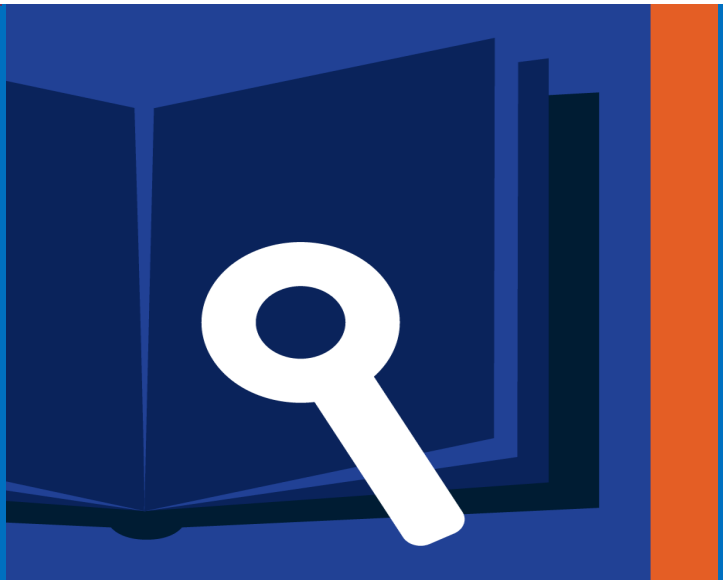
The CDSL Working Paper Series

WP2/2020



CYBER & DATA SECURITY LAB

Framing Big Data in the Council of Europe and the EU data protection law systems: Adding 'should' to 'must' via soft law to address more than only individual harms

Paul de Hert & Vagelis Papakonstantinou

This Working Paper to be published in the Computer Law and Security Review, 2021.

Reference to a CDSL WP should be made as follows: [Author(s)], [Title], CDSL Working Paper [number/year], available at https://cdsl.research.vub.be/en/publications

Abstract

On 19 November 2019 the Council of Europe hosted an international conference, immediately preceding the annual plenary meeting of its Committee of Convention 108, on "Convention 108+ and the future data protection global standard". One of the authors made a presentation on "Comparing the EU and Council of Europe approach to Big Data", and it is its contents and findings that are further elaborated in this paper; Its aim is, in essence, to incorporate the feedback received and to adapt past research on Big Data, that was mostly relevant to the EU, also on the Council of Europe data protection system. After a few preliminary remarks on Big Data terminology and possible regulatory approaches, Big Data regulation is examined against the EU and the Council of Europe data protection systems. Particular emphasis is given to the Council of Europe regulatory approach both in terms of Convention 108+ and with regard to its Guidelines on Big Data and AI. The authors believe that, because both the EU and the Council of Europe have avoided to refer to Big Data in their basic data protection regulatory texts (a most likely intentional omission), guidance is indeed needed, and it may well come in the form of soft law. The Council of Europe has taken the lead in this through its Guidelines; Their timely, comprehensive and balanced approach showcases the Council's will for such processing to indeed take place, but within a well-regulated environment, albeit not under a rigid regulatory construction.

Table of Contents

Table of Contents

1.Introduction

On 19 November 2019 the Council of Europe hosted an international conference, immediately preceding the annual plenary meeting of its Committee of Convention 108, on "Convention 108+ and the future data protection global standard". One of the authors made a presentation on "Comparing the EU and Council of Europe approach to Big Data"; It is the contents and findings of this presentation that are further elaborated in this paper, published in this Review's special issue on Convention 108+, after the kind invitation of the editors. However, this paper benefits from background that goes further back in time: It builds upon work carried out in the past by one of the authors on Big Data regulation in the EU.[1] It therefore constitutes the follow-up and update of that research, benefiting from the fruitful exchanges of the Council of Europe's conference.

Aim of this paper is, in essence, to incorporate the feedback received and to adapt past findings, that were mostly relevant to the EU, into the Council of Europe data protection system. However, this unavoidably carries the concrete consequence that, because research carried out in the context of the previous paper will not be repeated here, the analysis that follows will be admittedly misaligned, tilted toward the Council of Europe data protection system. While this is done for practical reasons, the authors believe that there is some further justification in this preference, in the sense that the Council of Europe has undertaken more concrete steps than the EU towards regulation of Big Data processing; It is exactly the assessment of this regulatory attempt both against EU standards and against the authors' own predisposition on the matter of regulation of Big Data that forms the core question of this article, namely whether, and if yes how best, to regulate Big Data personal data processing.[2]

∗ *Corresponding author: Vagelis Papakonstantinou, Faculty of Law & Criminology, Vrije Universiteit Brussel (LSTS), Pleinlaan 2, 1050 Brussels, Belgium E-mail addresses: paul.de.hert@vub.be (P. de Hert), evangelos.papakonstantinou@vub.be, vagelis@papakonstantinou.me (V. Papakonstantinou).*

[1] Paul de Hert and J Sajfert, 'Regulating Big Data in and out of the Data Protection Policy Field': (2019) 5 European Data Protection Law Review 338.

2 For a relevant analysis see, indicatively, Bart van der Sloot and Sascha van Schendel, 'Ten questions for future regulation of big data: a comparative and empirical legal study' (2016) 7 JIPITEC.

[3] EDPS Opinion on coherent enforcement of fundamental rights in the age of Big Data, Opinion 8/2016.

[4] See Opinion 3/2003 of the Article 29 Working Party, and also its Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU of 16 September 2014

[5] Apparently, a trend initiated in the 1990s by analyst Doug Laney (https://blogs.gartner.com/doug-laney/deja-vvvue-othersclaiming-gartners-volume-velocity-variety-construct-for-bigdata/)

[6] See, for example, the relevant Special Report in The Economist ("Data, Data Everywhere"), 27 February 2010.

