the police powers in obtaining personal data. There is consistency in ECtHR applying the availability of a legal framework to oversee interference with data protection rights along with the availability of an independent mechanism for remedies in its analysis of

[91] ECtHR: Ben Faiza v France App no. 31446/12
[92] ECtHR: Klass and Others v Germany App no. 5029/71
[93] ECtHR Benedik v Slovenia App no. 62357/14 Judgment 24.4.2018: 'Case concerned Slovenian police failing to get a court order to access the IP address of the suspect randomly caught by Swiss law enforcement while monitoring a file sharing site that included file sharing of child pornography'.

proportionality and necessity to pursue legitimate aims such as national security and public safety.

V-Conclusion

ECJ through its judgments following the principles of proportionality and necessity in Digital Ireland, Scherm and Watson paved the way for the adoption of the General Data Protection Regulation (GDPR)[94] through their balanced approach in guiding the EU Constitutional legislation in updating its data protection laws. ECtHR through its consistent approach of rejecting or allowing data rights interferences on its necessity and proportionality principles based on the robustness of the defined national legislation framework allowing such interferences provides the right balance in the universal interpretation of data protection rights globally. It is this fine balance that both the courts have achieved in protecting individual rights for data protection and the national security and public safety objectives which have helped shape the legislation in over 100 countries that are currently implementing data protection and privacy legislations.

Bibliography

Books

Woods L, Watson P & Costa M: *EU Law* 13th Edition Oxford University Press 2017
Loveland I: *Constitutional Law, Administrative Law, and Human Rights* 7th Edition Oxford University Press 2015

Cases/Opinions

ECtHR Klass v. Germany, (App no. 5029/71) Judgment 6 September 1978
ECJ Nold v Commission (Case 4/73) [1974] ECR 491
ECJ Internationale Handelsgesellschaft v Einfuhr und Vorratstelle fur Getreide und Futtermittel
(Case 11/70) [1970] ECR 1125
ECtHR Uzan v Germany (App no 35623/05) Judgment 2 September 2010
ECtHR Joint cases S. and Marper v UK (Applications nos. 30562/04 and 30566/04)
ECtHR Ben Faiza v France (Application no. 31446/12) Judgment 8 February 2018
ECJ Monika Esch-Leonhardt, Tillmann Frommhold and Emmanuel Larue v European Central Bank
Case No. T-320/02, ECJ McCullough v Cedefop T-496/13
ECJ Lindquist C -101/01
ECtHR M.M. v UK Application No. 24029/07

[94] GDPR: 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)' Source- https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679

ECtHR Roman Zakhrov v Russia (Application no. 47143/06) Judgment 4 Dec 2015
ECtHR Schalk and Kopf v Austria (Application no. 30141/04)
ECJ Joint cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR-I-11063
ECJ Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238 ('Digital Ireland')
ECJ Parliament v Council C-317 and C-318/04 (PNR)
ECJ Schrems v Data Protection Commissioner C-362/14 ("Schrems")
ECJ Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others ECLI:EU:C:2016:970 ('Watson').
ECJ Opinion 1/15 dated July 26, 2017 on EU-Canada Draft PNR Agreement
ECtHR Malone v. the UK **(**App no.8691/79) Judgment 2 Aug 1984
ECtHR Kruslin v. France (App No 11801/85)
ECtHR Amann v. Switzerland (App No 27798/95)
ECtHR Taylor-Sabori v United Kingdom (App No. 60696/00) Judgment 22 Oct 2002
ECtHR Khelili v. Switzerland (App No. 16188/07)
ECtHR , Mustafa Sezgin Tanrıkulu v. Turkey (App no. 27473/06)
ECtHR Szabo and Vissy v Hungry (App no. 37138/14)
ECtHR Joint Cases Big Brother Watch and Others v UK (App no 58170/13), Bureau of Investigative Journalism and ECtHR Alice Ross v UK (App no 62322/14) and Human Rights Organizations and Others v UK (App no 24960/15)
ECtHR Assocation confranternelle de la presse judiciaire v France (App no 49526/15)
ECtHR Rotaru v Romania (App no 28341/95)
ECtHR ECtHR MM v UK (App no 24029/07)
ECtHR Handyside v United Kingdom (Appl. No. 5493/72)
ECtHR Demir and Baykara v Turkey (App no. 34503/97)
ECtHR Centrum For Rattvisa v Sweden (App no. 35252/08
ECtHR Benedik v Slovenia (App no. 62357/14)

Convention/Charter/Legislations

ECHR 1950
CFREU 2009
Council of Europe Data Protection Convention 108, Strasbourg 1981
EU Directive 95/46/EC
EU Directive 2002/58
GDPR- EU Regulation 2016/679

Journals/Articles/Reports

European University Institute through HDL.NET® Information Services:
Source: http://hdl.handle.net/1814/28050 [Accessed on 1st May 2018]
A European Perspective on Data Protection and Access Rights – Authors-Antonella Galetta & Professor Paul de Hert, Tilburg University, Publication 2017 Source: https://pure.uvt.nl/portal/en/publications/a-european-perspective-on-data-protection-and-the-right-of-access(95eb239a-9c38-483c-b274-024496f7c96c).html
[Accessed on 22nd April 2018]

Summaries of EU Court Decisions Relating to Data Protection 2000-2015,Prepared by Laraine Laudati,28 Jan 2016.
Source: https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf
[Accessed on 5th June 2018]
Fact Sheet- Personal Data Protection ECtHR 2018 Source: https://www.echr.coe.int/Documents/FS_Data_ENG.pdf
[Accessed on 4th April 2018]

Other Sources

Drone Attacks using personal data: Source: https://reprieve.org.uk/press/2014_11_05_BT_OECD_intelligence_sharing_drones/
[Accessed on 21st May 2018]
Edward Snowden, The Guardian 2013 Article: Source: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [Accessed on 15 May 2018]
Wikileaks: Spy Files: Source https://www.wikileaks.org/spyfiles/russia/releases/
[Accessed on 3rd June 2018]
Boiling Frog: Source https://boilingfrog.com.au/new-data-retention-law-seriously-invades-privacy-time-took-action/ [Accessed on 3rd June 2018]
McKinsey Institute: https://www.mckinsey.com/featured-insights/digital-disruption/whats-now-and-next-in-analytics-ai-and-automation [Accessed on 14 May 2018]
Harvard Magazine : Source https://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal
[Accessed on 3rd June 2018]
Human Rights Watch: Source: https://www.hrw.org/world-report/2017/country-chapters/syria
[Accessed on 16th May 2018
Economist : Source https://www.eiuperspectives.economist.com/technology-innovation/digital-identity-%E2%80%93-precarious-balancing-act [Accessed on 3rd June 2018]
Documents of Council of Europe: Source- https://www.echr.coe.int/Documents
Documents of EU: and Source- http://www.europarl.europa.eu/charter/pdf/text_en.pdf and https://europa.eu

ISSN 1945-9098