Occasional Paper Series

Title: Between Security and Data Protection: Searching for a Model Big Data Surveillance Scheme within the European Union Data Protection Framework

Author: Dr Krzysztof Garstka*
Introduction

In order to counter the threat of terrorism and other forms of serious crime, State security and law enforcement agencies are increasingly turning to new technologies. One of the often-raised possibilities is that of collecting and analysing huge data sets through large-scale surveillance, in order to identify potential perpetrators and patterns which would otherwise remain hidden. The appeal of this approach is well underscored by Hijmans and Kranenborg, who noted that data is everywhere, and there is a high and growing incentive to use it for public and national security purposes.

On the other hand, data collected for public and/or national security purposes can often constitute personal data. In such a situation, a conflict arises between two key interests: security and data protection. Collecting, accessing, storing and analysing the personal data of EU citizens, for security-related purposes, is likely to trigger a variety of data protection concerns, and the Court of Justice of the European Union (CJEU) has handed down judgments regarding surveillance-related activity in cases such as Digital Rights Ireland, Schrems, Tele2/Watson and Ministerio Fiscal.

However, the CJEU decisions have not provided regulators and/or law enforcement agencies with specific, precise guidance on the overall shape of an EU law-compatible Big Data Surveillance scheme. A comprehensive analysis aimed at indicating the key elements of such a scheme is currently missing from the CJEU acquis. This mapping paper begins to fill this gap by extracting the relevant aspects of EU data protection law and considering how these might be applied to activities likely to appear in any Big Data Surveillance scheme.

It is difficult to deny the need for such an analysis, given that on the 30 of January 2018, the UK Court of Appeal applied the CJEU ruling in Watson to the data retention provisions of the Investigatory Powers Act 2016, and found them unlawful. In the aftermath of this decision, it is crucial to investigate what kinds of surveillance mechanisms would be lawful. Such a theoretical exercise can deliver practical value for regulators, law enforcement bodies, developers of technology and citizens, by showing where the lines between security and data protection are currently drawn. Clarity within this field is essential, in order to prevent unwarranted interferences with the right to data protection, but also to avoid the spending of time and resources on surveillance schemes which ultimately cannot be used if data is obtained in contravention of data protection laws (for example, on the basis of the “fruit of

---

* The author would like to thank Dr. Daragh Murray, Prof. Pete Fussey, Prof. Maurice Sunkin, Dr David Erdos and Miss Vivian Ng for their feedback and support in the creation of this report. The paper was developed within the Human Rights, Big Data and Technology project, supported by the Economic and Social Research Council [grant number ES/M010236/1].
1 Term defined in section 1 below.
3 Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources [2014].
4 Case C-362/14 Maximilian Schrems v Data Protection Commissioner [2014].
5 Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v Watson.
6 Case C-207/16 Ministerio Fiscal [2018].
7 Secretary of State for the Home Department v Watson [2018] EWCA Civ 70, at para. [27].
the poisonous tree” doctrine). The issues addressed in this paper are also important because of the key role of EU law in this field and because combatting terrorism and serious crime is undoubtedly an EU-wide concern.

Before proceeding further, it should be noted that this paper is purely focused on EU legislation and the binding interpretations of the CJEU; it does not cover the European Convention of Human Rights (ECHR) and the case law of the European Court of Human Rights (ECtHR), apart from occasional references. It is true that the EU and ECHR legal frameworks are closely related, as demonstrated by art. 52(3) of the CFREU, which provides that “(i)n so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention” – although it is noted that “(t)his provision shall not prevent Union law providing more extensive protection.” According to the Article 29 Working Party (A29 WP), a key advisory body in the field of EU data protection law, the cited article means that “the fundamental principles developed under both texts are therefore fully consistent,” and moreover, “since all EU Member States are also Parties to the ECHR [European Court of Human Rights] and the Convention, they have a positive obligation, also developed in case-law of the European courts, to secure effective protection of fundamental rights of all individuals within their jurisdiction.”

Without underlining this profound connection, the paper seeks to focus purely on EU law, seen as a cohesive set of rules and principles permeating an independent, sophisticated and expanding data protection regime, recently expanded by the entry into force of the General Data Protection Regulation, as well as of the Law Enforcement and Data Protection Directive.

This paper adopts the following structure. Following the overview of findings, section 1 outlines the concepts and technology behind Big Data Surveillance, as well as introduces the right to data protection – both conceptually and within the EU law framework. Section 2 commences the comprehensive analysis of the EU data protection law, by looking at the exclusions and limitations to its application in the Big Data Surveillance context. Section 3 explores the regulatory effect of the Law Enforcement and Data Protection Directive, while section 4 does the same with the CJEU’s case law interpreting art. 52 of the Charter of Fundamental Rights of the EU.

---


10 Working document 14/228, supra fn., at p. 21.


12 Directive 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

13 Art. 52 provides the conditions for balancing the fundamental rights and freedoms of the Charter.
Overview of findings

First of all, this paper concludes that no relevant EU data protection laws regulate bulk surveillance practices conducted for national security purposes. Such practices are therefore regulated by the European Convention on Human Rights and relevant national laws. In relation to non-national security purposes, such as the protection of public order or the prevention of serious crime, the Law Enforcement and Data Protection Directive is the key instrument applicable. Based on this Directive and relevant CJEU decisions, a preliminary model of a Big Data Surveillance scheme compatible with EU data protection law would be likely to embrace the following elements:

**The law establishing a Big Data Surveillance scheme**

The scheme should be established through national legislation (the “implementing law”), regulating both the scheme as a whole, and each of its four key data processing operations: collection; access; analysis; and retention.

**Objective(s) of the scheme**

A Big Data Surveillance scheme should follow a two-tier approach to its objectives. The primary, broader objective, enshrined in the implementing law, should be to combat ‘serious crime’ (as defined in national law) — specifying the nature of the covered offences in said law could be helpful. The second, narrower objective should be tied to a more specific threat lying within the first objective’s remit. For example, this could be securing a specific public event, which is in a credible risk of being affected by serious crime. A Big Data Surveillance operator should rely on and comply with the secondary objective when seeking collection, access, storage and/or use of data covered by the scheme. Such reliance should be supported by presentation of convincing evidence, showing that data is likely to help in achieving the secondary objective.

**The data which can be used**

First, the implementing law should specify (as narrowly as possible) the categories of personal data which could be used within the scheme, through one or more classifications. Then, when a relevant secondary objective appears, the scheme’s operators should approach the identified oversight body or judicial authority, seeking permission to perform each of the four processing activities on specified categories of data — i.e. only those which are supported by evidence showing their likelihood of being of actual use in fulfilling the identified secondary objective. That being said, there may be a provision in the national law bypassing this procedure, allowing for the use of other categories

---

14 See section 2.1.
15 See sections 3.1 and 4.1.
16 See sections 3.1, 4.3 and 4.4.
17 And in line with the key ECtHR decision in *Big Brother Watch v UK* (Applications nos. 58170/13, 62322/14 and 24960/15) (Sep. 13, 2018), at para [307]. For a succinct overview of this decision, see Murray and Ng’s article available at https://hrcessex.wordpress.com/2018/09/14/big-brother-watch-and-others-v-the-united-kingdom-some-initial-thoughts/
18 See section 4.3.
19 (Before the consideration of other requirements.)
20 See sections 3.4 and 4.3
21 See sections 3.1, 3.2, 4.1 and 4.3.
22 See sections 3.9 and 4.3
of data in cases of “validly established urgency” – this should, however, be extremely limited and operators are required to present clear and robust evidence for why the principal procedure was not followed.\textsuperscript{25}

The scheme’s operators should be very careful in choosing the categories of data they ask for, as they have to be necessary and proportionate in light of the identified secondary objective. EU law does not allow for a system which collects data indiscriminately,\textsuperscript{24} and symbolic/meaningless distinctions (for example, those whose only actual role is to legally justify wider collection of data than it would otherwise be allowed) should be refrained from, as they would not survive an art. 52 of the CFREU-based assessment.\textsuperscript{29}

The first set of distinctions which ought to be made should be one based on categories of data subjects\textsuperscript{36} – they should be demonstrably related to the serious crime(s) covered by the secondary objective. A very limited, emergency exception may be present here, allowing for temporary access to data of unrelated data subjects; however, the evidence threshold warranting this should be very high.\textsuperscript{27}

The second set of distinctions ought to be one based on time limits – if there’s no appropriate evidence suggesting that data created/collected during a certain time period would be likely to be of use, then it should be kept out of the scheme.\textsuperscript{28}

The third set should be based on geographical distinctions\textsuperscript{39} – if there is a choice of this kind, the same connection (as with previous sets) should be proven in the request. The final set of distinctions in this non-conclusive list is based on the data’s sensitivity – particularly strong evidence has to be presented when wishing to rely on one or more categories of sensitive data (as it is defined in EU law), and particular safeguards have to be in place for this to be legal.\textsuperscript{30}

\textit{Duration}

When the secondary objective-based connection between the successfully requested data and one or more of the scheme’s processing activities ceases, then this data should not be processed further in every processing activity where this is the case.\textsuperscript{31} When the secondary objective is achieved (e.g. the targeted terrorist/crime group has been successfully dismantled), all processing of requested data should stop.\textsuperscript{32}

\textit{Ensuring accuracy}

There should be specific steps taken to ensure that within the scheme’s activities, facts are distinguished from assumptions, as much as possible.\textsuperscript{33} For example, if members of a certain social media group are to be targeted, this

\textsuperscript{25} See section 4.3.
\textsuperscript{24} See section 4.2.
\textsuperscript{26} See section 4.
\textsuperscript{28} See sections 3.2, 3.4 and 4.3.
\textsuperscript{27} See section 4.3.
\textsuperscript{29} See section 4.3.
\textsuperscript{30} See section 3.4.
\textsuperscript{31} See sections 3.1 and 4.3.
\textsuperscript{32} See sections 3.1 and 4.3.
\textsuperscript{33} See section 3.3.
should be justified by objective, factual evidence, instead of broad assumptions based on, for example, their ethnicity. In taking such decisions, special care should be taken to limit the use of automated decision-making.34