[7] See also Peter Leonard, 'Customer data analytics: privacy settings for 'Big Data 'Business' (2014) 4 International Data Privacy Law 53, Nir Kshetri, 'Big Data's impact on privacy, security and consumer welfare' (2014) 38 Telecommunications Policy 1134

2. Big Data as an expression of enthusiasm. Three points about the need to regulate it

While the attempt to define Big Data or identify the legal challenges posed by it largely exceeds the purposes of this paper, here a brief presentation will be attempted in order to introduce three points that the authors would like to raise. As regards the former, there exists no commonly accepted definition of "Big Data". [2]The EDPS has attempted to define it as large amounts of different types of data produced at high speed from multiple sources, whose handling and analysis require new and more powerful processors and algorithms.[3] Similarly, the, then, Article 29 Data Protection Working Party has found that Big Data refers to "gigantic digital datasets held by corporations, governments and other large organizations, which are then extensively analyzed using computer algorithms".[4] This difficulty is not exclusive to lawyers: Information technology scientists also find it impossible to define it, having sought refuge to such elusive terms as the so-called three Vs of Big Data, namely variety, velocity and volume.

[5]The relative difficulty of defining the term "Big Data" becomes obvious merely by observation of its two constituting parts: Namely, what is "big"? In comparison to what? At which period of time? According to some metrics, humanity is doubling its data creation pace every few years.[6] Consequently, what constituted a large enough collection of data to be perceived as "Big Data" in 2014 would most likely not pass the "bigness" threshold in 2020.

In essence, Big Data is a made-up catchword. It is a term coined rather to express enthusiasm over a newly acquired technological capacity (humanity's ability to process large (- er) volumes of data) than a precise scientific method or type of processing.[7]It is aimed more at promoting than accurately describing. This new capacity may affect business methods or management strategies, and even create a few new professions, however it does not culminate into a new social phenomenon. Indeed, Google Trends, a metric of global online interest, if inquired on the term Big Data, demonstrates that it emerged forcefully around 2012, peaked around 2018, and is already in decline. As such, it appears that the term Big Data is bound to retreat to the background, incorporated into mundane business practices and daily lives same as was the case, in the past, with "cloud computing" (that Google Trends demonstrate emerged in 2008, peaked in 2012 and now is in 2008 levels) or, perhaps, the "Internet of Things" (which again under the same metric is now peaking), soon to be replaced by the newest technology trend.

Taking the above well-known findings into consideration the authors would like to raise three points – perhaps profiting from some cool-headed thinking afforded by the few years' time period that has lapsed since Big Data emerged.

The first point is of definitional nature: It refers to the confusion between Big Data and Big Data Analytics. Big Data denotes large collections of data, whereas Big Data Analytics refers to using these datasets for specific purposes (to extract patterns, create profiles, make predictions, etc.). However, there is clear difference between the two: Big Data is essentially only a large collection of data made possible by technology. Big Data stops at the point when data has been amassed and is ready to be processed. From a technical point of view, it is an end by itself (the making possible of creating and processing previously impossible to handle datasets); However, from a social point of view it is only a means towards meaningful analysis of this data set.

In other words, once assembled and made available, what happens afterwards to that data, the analysis that ensues, is realized by Big Data Analytics a completely different procedure that merits special analysis per set[8].

The second point is that Big Data poses a series of legal questions that are by no means exhausted within personal data protection confines.[9] If the phenomenon was to be comprehensively regulated, then legislators would have to take into account, apart from personal data protection, such issues as proprietary rights over (non-personal) data, public sector information (PSI), or even financial incentives addressed be each state to its internal market so as to invest in or apply Big Data. In other words, a holistic regulatory approach to Big Data would rather include framework, horizontal regulation than a standalone (personal data protection) act.

The third point is that regulation today is not single dimensioned. While legal acts (laws) are evidently found at its epicenter, the aims and purposes of regulation can be attained today also through other means: Most notably, and pertinently as regards Big Data, through official guidance issued by competent organisations. These organisations could be national (e.g., DPAs), international (the EDPB, the EDPS, or the Council of Europe respective organisations) or private (e.g., standards' issuing organisations), that are mandated to issue guidance without the typical status of law. Notwithstanding the discussion whether such guidance constitutes soft law or not (for brevity's sake this term shall be used from now on to denote it), the fact is that formal guidance issued by formal bodies develops indirect binding effect because their addressees (controllers,

[8] This distinction is clearly made in the Council of Europe's 2017 Big Data Guidelines (in p. 2), clarifying that "for the purposes of this analysis, the definition of Big Data therefore encompasses both Big Data and Big Data analytics".
[9] See also the, contemporary, EDPS suggestion for operation of a Big Data & Digital Clearinghouse (EDPS website accessed on December 2019
[10] De Hert and Sajfert, ibid.
[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
[12] Directive (EU) 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.

processors and individuals) are aware that it shall be taken into account by courts and DPAs while exercising their enforcement powers. At the same time, such guidance presents the advantage of being relatively quick to formulate and easy to update (at least if compared with formal laws). It can also be case-specific, regulating in detail a single type of processing.

In view of the above, the authors believe that comprehensive regulation in the form of a specialised legal act on Big Data is neither recommended or, even, attainable. Big Data has proven already too much of an elusive phenomenon to put down in legal provisions. The legal issues it poses transcend several fields of law; And it is only a matter of time before the term disappears: Today's "big" volumes of data will soon be incorporated into daily, mundane processing routine, thought of as the new "normal" processing circumstances perhaps incorporating artificial intelligence applications. On the other hand, the above do not mean that soft law is not needed, at least for an interim period of time: Indeed, its flexibility and time-relevance are critical assets when dealing with technological phenomena that storm into human lives and ask for immediate and responsive fixes rather than long-term legal provisions.

3. Big Data in the EU personal data protection system

Because this paper builds upon findings of a previous paper by one of the authors,[10] that focused on the approach adopted in the EU on Big Data particularly from a personal data protection point of view, readers are advised to consult its text for a more detailed analysis: Here only its findings will be summarised, for picture comprehensiveness purposes.

In the above paper De Hert and Sajfert put forward the following hypothesis: "Europe, to respond to the emergence of Big Data, has deployed two complementary strategies: On the one hand, counting on the vitality of existing data protection principles to frame a new development and thus continuing a principle-abiding approach in reform times (first strategy), and on the other, regulatory reform to enable Big Data developments based on a thorough re-evaluation of the regulatory principles (second strategy)".