**Exercise of data subject rights**

Should the scheme’s operators wish to limit the exercise of data subjects’ rights granted to the latter by the Law Enforcement and Data Protection Directive (LEDPD), they should be able to present convincing evidence showing that such limitations fall within the defined circumstances identified by the Directive.35 Particular care should be given in proving necessity and proportionality in limiting data subject rights where the secondary objective was achieved or the data in question is no longer likely to contribute to the objective’s fulfilment.36

**Usage of data and resulting information for further purposes**

Both personal data obtained for the Big Data Surveillance scheme, as well as information derived from the analysis of such data, should not be used for any other purpose beyond the approved secondary objective.37

**Data protection by design**

Aspects of the scheme which are currently lacking direct guidance from EU law should nonetheless be designed with the right to data protection in mind,38 and a suitable range of impact assessment activities should take place before the implementing law is enacted.39

**Security**

The security requirements set out by the LEDPD ought to be followed in the design, implementation and operation stages of a Big Data Surveillance scheme – and any security breaches should be notified in the indicated circumstances.40

**Oversight**

It is crucial for the implementing law to subject the scheme to effective, meaningful and independent oversight, by either a data protection authority or by a specialist, dedicated body.41 Such a body should have an extremely profound insight into all of the scheme’s operations, the power and expertise to influence or suspend those operations, as well as the guaranteed funding to exercise the above.42

---

34 See section 3.5.
35 See section 3.6.
36 See sections 3.6 and 4.3.
37 See sections 3.1, 4.3., and 4.4.
38 See section 3.7
39 See section 3.7.
40 See section 3.8.
41 See section 3.9.
42 See section 3.9.
1. Introduction to Big Data Surveillance and Data Protection as an Interest Protected within EU law

Big Data Surveillance can be defined as a drive to direct Big Data analytics to massive data sets obtained through various forms of mass surveillance. There are four key steps which can be distinguished within this concept, each of them posing different challenges for the purposes of this paper’s data protection-oriented analysis. The first is gathering of data, whether by the Big Data Surveillance operators themselves or by any other (public or private) third party. The second is accessing data from the third parties who gathered it in the first place. If the Big Data Surveillance operators gathered the data themselves, this second step does not occur. The third step is retention of data – this concerns retention by the Big Data Surveillance operators, not by the third parties such as providers of online services. Finally, the fourth step is analysis of the data, e.g. to reveal relevant patterns and factual connections.

Big Data Surveillance schemes are likely to operate against the backdrop of a complex set of relationships between multiple, potentially competing, legitimate interests – data protection being one of the more relevant ones. This section of the paper aims to explore the nature of the interest in data protection, in order to distinguish it from the right to privacy, and show how entrenched the former is within the framework of the EU law.

Protection of personal data is enshrined in art. 8 of the Charter of Fundamental Rights of the EU. By virtue of this provision, “everyone has the right to protection of personal data concerning him or her”. This is complemented by a short set of supplementary (binding) guidelines, which provide that:

“such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law”,

and that:

“(e)everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.”

Finally, article 8 also provides that “compliance with these rules shall be subject to control by an independent authority”.

The right to privacy is set out in art. 7 of the Charter of Fundamental Rights of the EU (CFREU) and provides that “everyone has the right to respect for his or her private and family life, home and communications”. This provision encapsulates the right to privacy and is modelled on Article 8 of the European Convention on Human Rights (ECHR).

Before moving forward, it is worth discussing the relationship between the two rights and explaining why there may be value in seeing and evaluating the right to data protection as a fundamental right independent of the right to privacy.

---

43 Charter of Fundamental Rights of the European Union, art. 8(1).
44 CFREU, supra fn. 43, art. 8(2).
45 CFREU, supra fn. 43, art. 8(2).
46 CFREU, supra fn. 43, art. 8(3).
First, both rights have significant overlap. For example, as Lysnkey noted, the CJEU’s judgment in *Digital Rights Ireland* (a case covered extensively in section 4 of this paper) would most likely be decided in the same manner if the key right involved was not the right to data protection, but the right to privacy. At its conceptual core, the right to privacy is aimed at preventing or rectifying harm resulting from information escaping the “privacy circles” people maintain around themselves. Such a circle might be drawn around an individual; an individual and their partner; an individual and their friends, and so forth, until the circle is so wide as to encompass the general public. Data protection is different, in that it seeks to prevent or rectify the harm resulting from other people’s use of one’s personal data, that is information relating to/identifying specific individuals. Data protection is not initially concerned with whether this information was in one of the individual’s circles of privacy—though it is often true that information which was private can be much more harmful than that which was public; and as a result, it often falls within the definition of “sensitive” data. This understanding of the privacy/data protection relationship was discussed by Attorney General Cruz-Villalón in *Digital Rights Ireland*, who wrote that data protection law is about protecting the personal sphere, which holds in its core the private sphere, protected by the right to privacy.

As Tzanou succinctly shows on the basis of CJEU case law, since 2003, the Court (and with it, EU law) has grown to accept the right to data protection as an independent right, and is now in the “mature” stage of embracing this stance with confidence. Furthermore, as the CJEU stated in the *Bavarian Lager* case - and as highlighted by Kokott and Sobotta - in comparison with the right to privacy, the right to data protection has a specific and reinforced system of protection within EU law; this statement is perhaps even more true today with the entry into force of the General Data Protection Regulation. This mapping paper relies on this understanding in order to assess the system of protection based exclusively on data protection; without undermining the profound value of the right to privacy in the discussed context.

---

48 A term to be understood broadly — in this context, it encompasses both direct harm to e.g. one’s reputation or mental state, as well as indirect harm, such as preventing the realisation of personal development and other rights and freedoms.
49 GDPR, supra fn.11, art. 4(1).
50 Or whether it is fake – see Garstka K, ‘From Cyberpunk to Regulation — Digitised Memories as Personal and Sensitive Data within the EU Data Protection Law’ (2017) JIPITEC 8(1)/293, at para. [33].
51 On which see more in section 2.2.3.
52 Opinion of the Advocate General in Joined Cases C-293/12 and C-594/12, at para [61].
54 Case C-28/08 Commission v Bavarian Lager [2010], at para [60].
2. Scope of Exclusions and Limitations of EU Data Protection legislation

Multiple EU legislative instruments aimed at protecting personal data contain exclusions tied to the notion of societal security interests. Such exclusions nullify or limit the application of data protection instruments to data processing activities which would normally fall under the given instrument’s scope. Consequently, before considering the guidance on Big Data Surveillance based on the more substantive provisions of those instruments, it is worth considering whether they would be likely to be applicable in the first place. The argument furthered in this section is that the Charter of Fundamental Rights of the EU (CFREU) and the Law Enforcement and Data Protection Directive (LEDPD) are the instruments fitting this criterion the most.

2.1. Absolute exclusions

The first category of exclusions are “absolute exclusions” which prevent data protection legislation from applying in the first place. Another term for these, proposed by Docksey, is exceptions; and these may be contrasted with the derogations,\(^{56}\) or “limitations” which reduce the degree to which an instrument applies *a posteriori* (these are covered in section 2.2).

2.1.1. Charter of Fundamental Rights of the EU

Article 8 of the Charter of Fundamental Rights of the European Union sets out the foundation of data protection laws in the EU and establishes several key requirements concerning data processing activities. As such, it should be considered as a data protection instrument.

Therefore, the first question to be asked is: does the CFREU contain any provisions which could fully exclude its application to Big Data Surveillance? As far as the analysed processing lies within the scope of EU law, the answer is “no”. Article 8 of the CFREU’s will remain applicable and will have to be balanced against other legitimate interests through art. 52 of the Charter.\(^{57}\) However, the situation changes if contested processing is seen as lying outside of the scope of EU law. Art. 51(1) of the Charter states that its provisions “are addressed to the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States *only when they are implementing Union law*.\(^{58}\) Art. 4(2) of the Treaty on European Union states that the Union “shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. *In particular, national security remains the sole responsibility of each Member State.*\(^{59}\) Hence, should the processing of personal data within a Big Data Surveillance scheme be seen as concerning national security, the Charter does not apply at all – in contrast to the European Convention on Human Rights.

---


\(^{57}\) With the balancing exercise including the more specific subarticles 8(2) and 8(3), see Tzanou, supra fn. 53, at p. 253.

\(^{58}\) (Emphasis added.)

\(^{59}\) Treaty on European Union, art. 4(2) (emphasis added).
2.1.2. General Data Protection Regulation 2016/679

The GDPR is the main data protection instrument in the EU, setting out a plethora of rights and obligations aimed at giving real substance to the right protected in art. 8 of the CFREU. However, the application of the Regulation’s rights and obligations can be nullified on the basis of art. 2(2). By virtue of this provision, the Regulation “does not apply to the processing of personal data […] by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU” or to processing “by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.” There are several aspects worth underlining here. First, the cited provision introduces the requirement of the “competent authority” carrying out the contested activity. This may prevent, for example, the exclusion of qualifying activities performed by private, “non-competent” bodies, which could be involved in the activities based on the excluded processing. Such a scenario is worth considering, given the strong presence of Big Data Surveillance technology-related companies such as Palantir or Cambridge Analytica. Second, GDPR is quite precise in indicating the specific activities related to criminal law or security (prevention, investigation, etc.). This may potentially result in a fairly high hurdle for the Member State law enforcement agencies, who may have to prove that a data processing activity contested under art. 2(2) of the Regulation falls under one of the specific purposes, as opposed to just being seen as, for example, concerning public security.