For the purposes of this paper the EU and the Council of Europe approaches are examined separately, thus breaking the "European" approach examined by De Hert and Sajfert into its constituting parts; Consequently, attention in this section here will be given only to the EU approach (next section will then focus on the Council of Europe).

Starting point for the 2019 EU Big Data analysis mentioned above was the lack of explicit reference to the phenomenon of Big Data in the 2016 EU basic data protection texts – the GDPR[11] and the LED[12] – and the adoption shortly after 2016 of a number of (six) legal EU initiatives demonstrating the EU wish to facilitate the adoption of Big Data: Directive (EU) 2019/770 on digital content and services, the revised Copyright

Directive, the reform of the PSI Directive, the 2018 EU Regulation on the free flow of non-personal data, the 2015 Payment Services Directive (PSD2), as well as, the development of Ethics Guidelines for Artificial Intelligence. In essence, then, EU's approach on Big Data, although silent in data protection law, has become quite vocal in other fields of law.

Consequently, before elaborating upon these (six) policymaking legal instruments, De Hert and Sajfert were critical of the "first strategy" outlined above: The fact that neither the GDPR nor the LED pay any particular attention to Big Data. In their words, "one cannot help being surprised by the apparent missed rendez-vous between data protection law and Big Data technologies". According to their findings, the EU essentially applies a strategy whereby existing data protection principles are expected to stand up to the task of regulating Big Data. Their research also extends to speculate on the reasons that may have led to such "silence on Big Data", noting however at the same time that, whatever these may be, the fact remains that practitioners and courts are expected to deal with Big Data through existing, general data protection provisions. Assistance, if at all, is to be expected only in the form of soft law, to be issued by any one of the bodies concerned (the EDPB, the EDPS, Member State DPAs).

As regards the "second strategy" identified in the same paper, the EU appears to have endorsed Big Data outside its data protection law confines. Its authors assert that all of the above specific policy instruments include provisions aimed at the necessary flexibility and incentives in order to expand Big Data processing. These findings are by no means contested in this paper: Here it is merely noted that the above legal instruments are not personal data protection instruments. As discussed in our introduction of this contribution, the regulation of Big Data falls under several fields of law, it being a horizontal rather than case-specific phenomenon, and their analysis in the above paper demonstrates this in practice. Having said that, however, De Hert and Sajfert have correctly identified a policy trend that runs through (though not throughout) all EU law-making bodies. This finding may be against their preferences, but if not seen from a data protection perspective it does formulate a coherent strategy on behalf of the EU.

De Hert and Sajfert do not examine further the EU data protection system, meaning also Regulation 1725/2018[13] or security-related regulatory instruments with personal data protection extensions (for example, the Europol Regulation,[14]the Eurojust[15] and EPPO[16] Regulations, etc.). However, this appears to have been a sensible choice: Their primary finding, that EU data protection "missed the appointment" with Big Data also stands for other instruments and provisions falling under the EU data protection system as well. The only reason, perhaps, to have included such analysis would have been to further strengthen their argument that this is indeed a conscious EU policy and not an incidental one: Because no attention is given to Big Data in the EU data protection edifice whatsoever, it can be inferred that, for its own reasons, the EU considers this

phenomenon not worthy of specific personal data protection legal treatment. Accordingly, this paper, by summarising the above findings, confirms their validity also for the aims and purposes of this analysis.

4. Big Data in the Council of Europe personal data protection system

The Council of Europe has been the first international organisation to have issued binding data protection legislation. In 1981 it released its Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108''), almost simultaneously with OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. However, the significant difference between the two instruments is that the Council of Europe's text had been binding upon its signatory states. In fact, for almost fifteen years, until the EU Data Protection Directive of 1995[17] came along, Convention 108 remained the only international instrument to have achieved such binding effect[18].

The second important aspect of Convention 108, that kept it relevant for almost thirty years, even after the introduction of the EU Data Protection Directive of 1995, is that it remained the only instrument to have developed binding effect for personal data processing carried out for security-related purposes. The EU Data Protection Directive of 1995 expressly excused itself from such role;[19] Similarly, EU's Framework Decision of 2008[20] that would have supposedly held that role, did not manage to develop any binding effect at national Member State level after all.21 In fact, it was only in 2016 (or, more precisely, 2018, as per its implementation at Member State level date) that Convention 108 could at long last pass the torch for security related personal data processing in the EU to the LED.

However, until such time Convention 108 underwent a modernisation process itself; The Council of Europe deemed since 2010 that, after some thirty years since its introduction, it was time for an update. Admittedly,

[13] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
[14] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.
[15] Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation, replacing and repealing Council Decision 2002/187/JHA.
[16] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office
[17] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[18] The UN Guidelines for the Regulation of Computerized Personal Data Files, as adopted by its General Assembly Resolution 45/95 of 14 December 1990, are also of a non-binding effect.
[19] See its Article 3.
[20] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.
[21] See its Article 1.

in the intermediate period of time the Council of Europe issued an amendment of Convention 108 in 1999, that should have allowed the EU to accede to the Convention, as well as an Additional Protocol in 2001, that required each ratifying party to establish an independent authority to ensure compliance with data protection principles and laid down rules regarding transborder data flows. However, an overhaul of its text finally came in the form of a "modernisation" (not a replacement); The process lasted for eight years, hindered among others by the release at the EU of its own Data Protection Reform Package, and in 2018 its Amending Protocol was finally formally adopted (formulating in this manner Convention 108 into Convention 108+).

Work at primary legislation level within the Council of Europe did not stand in the way of soft law development. Indeed, the Council of Europe released over the years a number of important data protection guidance within the fields of application of Convention 108. It is within this context that, as regards Big Data, the Council of Europe issued its Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data on 23 January 2017 (the "2017 Big Data Guidelines").[22] Taken together with the text of Convention 108+ that by now is adopted, they constitute the Council of Europe's standpoint on this topic. However, because the general Council of Europe data protection system is of importance while placing its approach to Big Data into perspective, a brief analysis of Convention 108+ will be attempted here first.

5. The emergence of Convention 108+, its basic premises for the Council of Europe data protection system, and the influence of the EU data protection system

New challenges to human rights posed by technological developments, as well as, the belief that Convention 108's implementation and follow-up mechanisms should be strengthened made it clear that its text needed to be modernised in order to address the issues emerging from the increasing use of the internet and new technologies and the greater flows of personal data.23 The process for Convention 108's modernisation was initiated in 2010: On 10 March 2010, the Council of Europe's Committee of Ministers encouraged the modernisation of Convention 108 and issued a relevant position paper during the 32nd International Conference of Data and Protection and Privacy Commissioners. Work started within the Convention 108' s Consultative Committee (T-PD), that organised several meetings and drafted several amendment proposals.[24] The Committee of Ministers subsequently entrusted an ad hoc Committee on data protection (CAHDATA)[255]

[22] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data, 23 January 2017.

with the task of finalising the modernisation proposals. This task was completed in June 2016. The last phase of the work was carried out by the Committee of Ministers, which reviewed the CAHDATA proposals and consequently adopted the protocol amending the Convention on the occasion of its 128th session held in Elsinore on 18 May 2018. The Protocol was opened for signature on 10 October 2018 by the contracting States to Convention 108.

Convention 108's modernisation work was carried out in parallel with reforms of other international data protection instruments[26]; Most notably, it run in parallel with the EU data protection reform package that led to the GDPR and the LED respectively. In this context, in view of common membership of all EU Member States also in the Council of Europe, a conscious effort was made so that the modernised Convention would adhere to, or at least be compatible with, the EU legislative reform thus achieving consistency, compatibility and ultimately a harmonised data protection environment in Europe. At the same time the modernisation process was ruled by the common perception that the general and technologically neutral nature of Convention 108's provisions should be maintained and supplemented by more detailed sectoral laws on the basis, for instance, of the Committee of Ministers' recommendations. This approach was triggered by the belief that the neutral nature of Convention 108 in combination with its open character would provide countries (apparently, non-EU), that wish to ratify it with flexibility when implementing its provisions through their legislation. As a result, its operation as a simple treaty accessible by all the parties was to be maintained and strengthened.

The modernization process that turned Convention 108 into Convention 108+ brought a number of novelties in the old Convention's text and updated several of its existing provisions. Most pertinently to the purposes of this paper, new rights for data subjects and new obligations for controllers were introduced, the establishment of consent as a legitimate basis for processing was confirmed, as well as, the Convention's

[23] See Paul de Hert and Vagelis Papakonstantinou, 'The Council of Europe Data Protection Convention Reform: Analysis of the New Text and Critical Comment on Its Global Ambition' (2014) 30 Computer Law & Security Review 633; Graham Greenleaf, '"Modernising" Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?' (2013) 29 Computer Law & Security Review 430.

[24] These proposals were adopted at its 29th Plenary meeting (27- 30 November 2012) and submitted to the Committee of Ministers.

[25] CAHDATA was set up by the Committee of Ministers under Article 17 of the Statute of the Council of Europe and in accordance with Resolution CM/Res (2011)24 on intergovernmental committees and subordinate bodies, their terms of reference and working methods, the Ad hoc Committee on Data protection (CAHDATA) was responsible with the modernisation of Convention 108 and its Protocol

[26] See the OECD's, revised in 2013, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

[27] See Walter J P, The modernization of the Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data (ETS No 108): Moving from a European standard towards a universal standard for data protection? in Zombor F (ed.) International Data Protection Conference 2011, Hungarian Official Journal Publisher, and Graham Greenleaf, ' Modernising" Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?' (2013) 29 Computer Law & Security Review, 430

enforcement mechanism were enhanced through strengthening of the role of supervisory authorities and promoting cooperation and coordination.

One of the basic novelties introduced in the Convention's modernised text is the acknowledgement of individuals' consent as a lawful basis for the processing of their personal data. Consent is thus placed within the general context of the lawfulness of the processing. Even though the legal bases for lawful personal data processing constitute a basic component of the EU personal data protection system (first in its 1995 Directive, in Article 7, and then in Article 6 of the GDPR), the Council of Europe had not included a relevant reference back in 1981 in its Convention 108. Convention 108+ now covers this omission by explicitly referring to free, specific, informed and unambiguous consent as a condition that makes personal data processing lawful. It is understood that, in an effort to keep its neutral and more generic character, the modernized version avoids including a full list of all the conditions of legitimate processing (Article 6 of GDPR lists six). Instead, it chooses to expressly regulate consent and leaves space to national law to set any other legitimate basis. The explanatory report accompanying the Convention further clarifies the notion of "legitimate basis laid down by law"[28].

Controllers are placed squarely at the centre of Convention 108+, whereas it could be argued that its 1981 version (admittedly, αs expected at that time) was mostly addressed to states, that were expected to introduce relevant laws within their jurisdictions. This approach has mostly been abandoned in Convention 108+, that now includes concrete and specific obligations for controllers, being essentially addressed (also) to them. In practice, Convention 108+ now includes a more comprehensive definition of a "controller" [29]. Additionally, joint controllers are acknowledged, even though, contrary to the GDPR[30] no specific definition is included in Convention 108+. Similarly, the roles of "processors" and "recipients" have been added to the text of Convention 108+; By now many of the obligations imposed on controllers also apply to processors as well.[31]

Rights for data subjects have been strengthened in the text of Convention 108+: Transparency of the processing is treated under its new Article 8 and establishes an obligation for the controller to take any appropriate measure in order to keep the data subjects – who may be users, customers or clients – informed about how their data are being used. The inclusion of the principle of transparency was considered essential as it safeguards, together with the rights of article 9 (right to object, right of access, right to rectification, right to erasure, right to be informed of the purpose of processing, right to have a remedy, right to obtain assistance of a supervisory authority) and the additional obligations of controllers of article 10 (be compliant and be able to demonstrate compliance with the Convention[32] examine the potential impact of processing on the rights and fundamental freedoms of the data subjects prior to the commencement of such processing)[33] the rights of data subject at all stages of the processing of their data. These rights may, in accordance with article 11 of

Convention 108+, be limited only where this is provided for by law, fundamental rights and freedoms are respected, for specific grounds, and when it constitutes a necessary and proportionate measure in a democratic society.