Nevertheless, it seems that the discussed use of Big Data Surveillance would be likely to be excluded from the scope of the GDPR. Prevention of terrorist attacks and/or tackling serious and organised crime is very likely to serve as an adequate purpose/activity in this regard. However, special care would have to be paid to have all modes of data processing forming part of the claimed activity conducted by the competent authority. Unfortunately, there is little guidance in the GDPR on which bodies would qualify for this category. Overall, in the context of Big Data Surveillance, the protections established in the GDPR are unlikely to apply.

2.1.3. Law Enforcement and Data Protection Directive 2016/680

The focus of the Law Enforcement and Data Protection Directive 2016/680 (LEDPD), as stated in art. 1(1), is the “protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.” Recital 19 of the GDPR states that “personal data processed by public authorities under this Regulation should, when used for [the earlier cited] purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680”. It is clear that the law enforcement activities excluded from the GDPR are presumptively regulated by the LEDPD.

This leads to a similar question – are there any relevant absolute exclusions in the text of the LEDPD which would remove the Big Data Surveillance-related processing from its scope? Yes, there are. Article 2(3) of the LEDPD excludes from its scope the processing of personal data which either takes place “in the course of an activity which falls outside the scope of Union law” or is conducted by “by the Union institutions, bodies, offices and agencies”.

---

60 GDPR, supra fn. 51.
61 (Emphasis added).
62 For the discussion of the role of “competent authority” in the context of the LEDPD, see section 2.1.3 below.
Indicative of art. 4(2) of TEU, rec. 11 of the LEDPD specifies that activities falling outside of the Union law are, among others, those “concerning national security, activities of agencies or units dealing with national security issues”. As a result, one of the key questions surrounding the applicability of LEDPD to the discussed use of Big Data Surveillance is whether the latter is applied to matters of national security (in which case the Directive does not apply) or public security (in which case the Directive applies). A clear, guiding answer to this dilemma is sorely lacking from the EU law. As for the second condition, the assumption is that this paper's inquiry is related to a Big Data Surveillance system operated by one or more of Member States' national agencies; hence, the second ground for exemption would be unlikely to apply.

Assuming that the scheme is not found to concern national security, the discussed processing activities would be most likely to fall under the scope of the LEDPD — provided the processing remains focused on the purpose(s) outlined in art.1(1). Should the processing divert from this purpose, art. 9(1) provides the arguably more restrictive GDPR would be applicable again. However, it should be added that this “downgrade” to the Regulation could also take place if any data processing activities occurring in the course of the Big Data Surveillance scheme are conducted by a non-“competent authority”. In contrast to the GDPR, the LEDPD does provide a definition of this term, identifying two possible categories of entities. The first one is “any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”. The second is “any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”.

Among the potential entities involved in the discussed use of Big Data Surveillance, which ones would fit this definition and keep the scheme within the distinct regime of the LEDPD? Bodies such as the police forces fit clearly within the first category. The situation is more complex when it comes to private entities and companies which could be cooperating with or be designated by the law enforcement authorities to be involved with a Big Data Surveillance scheme. The second criterion states that in order to qualify, the “body or entity” would have to be entrusted with authority “by Member State law”. Whether this would require a separate legislative instrument remains open to interpretation.

2.1.4. Privacy and Electronic Communications Directive 2002/58

It is well-established in EU law that surveillance measures involving the interception of communications raise issues which could fall within the remit of the Privacy and Electronic Communications Directive (E-Privacy Directive or EPD). Should such intercepted data be fed into the discussed Big Data Surveillance scheme, the rights and obligations set out in EPD could potentially become applicable. However, as with previously covered instruments, it is essential to begin by looking for absolute exclusion provisions in the text of the Directive.

---

63 LEDPD, supra fn. 14, rec. 11.
64 LEDPD, supra fn. 14, art. 3(7)(a).
65 LEDPD, supra fn. 14, art. 3(7)(b).
66 LEDPD, supra fn. 14, art. 3(7)(b).
In this regard, art. 1(3) of the EPD states that “(t)his Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law”. Based on this wording, it would seem unlikely that the EPD would regulate the discussed Big Data Surveillance scheme, a stance reinforced in recital 11 of the Directive.88

This interpretation, however, could be seen as challenged by the CJEU judgment in Watson, concerning the legality of mass data retention schemes.89 The Court found such schemes to be covered by art. 15(1) of the EPD, which allows national legislation for limitations to the Directive’s set of rights and obligations where they “constitute (...) a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system (...).”90 The evident overlap of this provision with art. 1(3) EPD was solved by the Court with the logic that if the latter provision was interpreted broadly, and the contested data retention schemes were to be excluded from the scope of the Directive, art. 15(1) EPD would be a blank provision, “deprived of any purpose”.71

CJEU reaffirmed this view of the relationship between arts. 1(3) and 15(1) of the EPD in a 2018 case of Ministerio Fiscal, adding that “the protection of the confidentiality of electronic communications and related traffic data, guaranteed by Article 5(1) of Directive 2002/58, applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies”.92 Additionally, the Court stated that EPD’s inapplicability to “the activities of the State in areas of criminal law” does not extend to the activities of providers of electronic communications services;93 and such activities were found to be involved in that case, centred around seeking access to SIM card ownership data.94

While the approach embraced in Tele2/Watson and Ministerio Fiscal opened the doors for much needed decisions and guidance, the question remains whether the Court crossed the borders drawn by art. 3(2) of the EPD.

2.1.5. E-Privacy Regulation

Just as the GDPR superseded the Data Protection Directive on the 25th of May 2018, it is likely that the draft E-Privacy Regulation95 will replace the EPD. The draft of this regulation passed the European Parliament (EP)'s Committee on Civil Liberties, Justice and Home Affairs on October 17, 2017 and at the time of writing, it still

---

88 Which states that “(…) this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes (…)”.
89 See supra fn. 5.
90 See supra fn. 67, art. 15(1).
91 Watson (CJEU), supra fn. 5, at para. [78].
92 Ministerio Fiscal, supra fn. 6, at para [36].
93 Ministerio Fiscal, supra fn. 6, at para [37].
94 Ministerio Fiscal, supra fn. 6, at para [38].
continues its journey through the EU legislative process. Consequently, it is not feasible to discuss the drafts of the Regulation in this section – however, this piece of legislation should definitely stay on the radar of regulators considering reliance on Big Data Surveillance systems.

2.1.6. Conclusions

Having sieved through the major EU data protection instruments, it’s fairly clear that, in principle, two of them would be most likely to apply to the discussed Big Data Surveillance scheme – the CFREU and the LEDPD (tailor-made for the discussed context); unless such a scheme is seen as related to matters of national security, in which case none of the discussed instruments applies. The GDPR could become applicable if the entities involved in the processing fall outside of the definition of a competent authority, provided in art. 3(7) of the LEDPD. There is a chance that the EPD may be applicable as well, especially if the Big Data Surveillance scheme is based on mass data retention solutions invalidated in Watson, and the CJEU’s pragmatic approach to the relationship between art. 3(2) and art. 15(1) EPD is maintained.

2.2. Limited Exclusions

If a data protection instrument is not fully prevented from applying to a form of data processing – for example, on grounds of national, as opposed to public security - its scope and mode of application can still be restricted by means of a limitation (or, using Docksey’s terminology, a derogation\(^78\)). This section considers whether this would be the case with a Big Data Surveillance scheme and the two data protection instruments which are most likely to remain applicable (CFREU and LEDPD), as well as the GDPR, which could, in the identified narrow conditions, remain applicable. Due to time and space concerns warranting the focus on only the directly and broadly applicable instruments, this paper’s analysis of the EPD is limited to section 2.1.4.

2.2.1. Charter of Fundamental Rights of the EU

The primary way in which the application of art. 8 CFREU (setting out the right to data protection) can be restricted is via art. 52(1) of the Charter, which provides that “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\(^77\).” Additionally, “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”. Applying this last criterion to the Big Data Surveillance context, the right to data protection can be limited by rights and freedoms of others tied to notions such as public security. However, it is necessary to look at Big Data Surveillance schemes through the whole lens of art. 52(1) and this will be covered separately in section 4. Art. 52(1) is not only a “limitation” provision, it underpins the interplay between data protection and security and has an ongoing influence on other related legislative measures.

---

\(^77\) Docksey, supra fn. 56, at p. 98.
\(^78\) (Emphasis added).
2.2.2. Law Enforcement and Data Protection Directive

The LEDPD contains provisions limiting the scope of data subject’s right to information, right of access, as well as rights to rectification or erasure of personal data or to restriction of its processing. The substance of those rights and their application to the legality of Big Data Surveillance schemes are explored in more depth later, in section 3.6. In the current section, focused on limitations, attention can be given to articles 13, 15 and 16 of the LEDPD.

Article 13 states that:

“Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned (...).”

Such restrictions can take place on one of five grounds. First, to “avoid obstructing official or legal inquiries, investigations or procedures”. Second, to “avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties”. The remaining three grounds are broader in nature, based respectively on protection of public security, national security and the rights and freedoms of others. The same five grounds can be relied on in the context of art. 15, to limit the right of access, and art. 16, to limit the right to rectification or erasure of personal data, or restriction of its processing.

At first sight, looking at the wide scope of the five grounds for limitation, it seems very likely that the operators of a Big Data Surveillance scheme would be exempt from enabling the data subject’s right to information, right of access and right to rectification or erasure of personal data and restriction of processing. However, it has to be remembered that – apart from the need to be set by a legislative instrument - such limitations can only be implemented “to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned”. The scope and applicable period of limitations are, in essence, subject to a balancing exercise which points towards art. 52(1) of the CFREU. Following the logic outlined in the previous section, the analysis based on this provision of the Charter is in section 4.

2.2.3. General Data Protection Regulation

As mentioned earlier, there may be occasions where a Big Data Surveillance scheme remains within the framework of the GDPR, due to the processing activities being conducted by a non-“competent authority”. In this case, it is worth considering whether the Regulation’s scope of application could nonetheless be partially restricted through a further, specific provision.