Finally, as regards its monitoring and enforcement mechanism, Convention 108's additional Protocol was also revised by Convention 108+, that incorporated its provisions under Chapter IV (supervisory authorities). Aim of the new Chapter is, among others, to strengthen the powers and tasks entrusted to national supervisory authorities. In practice, their list of powers has been complemented and now includes also the power to intervene, to perform functions relating to transborder flows of personal data, to engage in legal proceedings, or bring to the attention of judicial authorities violations of data protection provisions. In addition to these powers, the supervisory authorities are also tasked with a duty to raise awareness, provide information and deal with requests and complaints of data subjects. In performing theirs tasks each supervisory authority is to act with complete independence and impartiality. A new article in Convention 108+ (Article 17) specifically regulates the forms of cooperation and mutual assistance between the supervisory authorities.

Without the above amendments it is doubtful whether Convention 108, essentially in its 1981 wording, would suffice to cater for the processing needs of such novel types of personal data processing such as Big Data. However, the Council of Europe having concluded the procedure that culminated into Convention 108+, can by now confidently deal with new challenges posed by new processing conditions. In a light or less light way, all new GDPR features that support its new accountability and enforceability paradigm are included also in the Convention 108+ text (e.g. accountability, privacy by design, impact assessments, boosted supervision and data subject rights); The same is the case with the deliberate, reluctantly Big Data-friendly, broader definitions of the principle of purpose limitation and permitted further processing.[34] Convention 108+ through its conscious approach to achieve compatibility but to avoid the rigidity of the EU data protection system, may have perhaps achieved the balancing point between regulation and flexibility that any types of new personal data processing ideas require. In spirit, the Council of Europe text remains loyal to the old idea of data protection based on a series of principles, whereas the EU data protection law has taken the policy option to harden these principles (that are faithfully recalled in the beginning of the GDPR, but then elaborated in subsequent chapters with more precise rules and detail). The merits and drawbacks of each approach are well-known[35]. Principles are more flexible than rules. Indeed, their balancing and conditional priority will vary according to the context. Therefore, they can provide more tailored solution, than hard-core rules would do. Moreover, principles being more abstract are more likely to be universal and are thus more "exportable" across different jurisdictions. From a human rights perspective, there might be more resilience in the CoE approach as opposed to the GDPR where rules and exceptions to rules (an inevitability in every rule-based model) were fiercely battled by the respective stakeholders. A perfect illustration in the context of AI and Big Data analytics

is the phrasing of Article 9.1(c) Convention 108+ that reads broader than Article 15 GDPR in the sense that it explicitly grants data subjects access to the decision-making process and expands this right explicitly beyond automated decisions[36].

In a former publication the authors had suggested more prudence on behalf of the Council of Europe in following the policy options chosen by the EU[37]. The two Europes do not serve the same audience, and the Council of Europe with its facility to open up its conventions and treaties to third parties (in essence, non-European States), an option that is openly and successfully pursued with Convention 108, is filling in the global data protection gap caused by the persistent inactivity of the United Nations[38]. Choices by the drafters of Convention 108+ to incorporate EU-specific policy options and distinctions need, in our view, to be seen under the light of the principle-rule distinction, in the light of the respective missions of the two international organizations and in the light of effective regulation of Big Data (analytics). Under this light, for instance, is the 'new' distinction between controllers and processors[39] a good Big Data idea? This remains questionable[40].

Similar is the case with the introduction of consent and the suggestion that it should play a key role in data protection law in Article 5.2 of Convention 108+. 41 Numerous are the works in the Big Data-relevant literature highlighting the illusory nature of consent to data processing, the unmanageable flood of consent-requests, the invasiveness of unreadable default privacy settings, and the general lack of knowledge of users about technical details related to the protection of their data, in addition to constant changes in the regulations of service providers and other controllers.[42]This introduction of consent as a legitimate processing ground, together with the introduction of the EU-inspired 'household activities exemption' in article 3.2 of Convention 108+,[43] and the introduction of the other GDPR-inspired 'legitimate processing grounds' in the Explanatory Report to Convention 108+ (in particular grounds such as 'fulfillment of a contract'),[44] renders Convention 108+ as unfit as the GDPR to face Big Data relevant phenomena such as the digitization of our personal lives and increased reliance on smart devices that remain connected to the vendors of these devices.[45] Time will tell whether the efforts in the Explanatory Report to Convention 108+ to 'tame' consent by subjecting it to proportionality testing,[46] will pay off. This recalls recent attempts by the European Data Protection Board to tame the legitimate ground of 'performance of contract', by proposing strict interpretations[47].

[28] The notion of "legitimate basis laid down by law", referred to in paragraph 2, encompasses, inter alia, data processing necessary for the fulfilment of a contract (or precontractual measures at the request of the data subject) to which the data subject is party; data processing necessary for the protection of the vital interests of the data subject or of another person; data processing necessary for compliance with a legal obligation to which the controller is subject; and data processing carried out on the basis of grounds of public interest or for overriding legitimate interests of the controller or of a third party".

[29] The natural or legal person, public authority, service, agency or any other body, which, alone or jointly with others, has decision making power with regard to data processing.

[30] See Article 26 of the GDPR.

[31] See, indicatively, articles 7 and 10 of Convention 108+.

[32] Principle of accountability. 33 Data protection by design, impact assessments

The points highlighted in brief above on the influence exercised by the EU and its GDPR system to Convention 108+ allow the authors to introduce one of our main ideas proposed in this paper: The respective resilience of both Convention 108+ and the GDPR will partly depend on the success of their soft law guidance machinery. We will come back to this below. Globally assessed, neither Convention 108+ nor the GDPR contain or take into account a proper analysis of the risks of Big Data. Experts agree on their very basic shortcomings in this respect: Their individual rights perspective, even if supported by an administrative enforcement system set up around it, makes them unfit for the collective problems and challenges of Big Data and Big Data analytics, as a practice that is fundamentally not interested in individuals but in their behavior in order to define categories of social practices that are relevant for the controller.[48] In a next section, the focus will be turned to the Council of Europe soft law-machinery that should, in our view, be taken into account to further develop this assessment.

6. The regulation of Big Data and the Council of Europe 2017 Big Data guidelines

When glancing at the new-born convention drafted in an era of expanding Big Data processing an observation imposed itself: No mention of Big Data is to be found in the text of Convention 108+. In essence, as is the case also with the GDPR and the LED, Convention 108+ abstained from expressly dealing with it in its text. On the other hand, the Council of Europe did issue horizontal guidance on this topic, in the form of its 2017 Big Data Guidelines; It also issued, on a neighboring topic, its Guidelines on artificial intelligence and data protection (the "2019 AI Guidelines") on 25 January 2019.[497]

---

[33] Data protection by design, impact assessments.

[34] See on the broader definition of the purpose limitation principle, art. 5.2(b) of Convention 108+. The new text also adds a new Article 10 (additional obligations), embedding at least four additional data protection concepts potentially open to Big Data processing – the principle of accountability, the data protection/privacy impact assessments, data protection by design and the risk-based approach.

[35] Ronald M. Dworkin, 'The Model of Rules', 35 U. Chi. L. Rev. 17 1967-1968. All norms are according to Dworkin either rules or principles. Rules work in an all-or-nothing fashion. They are either valid, and in that case, they must be respected, or invalid. If there is a conflict of rules a possible way to solve it is to envisage an exception to a certain rule. Principles, on the contrary, are to be conceived in an "optimizing" perspective. They set an optimum standard, which has to be complied with, compatibly with the factual or legal situation. Comp. with Gallanth who conceives principles as normative statements which may or may not harden in rules of law, while rules of law themselves are always binding on relevant actors and are enforceable by courts or in general by government coercion (Kenneth S. Gallanth, The Principle of Legality in International and Comparative Criminal Law, Cambridge University Press, 2009, 7). For a description of the optimization thesis, see Robert Alexy, 'On the Structure of Legal Principles', Ratio Juris, vol. 13/3, 2000, 294-304, 295.

[36] See also par. 77 of the Explanatory Report specifying that "Data subjects should be entitled to know the reasoning underlying the processing of data, including the consequences of such a reasoning, which led to any resulting conclusions, in particular in cases involving the use of algorithms for automated- decision making including profiling".

[37] P. De Hert. & V. Papakonstantinou, 'The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition', Computer Law & Security Review, 2014, vol. 30/ 6, 633-642

[38] P. De Hert & V. Papakonstantinou, 'Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?', I/S A Journal of Law and Policy, 2013, vol. 9/2, 271-324; P. De Hert & V. Papakonstantinou, 'Moving Beyond the Special Rapporteur on Privacy with the Establishment of a New, Specialised United Nations Agency: Addressing the Deficit in Global Cooperation for the Protection of Data Privacy', in Dan Jerker Svantesson &

The title itself of the 2017 Big Data Guidelines is tacit acknowledgement that ours is indeed a world of Big Data. In other words, Big Data processing is a fact, a reality that cannot be ignored or denied. Indeed, the Guidelines introduce the topic by clarifying that Big Data "can be a source of significant value and innovation for society, enhancing productivity, public sector performance, and social participation".[50] They then set their scope at providing "general guidance, which may be complemented by further guidance and tailored best practices within specific fields of application of Big Data".[51]

The 2017 Big Data Guidelines have been issued within the context of Convention 108, and as such constitute a data protection soft law instrument. The approach is decidedly a data protection one, approximating the topic through the lens of data protection principles and offering solutions through the use of the data protection toolkit. In the light of our observations in the previous section, this means the application of an individual rights-based logic to a phenomenon that brings about bigger risks to groups. The Guidelines seem to be perfectly aware of this, and open with an astute characterisation of these bigger risks, to follow up with their stated purpose, viz. making the individual rights system of data protection more effective in the Big Data context – no less, no more.[528] In this vein, control is placed at their epicentre: Control as in a person's right to

---

Dariusz Kloza (eds.), Trans-Atlantic Data Privacy Relations as a Challenge for Democracy, Cambridge: Intersentia Pu Ltd, 2017, 521-533

[39] See the new Article 2 (d) and (f) of Convention 108+.

[40] Comp. 'Abandon the distinction between controllers and processors. Think in data processing chains. Treat every organization in that chain as a single controller, whose obligations depend on its role in the data processing chain. Do not hold parties at one end of the chain accountable/liable for the mistakes by parties at the other end of the chain to facilitate commerce" (Jeroen Terstegge, 'Do we need a new GDPR? While it is so outdated already', Netkwesties, 4 February 2020, https://www.netkwesties.nl/1421/3)

41 "Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law".

[42] See, for example, Betkier M, Privacy Online, Law and the Effective Regulation of Online Services, Intersentia, 2019, p.286.

[43] 'This Convention shall not apply to data processing carried out by an individual in the course of purely personal or household activities'.

[44] See the Explanatory Report to the Modernized Convention, Strasbourg, 10 October 2018, CETS 223.

[45] Comp. 'The primary purposes of why our personal data are created in those services is often covered by the personal and household use exception of the GDPR. This means that the GDPR will not stop us from uploading all these data and consequently will not stop the controllers from collecting it (except by terminating the service altogether). Everything the controllers do with our data, apart from providing the services, is therefore technically secondary use of our data. The GDPR will not cause, nor does it intend to end free online services" (Jeroen Terstegge, ibid). See equally on the challenge of the ubiquity of 'volunteered' data, particularly through the rise in wearable devices and social media networks, McDermott Y, 'Conceptualising the right to data protection in an era of Big Data', Big Data & Society January-June 2017: 1–7): " The rise in the so-called 'quantified self', or the self-tracking of biological, environmental, physical, or behavioral information through tracking devices, Internet-of-things devices, social network data and other means, may result in information being gathered not just about the individual user, but about people around them as well. Thus, a solely consent-based model does not entirely ensure the protection of one's data, especially when data collected for one purpose can be re- purposed for another").