---

78 LEDPD, supra fn.14 art. 13(3).
79 LEDPD, supra fn.14, art. 13(3)(a).
80 LEDPD, supra fn. 14, art. 13(3)(b).
81 LEDPD, supra fn. 14, art. 13(3)(c).
82 LEDPD, supra fn. 14, art. 13(3)(d).
83 LEDPD, supra fn. 14, art. 13(3)(e).
84 LEDPD, supra fn. 14, art. 13(3) (emphasis added).
85 LEDPD, supra fn. 14, art. 9(2).
The short answer is a definite yes. In contrast to the LEDPD, where limitations are divided on specific rights, the GDPR has a single article which deals with a wide set of rights and obligations collectively. Art. 23(1) provides that Member States “may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as art 5 (...)”. A restriction of this kind needs to respect “the essence of the fundamental rights and freedoms” and be “a necessary and proportionate measure in a democratic society to safeguard (...)” at least one purpose from an indicated set. Those which arguably best match the discussed use of Big Data Surveillance are: national and public security,86 defence,87 the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security,88 as well as “a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority” in situations falling within the scope of the other cited purposes.89

The discussed use of Big Data Surveillance would be very likely to fit at least one of those purposes, and hence, it is very probable that the indicated rights and obligations would not apply in the discussed context.

Additionally, there is a layer of GDPR which could lead to the limited exclusion of special categories of data covered by arts. 9 and 10 of the Regulation. The first of those provisions prohibits the processing of personal data revealing information such as racial or ethnic origin, political opinions or data concerning health, unless one of the enabling conditions listed in art. 9(2) is present. Of the enabling conditions, the one in art. 9(2)(g) is particularly important in the discussed context – it allows for processing of sensitive data where it “is necessary for reasons of substantial public interest, on the basis of Union or Member State law”90 (provided adequate safeguards are in place). It is very possible that safeguarding public security could be relied on in this regard.

Art. 10 is at least as deserving of a note in this section, for it states that personal data “relating to criminal convictions and offences or related security measures” can be lawfully processed “only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects”. Hence, the GDPR’s prohibition on the processing of such data within the BDS scheme would be lifted, provided the indicated conditions of art. 10 are met.

---

86 GDPR, supra fn. 51, art. 23(1)(a) and (c).
87 GDPR, supra fn. 51, art. 23(1)(b).
88 GDPR, supra fn. 51, art. 23(1)(d).
89 GDPR, supra fn. 51, art. 23(1)(h).
90 GDPR, supra fn. 51, art. 9(2)(g).
3. The Boundaries Set to Big Data Surveillance by the LEDPD

Having considered which data protection instruments could be fully or partially precluded from applying to the discussed use of Big Data Surveillance, the next, crucial step is to consider the relevant provisions of instruments which have been found most likely to apply. Among those, it is sensible to start with the LEDPD, due to its specified, dedicated focus, fitting the use of Big Data Surveillance.

3.1. Data protection principles

The first, core element of the LEDPD which could influence the contested use of Big Data Surveillance is found in art. 4 of the Directive, which sets out the key data protection principles, tenets to which the relevant data processing activities should adhere to. Art. 4 states that “Member States shall provide for personal data to be:

a) processed lawfully and fairly;

b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

c) adequate, relevant and not excessive in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

The first data protection principle of the LEDPD is that data should be “processed fairly and lawfully”. It differs from its counterpart in the GDPR (art. 5(1)(a)), which complements the requirements of fairness and lawfulness with the notion of data being processed in a manner transparent to the data subject. It seems that elevating transparency to the principle level is not fitting for the subject area covered by the LEDPD.

Reference to fairness in the first data protection principle of the LEDPD, arguably, does not offer any direct guidance on the legality of Big Data Surveillance. The case is potentially different with the second aspect of the principle, in that the processing has to be lawful. This term is further elaborated on in art. 8 of the Directive, which provides that this condition is met “only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or
Member State law”. Furthermore, the said law has to “specify at least the objectives of processing, the personal data to be processed and the purposes of the processing”.

What this means for Big Data Surveillance is that there first has to be a specific objective, set out in Union or Member State law, and carried out by a competent authority for at least one of the purposes set out in art. 1(1) (“prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”). This objective could be identified, for example, as prevention of terrorist attacks in the public space of the Member State, with the competent authority being a police force or an intelligence agency (as discussed in section 2.1.3), and the fitting purpose being “prevention of criminal offences and threats to public security”.

Secondly, all contested processing activities – such as collecting, accessing, retaining and analysing – have to be necessary for the performance of the task. This indicates that the operator of the Big Data Surveillance scheme would have to prove that each of those is necessary, and the scheme does not include processing which is not. However, a certain question arises – if, for example, more data is retained than necessary, does this mean that the whole processing activity loses its “necessary” status and makes the Big Data Surveillance scheme illegal, or is it only the exceeding part which becomes illegal, with the overall retaining activity and the scheme remaining lawful?

Continuing to the last aspect of the principle of lawfulness, the EU or Member State law warranting the legality of those processing activities has to specify, at least, the objectives of processing, the types of personal data which can be processed and the purposes of processing. While the distinction between an objective and purpose could be explored linguistically, it is possible that both of those could be justified with the earlier used combination of preventing terrorist attacks in public spaces of the Member State (objective) and prevention of criminal offences and threats to security (purpose). An arguably more challenging issue would be how specific the law in question has to be in setting out the types of personal data which would be processed within the various stages of the Big Data Surveillance scheme. Would it be enough to identify this merely as e.g. “non-sensitive”? Would a technical indication of e.g. metadata, social network data and/or air travel records be sufficient? Or would the law have to, for example, pinpoint all of the sources of such data or set out the age groups/ethnicities/religious groups concerned? Unfortunately, there is little clarity on what would be acceptable in this context.

The second data processing principle of the LEDPD is that personal data has to be “collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes”. In applying this to Big Data Surveillance, it seems that justifications proposed in respect of the first principle largely overlap with the needs of the second. The purpose of preventing criminal offences and threats to security could be raised in order to comply with the first element of the “purpose limitation” principle – though it remains unclear how it should be formed in order to be seen as specified, and explicit. Refraining from processing activities which are not necessary for the performance of the task mentioned in art. 8 can be equivalent to refraining from processing which is incompatible with the indicated purpose(s). Consequently, this means that both the findings and the interpretative challenges of the first principle carry over to the second one.

---

91 LEDPD, supra fn. 14, art. 8(2).
92 LEDPD, supra fn. 14, art. 4(1)(b).
93 If anything, the former is more demanding than the latter.
At this point, it is worth mentioning art. 4(2) LEDPD. By virtue of this provision, data which were collected for a purpose different to one fitting art. 1(1) can still be processed for that latter purpose, under two conditions. First, the data controller has to be “authorised to process such personal data for such a purpose” through EU or Member State law. In the Big Data Surveillance context, the chosen competent authority could be authorised to use such data through e.g. the relevant piece of legislation. Second, processing of such data has to be “necessary and proportionate” to the art. 1(1) purpose in question. The notions of necessity and proportionality involve consideration of the impact on other legitimate interests and objectives – given the lack of further clarifications in the LEDPD, the consideration of what could be seen as necessary and proportionate in the Big Data Surveillance context points towards the analysis of art. 52 of the CFREU and is covered later, in section 4.3. For now, it can be said that operators of the Big Data Surveillance scheme would be able to use the data which was collected for purposes other than those underlying the operation of the scheme; provided the enabling piece of law allows it, and such use is necessary and proportionate to that purpose.

The third principle to be covered in this section is that personal data should be “adequate, relevant and not excessive in relation to the purposes for which they are processed”.94 The overall idea of “not going beyond what is necessary”, as it was extracted in relation to the first and second principles, fully covers the discussion of the third principle as well. As such, there is not much to add in this regard.

The fourth principle is that personal data ought to be “accurate and, where necessary, kept up to date;” and that “every reasonable step must be taken to ensure that personal data that are inadequate, having regard to the purposes for which they are processed, are erased or rectified without delay”.95 This principle is less focused on preventing the overextension of personal data being processed, and more directly focused on preventing the harm which may result from one’s very specific personal data being processed – in this case, where such data would be inaccurate. Inaccuracy can be a significant trigger for harm, as one’s legitimate interests may be harmed by others without the latter intending or even being conscious of that harm (algorithmic processing/decision-making being a prime example for the second circumstance, as they can lead to e.g. over-extensive policing activity96).

How should the designer of a Big Data Surveillance scheme act to ensure compliance with the principle of accuracy? It seems that procedures should be implemented to ensure (or maximize the chances) that personal data which is processed at all four stages of the process is accurate and up-to-date. Data which is inaccurate should be erased or rectified – and most likely, the same should happen whenever considerable doubts exist regarding the accuracy of data processed. Of course, the question remains how often and with what degree of scrutiny should this accuracy verification take place, and how different would the answers be for different types of personal data.

Moving towards the fifth principle, it states that personal data should be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed”.97 This requirements also stems from the notion of necessity, but narrows it towards anonymization; it essentially requires it to be performed as soon as the presence of the individually identifying factor(s) is no longer required for the stated purpose. In the Big Data Surveillance context, it could mean, for example, that if the scheme was at certain

---

94 LEDPD, supra fn. 14, art. 4(1)(c).
95 LEDPD, supra fn. 14, art. 4(1)(d).
97 LEDPD, supra fn. 14, art. 4(1)(e).
point used to prevent the acts of terrorism conducted by a specific group, but members of the group have been arrested, anonymizing steps should be undertaken with regards to data of other individuals caught up in the information. This could be translated to the removal of personally identifying characteristics of personal data sets which were used in the procedure to achieve this goal, and which are of no further use in prevention of other threats the Big Data Surveillance scheme is supposed to tackle (by virtue of its underlying law).