[46] Explanatory Report to the Modernized Convention, §42: "An expression of consent does not waive the need to respect the basic principles for the protection of personal data set in Chapter II of the Convention and the proportionality of the processing, for instance, still has to be considered".

[47] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, 8 October 2019.

control his or her data when being processed in a Big Data context, but also control over the further uses of the data, after Big Data processing has been concluded. The preferred tool for the Council of Europe in this case is a "more complex process of multiple impact assessments of the risks related to the use of the data". In this manner the Council of Europe chooses to mix Big Data processing and Big Data further uses of the processing findings (see our introduction section above, under 1). While this may appear a confusing lack of distinction, the Council of Europe would have had no other way if it wished to provide a holistic regulatory approach on this topic.

Accordingly, the 2017 Big Data Guidelines "recommend measures those parties, controllers and processors should take to prevent the potential negative impact of the use of Big Data on human dignity, human rights, and fundamental individual and collective freedoms, in particular with regard to personal data protection". In other words, their aim is to mitigate the many risks of Big Data in a personal data protection context. Big Data is viewed as a potentially harmful for individual rights type of processing, and measures need to be applied each time so as to minimise risks. The approach is, in this way, defensive, treating personal data protection as

[48] Saint-Bonnet F, L'individu privé de royaume. Réflexions sur l'histoire de la vie privée, Tribonien. Revue critique de la législation de jurisprudence, 2018/1, pp.48-61; Rhoen M, Big data, Big risks, Big power shifts, Ridderprint, 2019, p.210; L. Taylor, L. Floridi & B. van der Sloot B. (eds), Group privacy. New challenges of data technologies, Philosophical Studies Series, vol 126, Springer, 2017, p.238

[49] Consultative Committee of The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, "Guidelines on artificial intelligence and data protection", on 25 January 2019.

[50] Council of Europe, 2017 Big Data Guidelines, p.1

[51] Ibid.

[52] "Big Data represent a new paradigm in the way in which information is collected, combined and analysed. Big Data - which benefit from the interplay with other technological environment such as internet of things and cloud computing - can be a source of significant (…). Not all data processed in a big data context concern personal data and human interaction but a large spectrum of it does, with a direct impact on individuals and their rights with regard to the processing of personal data. Furthermore, since Big Data makes it possible to collect and analyse large amounts of data to identify attitude patterns and predict behaviors of groups and communities, the collective dimension of the risks related to the use of data is also to be considered. This led the Committee (…) to draft these Guidelines, which provide a general framework for the Parties to apply appropriate policies and measures to make effective the principles and provisions of Convention 108 in the context of Big Data" (Council of Europe, 2017 Big Data Guidelines, p.1) (italics added).

[53] Council of Europe, 2017 Big Data Guidelines, p.1.

[54] See also Alessandro Mantelero, 'Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework' (2017) 33 Computer Law & Security Review 584.

[55] Council of Europe, 2017 Big Data Guidelines, p.1.

[56] Ibid

[57] See under Section I. ('General Guidance'), point 4: "In line with the guidance on risk assessment provided in the Guidelines on Big Data adopted by the Committee of Convention 108 in 2017, a wider view of the possible outcomes of data processing should be adopted. This view should consider not only human rights and fundamental freedoms but also the functioning of democracies and social and ethical values".

[58] See I.5 & I.6: "AI applications must at all times fully respect the rights of data subjects, in particular in light of article 9 of Convention 108+. AI applications should allow meaningful control by data subjects over the data processing and related effects on individuals and on society".

[59] To believe literature this is far from the case. See D.K. Citron, 'Technological due process'. Washington University Law Review, 2008, vol. 85, 1249-1313; H. Lammerant & P. De Hert, 'Predictive Profiling and its Legal Limits: Effectiveness Gone Forever?', Exploring the Boundaries of Big Data in van der Sloot, B., Broeders, D. & Schrijvers, E. (eds.)., Amsterdam University Press, 2016, (145-173), 165-166.

a checking point, an intervention for the safeguard of individuals. Other legal requirements of the Big Data processing per se (e.g., property rights over the data) are of no concern here.

The 2017 Big Data Guidelines take the Convention 108+ system for granted. At the time of their release, of course, Convention 108+ was not yet formally adopted. However, one should keep in mind that the CAHDATA Committee finished its work on Convention 108 in June 2016; The Committee of Ministers took two years to adopt its text, however there was ample time for the Guidelines to take the modernised text into account, as after all formally acknowledged in their text: "These Guidelines have been drafted on the basis of the principles of Convention 108, in the light of its on-going process of modernisation".[53]

On a practical level, [54]the Guidelines strive for specificity, suggesting "a specific application of the principles of Convention 108, to make them more effective in practice in the Big Data context".[55]In the same context, their purpose is to "spell out the applicable data protection principles and corresponding practices, with a view to limiting the risks for data subjects' rights". [56]This is achieved in Chapter IV, where the actual principles and guidelines are laid down.

The Guidelines begin with requiring an "ethical and socially aware use of data" (IV.1), which is an important opening statement per se, placing ethical and social considerations at the forefront of dealing with Big Data issues. While asserting that "personal data processing should not be in conflict with the ethical values commonly accepted in the relevant community or communities and should not prejudice societal interests", the Guidelines offer as concrete guidance the establishment of an ad hoc ethics committee to identify the ethical values and risks involved in Big Data personal data processing.

A "precautionary approach" is favored by the Guidelines (IV.2). Making the principles of legitimacy of the processing and quality of the data concrete onto Big Data circumstances, as well as, in accordance with the obligation to prevent or minimize its impact on the rights and freedoms of individuals, a 3-step risk assessment is recommended to identify and evaluate risks, develop and provide appropriate measures and monitor their adoption and effectiveness. The risk assessment is intended to be carried out preferably by experts in the respective field, and to actually constitute a participatory process involving all affected stakeholders.