The sixth and final principle is focused on security of personal data and preventing harm which could result from shortcomings in this area. Art. 4(1)(f) of the Directive states that personal data ought to be “processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.” What this means for the potential operators of the Big Data Surveillance scheme in question is that they have to prepare, operate and continuously update a sophisticated set of technologies and procedures which would be implemented at each of the four stages of Big Data Surveillance-related processing, to ensure maximum security of the processed data.

3.2. Distinguishing between categories of subjects

Looking beyond the key data protection principles, the LEDPD contains multiple further provisions which could affect the design and operation of a Big Data Surveillance scheme. The first of those can be found in art. 6 of the Directive, which states that Member States should ensure “where applicable and as far as possible” that the relevant data controllers “make a clear distinction between personal data of different categories of data subjects”. The article gives four examples of such categories –

a) “persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;” (suspects)

b) “persons convicted of a criminal offence;” (convicts)

c) “victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence;” (victims)

d) “other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b)” (related parties/witnesses)

At first sight, this article may seem as if it’s lacking a certain component – the data controllers are to make a distinction, but it is not specified what should be the basis or goal of this activity. Recital 31 of the Directive attempts to support the understanding of this article, but its explanation is limited to stating that multiple categories of personal data are inherently processed in the areas covered by the Directive, and hence, “a clear distinction should, where applicable and as far as possible, be made between personal data of different categories (...).” Looking beyond the wording of the Directive, it is possible to see art. 6 as stemming from the principle of data accuracy; if no distinction is made between various types of data subjects, it is possible that they may suffer harm due to being inaccurately classified as a member of a wider group, and not being treated differently, where they
should have been. To give a Big Data Surveillance-related example – if victims’ data was collected in a situation where it is unlikely to help in prevention of further terrorist acts or serious crimes, their right to data protection would be unnecessarily infringed, through lack of compliance with art. 6. Another way of justifying this provision’s requirement is that it is supposed to guide parties such as Big Data Surveillance designers/operators towards collecting data of the four indicated categories of data subjects, while leaving other categories and public as a whole outside of the equation. Finally, art. 6 can also be seen as a conceptual extension of the purpose specification principle, outlined in the previous section.

Hence, designers of a Big Data Surveillance scheme would have to make sure that a distinction is made between various categories of personal data, at all stages of the process – when data is collected, accessed, retained and analysed (with the last one probably being the most important). Regarding the depth of distinctions made, apart from giving attention to the four categories of data subjects listed in art. 6, it seems feasible to suggest that a distinction should be made every time a group of people can be reasonably distinguished in order to prevent unjustified, noticeable harm (potential or actual) which could result from their data being processed within the scheme. And oftentimes, such an approach may align with the goals of the Big Data Surveillance operators, i.e. to obtain precise, factual connections which could assist in prevention of terrorism or serious crime.

### 3.3. Distinguishing between facts and assumptions

The next requirement of the LEDPD is also based on making a suitable distinction – this time between facts and opinions. Art. 7(1) obliges the Member States to “provide for personal data based on facts to be distinguished, as far as possible, from personal data based on personal assessments”. In doing so, the provision shares the goals behind art. 6. Insufficiently verified personal data can prove to be unjustly harmful to the legitimate interests of the data subject. For example, an opinion that someone is a close acquaintance of a terrorist suspect could cause the Big Data Surveillance scheme to suggest the presence of factual connections which could in turn prompt the scheme’s operators to subject the data subject to additional scrutiny.98

Consequently, the Big Data Surveillance scheme designers should ensure that adequate checks are in place to distinguish facts from mere opinions, during each of the key four stages of the process. Such and similar efforts would be required by art. 7(2) of the LEDPD, which provides that “(a)s far as possible, in all transmissions of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date shall be added”. That being said, drawing correctly the line between facts and assumption can be an exceedingly difficult task, and the LEDPD gives little guidance to facilitate it. For example, a conclusion reached by an intelligence analyst may nearly always be challenged on the ground of being an opinion.

### 3.4. Treatment of sensitive data

In EU data protection law, certain categories of data are labelled as “sensitive” or “special” due to the fact that they are judged to have the intrinsic potential to cause specific harm to the interests of the data subject. In LEDPD, sensitive personal data is that which reveals “racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely

---

identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”. In this regard, the LEDPD mirrors art. 9 of the GDPR. The Directive provides that such data can only be processed where it is “strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject” and under one of the three specific conditions. The first is that it has to be authorised by EU or Member State law. The second occurs where processing is conducted to “protect the vital interests of the data subject or of another natural person”. Finally, the third takes place “where such processing relates to data which are manifestly made public by the data subject”.

Sensitive personal data could be particularly useful for the discussed Big Data Surveillance scheme, due to the depth of information it can reveal about persons. In order to take advantage of such data, Big Data Surveillance operators would need to prepare convincing evidence, indicating that the use of sensitive data is necessary, and that “ordinary” personal data is insufficient for the aim of fighting terrorism and/or serious crime. Also, it is very likely that additional, sensitive data-specific safeguards would have to be in place – unless the contrary can be proven. When looking at three possible supplementary conditions, it seems that the first one would be easiest to meet by the Big Data Surveillance operators, provided there exists a relevant piece of legislation, allowing for the use of sensitive data specifically. The second condition is primarily dependent on the interpretation of what constitutes a “vital” interest. There definitely would be a good case for stating that ensuring security in public spaces and preventing threats to health and life of citizens are directly connected to the vital, fundamental interests of society. Finally, the definition of what constitutes data made “manifestly” public would be crucial for the third supplementary condition. It can be assumed that the intention here is to cover data the data subject has purposively decided to make available to anyone – so a Facebook post made available only to the data subject’s “friends” would not fit the bill.

It is crucial to remember that regardless of which of the three pathways to legitimacy is relied on, the criterion of necessity applies, in the same way.

### 3.5. Automated decision-making

It may be possible for automated decision-making systems to be a part of a Big Data Surveillance scheme; for example, when deciding on the subsets of data that are to be collected. This is where art. 11(1) of the LEDPD comes into play, obliging the Member States to “provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited” – unless this is authorised by EU or MS law and supported by “appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller”.

The goal of this obligation is to prevent harm which may result from both human and machine mistakes tied to the human decision to off-load certain decisions to computer programs. It is very easy to imagine how the automated decision-making system based on the predictive data emerging from a counter-terrorism oriented Big Data

---

99 LEDPD, supra fn. 14, art. 10.
100 Though it should be noted that art. 10 of the Regulation (outlined in section 2.2.3) is not reflected in the LEDPD.
101 LEDPD, supra fn. 14, art. 10(a).
102 LEDPD, supra fn. 14, art. 10(b).
103 LEDPD, supra fn. 14, art. 10(c).
Surveillance scheme could produce “an adverse legal effect concerning the data subject” or affect him/her significantly.

There is a range of law enforcement measures which, if applied, could match either or both of the indicated circumstances. The guidance which emerges for the operators of the discussed Big Data Surveillance scheme is that they should, in principle, avoid using automated decision-making systems without human oversight taking place before an action likely to carry the sort of impact described in art. 11 is taken. Any deviations from the “human in the loop” principle should be rare and sufficiently justified; and following art. 11(2), should such deviations relate to the automated decision-making with the use of sensitive data, additional, suitable safeguards ought to be present.

3.6. Data subject rights

The LEDPD sets out a set of data subject rights, which could be invoked in relation to data processing activities forming a Big Data Surveillance scheme. This section begins by setting those rights out, and then considers under which conditions they could apply to the studied use of personal data.

There are arguably four key rights relevant to the processing covered by the LEDPD – a slightly shorter list than in the case of the GDPR. The first one appears in the previous section – the right to obtain human intervention in cases of automated decision-making. The second is the right of access to information about processing, present in art. 13. The third is the right of access to processed personal data, set out in art. 14. Finally, there is the right to rectification or erasure, set out together with the right to object to data processing in art. 16.

The exercise of rights set out in arts 13, 15 and 16 can be limited within the Directive on the grounds tied to the integrity of the law enforcement processes and wider notion of security. It is also important to mention art. 18 of the Directive, which allows the Member States to further limit the exercise of rights set out in arts. 13, 14, and 16 in cases “where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings”, provided this is done in accordance with a relevant Member State law.

The usual challenges arise when one considers the application of data subject rights to the position of potential Big Data Surveillance operators. Exercise of such rights may (though does not have to) undermine the operators’ efforts, by e.g. releasing information which reaches the potential perpetrators, or removing information which could help in drawing the desired, useful factual connections leading to prevention of terrorism and/or serious crime. Also, the burden on operators’ resources has to be considered as well. Consequently, it is fairly likely that the Big Data Surveillance operators would seek to limit the exercise of the discussed rights, as far as possible. Would they be likely to succeed? In section 2.2.2 above, it was shown that while the Big Data Surveillance operators’ goals and activities would provide a good match to the indicated grounds for exemption, the criteria of necessity and proportionality would be essential in the resulting balancing exercise with corresponding fundamental rights and legitimate interests. The arguably most crucial point of interpretation here is how specific should the Big Data Surveillance operators be in providing evidence of necessity and proportionality, and at what stage should such evidence be provided. Requiring a specific, fully individual analysis for every data subject, explaining why this particular exercise of a right cannot be allowed could be seen as asking for too much. On the other hand, allowing the denial of requests on a broad ground of security (public or national), without any further details, could very well

---

104 See section 2.2.2.
be seen as asking for too little. Perhaps the adequate point of balance would lie in the vicinity of a group-based explanation approach, with a specification of the threat concerned. To draw up an example, the same denying reply could be addressed to a particular category of subjects (e.g. suspects) whose non-sensitive data is processed, based on the threat to specific, ongoing investigations. Such replies could then be securely stored and remain available for review by the oversight body.

3.7. Data protection by design

While data subject rights within the LEDPD become relevant after the processing of personal data has already started, this Directive also places certain obligations on the data controllers which take effect even before the processing has started. A key example here is provided in art. 20, which requires the data controllers to take organisational and technical measures, of their own initiative and design, aimed at compliance with data protection principles. An example given in the provision is pseudonymisation of data in order to comply with the data minimisation principle.\(^\text{105}\)

Formalisation of the concept of data protection by design is fairly new in the field of data protection law. It is also a part of the wider trend aimed at enhancing accountability of information-processing entities.\(^\text{106}\) Art. 20 can be seen as a broader, less clear provision, encouraging the consideration of data protection issues early on, without a direct line of punishment for failure to do so. By its nature, it lacks explanation of how innovative, effective, and resource-intensive those preliminary acts of design should be.

For the Big Data Surveillance operators, the best way to ensure compliance is to conduct a thorough, dedicated assessment of technological and organisational measures which could be taken at each step of the Big Data Surveillance process, in order to maximise compliance with the LEDPD’s data protection principles and obligations. Such an assessment should also be periodically renewed, with an option for emergency reviews, should the situation call for it (e.g. if new technology emerged, if new type of threat appeared, etc.).

3.8. Security obligations

The LEDPD is quite specific and prescriptive when it comes to the data security obligations of the data controllers. While art. 29(1) of the Directive provides for a broad duty to take reasonable technical and organisational measures aimed at ensuring the security of personal data (sensitive data in particular), art. 29(2) is much more direct. Among the list of ten examples it provides, one can find measures which are to “deny unauthorised persons access to processing equipment used for processing (‘equipment access control’);\(^\text{107}\) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data (‘storage

---

\(^{105}\) See section 3.1 above.


\(^{107}\) LEDPD, supra fn. 14, art. 29(2)(a).
control’),”\textsuperscript{108} and “ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment (‘communication control’).”\textsuperscript{109}  

In terms of compliance with art. 29, the Big Data Surveillance operators would, in principle, be required to design and implement measures reflecting each of the ten categories present in art. 29(2). However, it should be noted that this obligation is conditional on a preliminary “evaluation of the risks” – hence, it can be assumed that if a Big Data Surveillance operator would be able to show that implementing a specific security measure is likely to create a sufficiently grave and probable “risk”, then the scope of art. 29(2) could theoretically be limited.

It is also worth bringing attention to arts. 30 and 31 which require the data controllers to communicate personal data breaches to supervisory authorities and data subjects respectively. In art. 30, the controller is obliged to notify the authority “without undue delay and, where feasible, not later than 72 hours after having become aware of [the breach]” – though notification is not required where there is a low likelihood of “a risk to the rights and freedoms of natural persons”.\textsuperscript{110} In art. 31, the obligation to communicate the breach to the data subject is conditional on there being a likelihood of the breach resulting in a “high risk to the rights and freedoms of natural persons”\textsuperscript{111} – a step higher than art. 30. Furthermore, art. 31(3) sets out three scenarios in which notification to the data subject would not be required. First, where the data controller took measures which made the leaked data “unintelligible to any person who is not authorised to access it”.\textsuperscript{112} Second, where measures were taken post-breach, as a result of which the earlier mentioned high risk to rights and freedoms “is no longer likely to materialise”.\textsuperscript{113} Third, where communicating the breach to the data subject “would involve a disproportionate effort” – in which case a “public communication or a similar measure” has to take place.\textsuperscript{114}

In order to maximise compliance with arts. 30 and 31, the Big Data Surveillance operators ought to start by focusing their efforts on procedures which would prevent the leaked data from being legible enough to outsiders to identify the individual data subjects, thus decreasing the risk to corresponding rights and freedoms. Additionally, given that such methods of anonymization are unlikely to be impenetrable, efforts should be taken to prepare suitable \textit{ex post} measures and evidence tied to the proportionality of contacting each data subject separately. Finally, consideration should be given to the appropriate form of a public communication concerning the potential breaches, which would meet the legitimate expectations, without unduly undermining the effectiveness of the Big Data Surveillance operation.

\textbf{3.9. Independent supervision}

The final aspect of the LEDPD which must be covered in this paper is its set of requirements tied to the external supervision of the discussed data processing activities. As the CJEU stated in \textit{Commission v Germany}, supervisory authorities form “an essential component of the protection of individuals with regard to the processing of personal
Given the strategic importance of the discussed Big Data Surveillance scheme, the vast array of risks attached to it, and the considerable power which could be obtained by using the scheme, it is necessary for the suitable, effective supervision of Big Data Surveillance scheme(s) to take place. Section of the LEDPD which is aimed at achieving this goal starts at art. 41, which obliges the Member States to "provide for one or more independent public authorities to be responsible for monitoring the application of this Directive". The cited article suggests that Member States may indicate this authority to be the same one responsible for monitoring the application of the GDPR. Art. 42 of the LEDPD outlines several requirements aimed at providing the independence of the supervisory authority. These start with ensuring that the authority remains completely independent, what includes that they should "remain free from external influence, whether direct or indirect, and that they shall neither seek nor take instructions from anybody". The authority should also be able to choose its own staff and have a separate, dedicated budget.

Art. 46 lists twelve activities which the supervisory authority should undertake on its territory. Among those, the crucial one is to "monitor and enforce the application of the provisions adopted pursuant to this Directive and its implementing measures". This could be seen as further elucidated by the latter provisions on the list, which include conducting investigations into the lawfulness of processing (especially after data subjects' complaints), monitoring developments (e.g. technological) which may impact the protection of personal data and providing preliminary consultations for data controllers (where new "high-risk" filing systems are to be created), as well as exercising the data subjects' rights as the latter's representative.

It goes without saying that the Big Data Surveillance operators would have to cooperate with the supervisory authority assigned to them for the purpose of compliance with the national law enacting the LEDPD. It is also quite clear that preliminary impact assessments, mentioned in the previous paragraph, would have to take place. The key question, however, is which entity would undertake the supervision in question. The Directive leaves discretion in this matter to the Member States, allowing for this to be either the general data protection authority (DPA), or some form of a more specialised body.

---

115 Case C-518/07 Commission v Germany, at para. [23].
116 For the ECtHR's position on supervisory requirements, see Big Brother Watch v UK (supra fn. 17), paras. [317] and [377] in particular. As Murray and Ng argue, the ECtHR downplayed (in a surprising manner) the importance of judicial/independent supervision (supra fn.17).
117 LEDPD, supra fn. 14, art. 41(3).
118 LEDPD, supra fn. 14, art. 42(1).
119 LEDPD, supra fn. 14, art. 42(2).
120 LEDPD, supra fn. 14, art. 42(5).
121 LEDPD, supra fn. 14, art. 42(6).
122 LEDPD, supra fn. 14, art. 46(1).
123 LEDPD, supra fn. 14, art. 46(1)(f) and (g).
124 (I.e. data processing operations/schemes)
125 LEDPD, supra fn. 14, art. 17.
126 Looking to the ECtHR case law and the decision in Szabo and Vissy v. Hungary (Application no. 37138/14) (Jan. 12, 2016), para [75], it seems that within the ECHR framework, relying on judicial authority in the discussed context would be the most adequate option.
At this point, it is worth mentioning a study conducted by the Article 29 Working Party,\textsuperscript{127} which explored the existing arrangements in Member States pertaining to the supervision of intelligence services. Given that such services would be quite likely to perform as Big Data Surveillance operators (they exist in 26 out of 27 EU countries\textsuperscript{128}), the findings of the study are definitely of interest to this paper. Firstly, supervision is based either on general data protection laws or on specialised laws governing the processing of personal data by intelligence services.\textsuperscript{129} In thirteen states, the DPAs’ authority “includes the national security and intelligence services within scope”;\textsuperscript{130} in nine states, DPAs have no authority over intelligence services; and only Sweden and Slovenia have full DPA supervision over such services’ compliance with data protection laws.\textsuperscript{131} Furthermore, twenty Member States declared that they have parliamentary oversight/control over intelligence services’ activity.\textsuperscript{132}

From the perspective of potential Big Data Surveillance operators, a lot would depend on which Member State they come from, and what supervision arrangements are already in place there. It is certain that the lawmakers wishing to implement Big Data Surveillance for the discussed purposes would have to ensure that such arrangements are based around an entity which is independent when viewed from the multiple angles specified by the LEDPD.\textsuperscript{133} Regardless of what this entity would end up being, the Big Data Surveillance operators should, from the very start, be open to meaningful cooperation with it.

\textsuperscript{128} A29 WP Opinion 04/2014, supra fn. 127, at p. 9.
\textsuperscript{129} A29 WP Opinion 04/2014, supra fn. 127, at p. 9.
\textsuperscript{130} A29 WP Opinion 04/2014, supra fn. 127, at p. 10.
\textsuperscript{131} A29 WP Opinion 04/2014, supra fn. 127, at p. 10.
\textsuperscript{132} A29 WP Opinion 04/2014, supra fn. 127, at p. 10.
\textsuperscript{133} The ECtHR case law could offer further guidance with regards to the meaning of independent supervision; for example, see Szabo and Vissy v. Hungary [2016] (supra fn. 126), at paras [77] to [80].
4. Big Data Surveillance and Art. 52(1) of the CFREU

Having explored the boundaries set to Big Data Surveillance by the LEDPD, this report can now proceed to its second major section, focused on guidance stemming from the CFREU itself, and from the CJEU’s relevant interpretations of this instrument. As covered in section 2.2.1, art. 52(1) is the key, overarching provision governing the relationship between security and data protection in the current context. In Digital Rights Ireland, the CJEU underlined that any processing of personal data constitutes an interference with the right protected by art. 8 of the Charter134 - and in the context of Big Data Surveillance measures, security is the key legitimate interest which may justify the corresponding forms of such an interference. Whenever guidance flowing from instruments such as the LEDPD leaves space for interpretation, the CJEU is going to look towards art. 52. Additionally, as Lyskey notes, the domestic legislation implementing EU data protection instruments (such as that governing data retention regimes in accordance with art. 15(1) of the E-Privacy Directive135) can itself become, as it was stated in the Pfleger136 case, subject to an art. 52-based review.137 And indeed, this is what happened in the crucial Watson138 case.

For the purposes of this section, it is worth taking a second look at the text of this provision, which states that:

“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.”139

For the purposes of this paper, five key elements of guidance can be extracted. The interference has to be:

1. Provided by law
2. Respecting the essence of the right interfered with
3. Necessary and proportionate
4. Meeting an objective of public interest
5. Meeting the need to protect rights and freedoms of others

Each of those elements is discussed separately in this section. While, as Lyskey rightly states, the CJEU has a much thinner portfolio of cases on the interaction between data protection and security than the European Court of Human Rights (ECtHR) does on the related interface between privacy and security140 certain strands of Big Data Surveillance-oriented guidance can be nonetheless extracted from the art. 52(1) judgements of the EU’s highest court.

134 Digital Rights Ireland, supra fn. 3, at para [36].
135 EPD, supra fn. 67
136 Case C-390/12 Pfleger [2014].
137 Lyskey, supra fn. 47, at p. 168.
138 Watson (CJEU), supra fn. 5
139 CFREU, supra fn. 43, art. 52.
140 Lyskey, supra fn. 47, at p. 161.
Before proceeding further, it has to be underlined that not all relevant statements made in the CJEU judgements always fall clearly under one specific element of art. 52(1). Consequently, approximations of classification may take place in the following sections.

4.1. Provided by law

The first element required to justify an interference with a Charter-protected right or freedom is that it has to be “provided for by law”. As stressed by the CJEU in Schrems, “EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court’s settled case-law, lay down clear and precise rules governing the scope and application of a measure”.141

The importance of the “provided by law” requirement was underlined in the European Essential Guarantees paper, which set out an advisory list of four principles prepared by the art. 29 Working Party. The Guarantees build on the EU and ECHR law requirements to “provide guidance when assessing if an interference with a fundamental right can be justified and apply to all data processing operations, including transfers on the basis of Articles 25 and 26 of the [Data Protection] Directive.”142 While it has to be remembered that the Guarantees (in contrast to the Charter and the CJEU case law) are not legally binding, it is worth referring to them in this section, as both an advisory source and a resource highlighting the relevant interpretative challenges.

The first of those guarantees is that “the processing must be based on a precise, clear and accessible (i.e. public) legal basis”.143 Such a basis should be set out in statute law and cover “the nature of the offences which may give rise to an interception or surveillance order”, a “definition of the categories of people that might be subject to surveillance”, “a limit on the duration of the measure”, “the procedure to be followed for examining, using and storing the data obtained”, and the “precautions to be taken when communicating the data to other parties.”144 Additionally, if the law in question entails retention of communications data, it ought to set out the conditions of access to such data – a statement supported by the Digital Rights Ireland and Tele2/Watson cases.145

What does the first element of art. 52 mean for the discussed use of Big Data Surveillance? First of all, it has to be noted that it matches conceptually the first data protection principle of the LEDPD, which states that personal data should be “processed fairly and lawfully”.146 Unfortunately, the CJEU cases do not provide much further answers to questions which arose in section 3.1 of this paper, apart from the requirement to supplement data retention provisions with provisions on data access. For example, it is unknown whether the planned Big Data Surveillance analytical activities should be set out in the discussed legislation, and if yes, then to what extent should they be narrowed down and to what extent can they remain flexible.

141 Schrems, supra fn. 4, at para. [91].
142 Article 29 Working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (2016), 16/237, at p. 3. Instead of the Data Protection Directive, the Guidelines can now be seen as applying to the GDPR.
143 A29 WP Working Document 01/2016, supra fn. 142, at p. 7.
144 A29 WP Working Document 01/2016, supra fn. 142, at p. 7. It should be noted this position was built through references to the European Court of Human Rights case law.
145 Digital Rights Ireland, supra fn. 3, at para. [60], and Watson (CJEU), supra fn. 5, at para [117].
146 LEDPD, supra fn. 14, art. 4(1)(a) (emphasis added).
4.2 Respecting the essence of those rights

The second element of art. 52 is probably the most elusive one. It states that an interference with a right or freedom should “respect [its] essence”.147 In CJEU case law, this concept appeared in cases such as Schrems148 and PNR149. In Schrems, it was stated that “legislation permitting the public authorities to have access on a generalised 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”.150 This could, potentially, be the same position that would be maintained in relation to the right to data protection, the essence of which is not discussed in the judgement. In PNR, which was an opinion of the Grand Chamber revolving around a data exchange agreement concerning passenger name records (PNR), the CJEU stated that the PNR exchange agreement is “not liable adversely to affect the essence of the fundamental right(...) enshrined in article(...) 8 of the Charter”.151 This finding was based on the discussed agreement containing provisions limiting “the purposes for which PNR data may be processed”152 and laying down “rules intended to ensure, inter alia, the security, confidentiality and integrity of that data, and to protect it against unlawful access and processing”.153

For Big Data Surveillance operators, the resulting guidance is that, first - assuming equivalence in the Schrems judgement between arts. 7 and 8 of the CFREU - the scheme should not allow them to have access to the content of electronic communications on a “generalised” basis. Second, by making a parallel between the PNR agreement and Big Data Surveillance-enabling legislation, it may be stated that the latter should contain purpose-limiting and security-oriented provisions. Requiring the presence of the former is directly corresponding to the second data protection principle of the LEDPD,154 which states that personal data should be “collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes”.155 Similarly, requiring the presence of security-oriented provisions can be directly connected to the sixth data protection principle of the LEDPD, stating that data should be “processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures”.156

It is evident that the cited parts of the CJEU’s decisions do not offer helpful guidance in relation to the key uncertainties which appear in the context of the LEDPD – such as whether the term “generalised” can be interpreted as “indiscriminate” (in the context of basis of access), or what should be the content of purpose-limiting and security-oriented provisions. Answers may appear with further interpretation of the “essence” of the right to data protection.

147 CFREU, supra fn. 43, art. 52(1).
148 Schrems, supra fn. 4.
149 Opinion 1/15 on the EU-Canada PNR agreement (2017), at para. [149].
150 Schrems, supra fn. 4, at para. [94].
151 PNR, supra fn. 149, at para [151].
152 PNR, supra fn. 149, at para [150].
153 PNR, supra fn. 149, at para [150].
154 (Discussed in section 3.1 above)
155 LEDPD, supra fn. 14, art. 4(1)(b).
156 LEDPD, supra fn. 14, art. 4(1)(f), also discussed in section 3.1 of this paper.
There is an additional element of essence-related guidance from the CJEU which is worth mentioning here, despite not being specifically related to the essence of the right to data protection itself. In Schrems, the CJEU stated that “legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.”\textsuperscript{157} It is interesting how this position would be reconciled with LEDPD’s restrictions on the exercise of the indicated rights – for example, if the Big Data Surveillance operators were, in practice, able to deny all corresponding data subjects’ requests.

4.3. Principles of necessity and proportionality of limitations

Art. 52 provides that “(s)ubject to the principle of proportionality, limitations may be made only if they are necessary”. Drawing on the European Court of Human Rights decision in Szabó v Hungary,\textsuperscript{158} to outline the relationship between necessity and proportionality: the necessity test explores the overall necessity of a measure/interference in a democratic society; by contrast, the proportionality test seeks to ensure that the said measure/interference is well balanced with the legitimate aim pursued.\textsuperscript{159} In this regard, both principles are directly connected to the first data protection principle of the LEDPD, which (as it was explained in section 3.1 above) contains the requirement of objective-based necessity. Consequently, the concepts of proportionality and necessity are sufficiently interrelated and overlapping in the discussed context to be covered together in this paper, without undermining the distinction in the nature of those concepts. Additionally, necessity and proportionality are joined together in the second Essential Guarantee set out by WP29.\textsuperscript{160}

The criteria discussed in the following section are, without doubt, of key importance in the Big Data Surveillance scheme debate and feature prominently in the CJEU case law. In this regard, special attention should be given to the Tele2/Watson case, which provides several strands of guidance, woven around the notion of necessity in particular. The following paragraphs focus on this decision and consider the application of each element of guidance sequentially.

Firstly, according to the CJEU, only the objective of “fighting serious crime” can be seen as capable of justifying the retention of all traffic and location data\textsuperscript{161} – thus, Big Data Surveillance scheme designers wishing to do include such retention would need to focus on the same objective. However, a consequent question emerges; what about the scheme’s iterations based on less privacy/data protection-invasive elements? The CJEU addressed this question in the newer Ministerio Fiscal decision, proclaiming (in the context of the E-Privacy Directive’s provisions), that while serious interferences with arts. 7 and 8 Charter rights require focusing on the objective of fighting serious crime, the less serious interferences can be justified within activities aimed at tackling non-serious crime.\textsuperscript{162} What makes an interference “serious” is an ongoing, unsettled question in this context. However, by drawing a comparison with the interference in Ministerio Fiscal (obtaining data on SIM card ownership, for a narrow period of time, for one

\textsuperscript{157} Schrems, supra fn. 4, at para. [95].
\textsuperscript{158} Szabo and Vissy v. Hungary (Application no. 37138/14) (Jan. 12, 2016)
\textsuperscript{159} Szabo, supra fn. 158, at para. [74] – [75].
\textsuperscript{160} A29 WP Working Document 01/2016, supra fn. 142, at p. 7.
\textsuperscript{161} Watson (CJEU), supra fn. 5, at para. [102].
\textsuperscript{162} Ministerio Fiscal, supra fn. 6, at para [57].
stolen phone), it could well be argued that Big Data Surveillance schemes would almost invariably involve a serious interference with Charter rights – and hence, as a general position, such schemes would need to be focused on tackling serious crime.

However, a broad indication of this objective was not found to fulfil the art. 52-based test of necessity in Watson.\(^{163}\) Hence, even if not seeking to rely on the same, wide retention scheme, Big Data Surveillance scheme designers should most likely ensure to be more specific in this regard, even if the case does not offer guidance with regards to the degree of precision required. For example, should this be limited to a specific incident/group/geographical location/etc.?

On this note, it should be added that EU law does not, as noted in Digital Right Ireland,\(^{164}\) provide a definition of what “serious crime” is, leaving this in the hands of national legislation. One example of such a national definition is provided by the UK's Investigatory Powers Act 2016, which characterises serious crime as an offence for which one “could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more”\(^{165}\) or where “the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose”.\(^{166}\) It is a remaining question whether this and other national definitions align with the CJEU's understanding of “serious crime”, as the UK's definition seems to be significantly disparate from the Court's earlier case law, as noted by Murray, Fussey and Sunkin.\(^{167}\) Additionally, in Ministerio Fiscal, the CJEU was asked whether the length of prison sentences is a sufficient sole criterion for determining the legality of “serious crime” definitions\(^{168}\) but did not provide a direct, clarifying answer. Big Data Surveillance designers should be aware of the CJEU's treatment of this issue, in addition to following their respective national definitions of serious crime.

Secondly, the CJEU linked the notion of necessity with making a distinction between various categories of involved data subjects. The Court’s analysis started by showing that a communications data retention scheme covering “all subscribers and registered users and all means of electronic communication as well as all traffic data”\(^{169}\) has an impact on “all persons using electronic communication services”,\(^{170}\) even if there is no link between them and serious criminal offences.\(^{171}\) This, in the Court’s view went beyond what is strictly necessary for art. 52 purposes. Therefore, it seems that in order to meet the criteria of strict necessity, Big Data Surveillance operators would have to distinguish between various categories of data subjects, most likely not only at the stage of initial collection of data, but also in stages of accessing, storing and analysing data.

The Court also offered some guidance with regards to what kind of distinctions would be likely to matter in the discussed context – the challenged legislation was criticised for not being “restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved,

\(^{163}\) Watson (CJEU), supra fn. 5, at para. [103].
\(^{164}\) Digital Rights Ireland, supra fn. 3, at para [60].
\(^{165}\) Investigatory Powers Act 2016 c. 25, s. 263(1).
\(^{166}\) IPA 2016, supra fn.165, s. 263(1).
\(^{167}\) See the HRBTD project's Response to IPCO Invitation for Submissions on Issues Relevant to the Proportionality of Bulk Powers, available at [https://www.hrbdt.ac.uk/our-research/surveillance-human-rights/#publications], at p. 3.
\(^{168}\) Ministerio Fiscal, supra fn. 6, at para [26].
\(^{169}\) Watson (CJEU), supra fn.5, at para. [105].
\(^{170}\) Watson (CJEU), supra fn. 5, at para. [105].
\(^{171}\) Watson (CJEU), supra fn. 5, at para. [105].
in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime”. The indicated factors were rephrased in a latter part of the judgment, stating that art. 15 of the 2002/58 Directive, seen through the lens of the relevant Charter rights, “does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary”. This reasoning could be seen as indicating that Big Data Surveillance systems used for discovering and preventing threats within large sets of data containing a considerable amount of unrelated subjects’ personal data may struggle to fulfil the criterion of legality within the EU data protection regime.

That being said, vital questions remain – would it be acceptable to process a data set limited to a specific town where a previous perpetrator used to live? How should the time limits on collection/access/storage/analysis of data be set, especially in situations where the threat level is difficult to assess? There is a large scope for further interpretation of this guidance.

The described notions are reinforced further in the judgment. The Court stated that the legislation at hand must set out the circumstances and conditions warranting the preventive adoption of data retention measures. Also, it is crucial to maintain the connection between data retained and objective pursued, based on factors such as the scope of the measure and public affected.” Later, the importance of objective evidence is underlined – it has to show an at least indirect connection between the data of the affected public and serious criminal offences, as well as show that such data can “contribute in one way or another to fighting serious crime or to preventing a serious risk to public security.” Finally, the Court expands its reasoning regarding the geographical distinctions in setting limits to data retention – such distinctions can be drawn where objective evidence shows a “high risk of preparation for or commission of” serious criminal offences.

The CJEU also provided guidance with respect to accessing retained data, stating that access to retained data cannot exceed the limits of what is strictly necessary, and it is for the national legislation to establish appropriate access conditions. By making a reference to the ECHR case of Zakharov, the CJEU stated that “access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime.” Interestingly enough, this is followed by an exception tied to accessing data belonging to a wider group of individuals – “in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective

---

172 Watson (CJEU), supra fn. 5, at para. [106].
174 Watson (CJEU), supra fn. 5, at para. [109].
175 Watson (CJEU), supra fn. 5, at para. [110].
176 Watson (CJEU), supra fn. 5, at para. [111].
177 Watson (CJEU), supra fn. 5, at para. [105].
178 Watson (CJEU), supra fn. 5, at para. [116].
179 Watson (CJEU), supra fn. 5, at para. [119].
contribution to combating such activities.” 180 Finally, the Court adds that “as a general rule, apart from cases of “validly established urgency”, there should be a judicial or administrative review governing access of competent national authorities to the retained data”. 181

On the basis of those statements, several strands of guidance for Big Data Surveillance operators can be extracted. In seeking access to data, they ought to make distinctions between data subjects which, in practice, largely reflect those set out by the LEDPD. However, it seems that the scheme would be able to rely on data of other people in the described “emergency” conditions, provided that convincing evidence can be presented after the event – assuming, to the relevant oversight body. Outside of those situations, it seems that the operators in question would need to obtain judicial or administrative permission before getting access to a new data set.

The earlier data sharing case of Schrems echoes several strands of guidance from Watson. In the former case, the CJEU stated in the context of the EU – US data transfers that the criterion of strict necessity is not fulfilled where legislation warranting such transfers does not make “any differentiation, limitation or exception” regarding the pursued objective, as well as does not rely on “an objective criterion being laid down by which to determine the limits of the access of public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail”. 182

4.4. Meeting an objective of general interest

The fourth element of the art. 52 test is that the interference with a right or freedom has to “genuinely meet objectives of general interest recognised by the Union”. 183 In its decisions, the CJEU recognised public security as such an objective, most notably in the PNR case, where it stated that public security considerations are “capable of justifying even serious interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter”. 184 That being said, the use of data in the PNR case was aimed at “the fight against terrorist offences and serious transnational crime” 185 – it remains an open question where the threshold lies for threats lying outside of this category.

Applying the Court’s reasoning to Big Data Surveillance schemes, it seems that schemes expressly focused on terrorism and serious international crime shouldn’t have a problem fulfilling the “objective” of general interest criteria. By analogy, there does not seem to be a good reason for why serious national crime would not qualify as well – the earlier discussion of Watson in section 4.3 (placing the focus on “serious crime” without a geographical/jurisdictional limit) supports this position. On the other hand, anything below the serious crime level would be unlikely to qualify here – if the decision in Watson made such a finding in relation to communication data retention schemes; 186 a Big Data Surveillance scheme, involving a profound analytical element and likely to include data retention, would be even less likely to pass through the gate.

180 Watson (CJEU), supra fn. 5, at para. [119].
181 Watson (CJEU), supra fn. 5, at para. [120].
182 Schrems, supra fn. 4, at para. [93].
183 CFREU, supra fn. 43, art. 52(1).
184 PNR, supra fn. 149, at para. [149].
185 PNR, supra fn. 149, at para. [148].
186 Watson (CJEU), supra fn. 5, at para. [102].
4.5. Need to protect rights and freedoms of others

The final, fifth element required for the interference with a Charter right or freedom to be legal is that it has to meet “the need to protect rights and freedoms of others”. The objective of protecting security is strongly supported by the Charter rights and as long as the Big Data Surveillance scheme can demonstrate a causal link between its activity and ensuring security, it should be capable of fulfilling the fifth element of the art. 52(1) test.

187 CFREU, supra fn. 43, art. 52(1).
188 See arts. 2, 3, 6, 12, 17 and 45 of the CFREU.
Supplementary Disclaimers

There are several additional disclaimers which ought to be made with regards to the scope of this mapping paper. First of all, the paper is focused only on EU legislation and CJEU judgments, and not on the national implementations of EU laws, or the corresponding judgements of Member States’ courts. This is due to time and space considerations.

Secondly, the paper’s intention is to focus on the right to data protection, and its relevance as an interest placed against that of national/public security. While the debate on the relationship between the right to privacy (recognised in both ECHR and CFREU) and the right to data protection (recognised expressly only in CFREU) is vivid and ongoing, this paper embraces the latter right independently of the former – for reasons earlier discussed in section 1.

Thirdly, this is a doctrinal legal paper. Its analytical content is not aimed at delineating the current state of Big Data Surveillance technology, or locating its most effective form. Instead, the paper is rather focused on exploring the legal dimension in which European Big Data Surveillance schemes would have to function.

Moreover, the paper does not intend to provide a holistic overview of various forms of surveillance within the EU legal framework – an excellent study of this kind is provided e.g. by Tzanou, in her 2017 book. Instead, the paper looks at the legality of surveillance measures in the context of Big Data Surveillance and aims to construct a model of a legal scheme of this kind.

Finally, the paper’s analysis stops at the moment in which a Big Data Surveillance scheme produces patterns and correlations useful to law enforcement bodies – it does not assess the legality of various potential uses of such information, such as within automated decision-making systems. This is for reasons of cohesion, as well as time and space.
The Human Rights, Big Data and Technology Project

Human Rights Centre, University of Essex, Colchester CO4 3SQ
+44 (0)1206 872877

@HRBDTNews
www.hrbdt.ac.uk