The same risk assessment ought to comply with the requirements of free, specific, informed and unambiguous consent and the principles of purpose limitation, fairness and transparency of the processing; effectively, controllers should identify the potential impact on individuals of the different uses of data and inform individuals thereof (IV.3). In addition, the results of the risk assessment process should be made publicly available.

Once the risk assessment has been completed and publicized the Guidelines recommend that it constitutes the basis of the Big Data processing by the controller. In essence, on the basis of this assessment controllers should adopt adequate by-design solutions, taking in particular into consideration whether sensitive data are being processed (IV.4). Similarly, according to the same risk assessment findings consent may be enhanced with additional information provided or specially-designed interfaces to simulate the effects of the use of the data. Pseudonymisation or anonymization techniques, as appropriate, should also be considered (IV. 4 and IV.6 respectively).

As regards the stage of decision-making, the Guidelines prescribe that, notwithstanding anything to the contrary, the use of Big Data should preserve the autonomy of human intervention in the decision-making process (IV.7). In this context, decisions should not be merely de-contextualized information or data processing results, and, whenever decisions are likely to affect individuals significantly, human intervention is recommended (provided with enough power to deviate from the recommendations of the Big Data processing). At all times individuals adversely affected ought to be provided with the right to challenge the respective decisions before a competent authority.

The Guidelines conclude with two important practical recommendations: First, as regards open data, public and private entities are alerted as to the seriousness of their open data policies given that open data might be used in a Big Data context to extract inferences about individuals and groups (IV.8). Second, in order to help individuals, understand the implications of the use of their personal information in a Big Data context, digital literacy of the public should be considered an essential educational skill (IV.9).

The Council's decision to release the 2017 Big Data Guidelines means that the omission of Big Data in the text of Convention 108+ is deliberate: Essentially, it was the same committees working on both documents. In this, both the Council of Europe and the EU avoided top-level regulatory data protection intervention explicitly on Big Data. From their part, the Guidelines take note of the, then draft, text of Convention 108+, something that makes them, in this manner, soft law issued on the basis of Convention 108+ and not Convention 108. They ought therefore to be construed as still valid soft law emanating from the Council of Europe in the field of data protection for the regulation of Big Data processing. Their approach showcases the Council's will for such processing to indeed take place, but within a well-regulated environment, albeit not under a rigid regulatory construction.

7. The regulation of Big Data and the Council of Europe 2019 AI guidelines

Although the 2017 Big Data Guidelines explicitly targeted both Big Data and Big Data analytics, as seen above, and identified the process and consequences of algorithms, follow-up guidelines by the Council of

Europe saw the light in 2019, specifically addressing the data protection implications of artificial intelligence. The 2019 AI Guidelines are a much briefer document (only three pages-long) and do not seem to communicate well about their necessity. However, their release invites unavoidably the question about their relationship with the 2017 Big Data Guidelines.

Whatever might have been the precise intention behind drafting the 2019 AI Guidelines, it had been done in a powerful, straightforward way. Their first page starts with a 'should' message of looking beyond an individual rights and interest perspective,[57] and then continues with a 'must' message, viz. AI 'must' respect data subject rights and 'must' allow meaningful control.[58] The two remaining pages provide a set of baseline measures that AI developers, manufacturers, and service providers (Section II with 12 guidance rules) and governments and policy makers (Section III with 9 guidance rules) should follow to ensure that AI applications do not undermine the human dignity and the human rights and fundamental freedoms of every individual, in particular with regard to the right to data protection. Amongst the novelties of the 2019 AI Guidelines are the recommendations that developers, manufacturers, and providers run on a permanent basis DPIA's (as per the GDPR) but also as well Social and Ethical impact assessments; Those controllers should apply technical measures to assist individuals (notification buttons, online consent forms etc.); And that by-design solutions, such as simulations of processing before running on a large scale, ought to be applied. Equally important (and more explicitly compared to the GDPR), are their recommendations to make impact assessments and all other relevant information available on the internet for everyone to see and to encourage 'participatory forms of risk assessment' (II.7).

Particularly Section II of the 2019 AI Guidelines succeeds in bridging between the 'must' (must comply with the individual rights based Convention108+) and the 'should' (should protect broader interest). Instrumental in this respect is the use of broader buzz-words in the recommendations addressed to developers, manufacturers and service providers 'to adopt a values-oriented approach in the design' (II.1), 'to adopt a precautionary approach' (II.2), 'to adopt in all phases a human rights by-design approach' (II.3), and 'to adopt forms of algorithm vigilance throughout the entire life cycle of these applications" (II.10). This rainfall of jargon is complemented with very concrete instructions (that show expert understanding of AI) about test or training data used in AI (II.4).

Section III, with guidance to policy makers and governments, is less innovative and less granular (apart from the recommendation to amend public procurement procedures to have some grip on state use of AI (III.2)). What it does for most of its part is mandating governments and policy makers to make sure the broad recommendations to developers, manufacturers and service providers discussed above are implemented and that enforcement is effective.

It is best to read the 2017 Big Data and 2019 AI Guidelines as a whole adding more fresh insights on Big Data analytics to the Big Data insights formulated in 2017. The central message of both Guidelines is that basic data protection principles and Big Data processing can exist in a symbiosis, if the controllers take the responsibility on their shoulders and at the same time follow the steps prescribed in Article 10 of Convention 108+, essentially building data protection in the early stages of the design of the processing: The controller should carry out an initial risk assessment; This should be followed up with a proper risk management policy and concrete efforts to minimize the risks; And, the controller should carry out a data protection impact assessment, if it is likely that the processing will affect the rights and fundamental freedoms of data subjects.

The option in both Guidelines to formulate specific guidance to categories such as developers and governments is remarkably effective. In this way the Council of Europe adopts more specific solutions for Big Data than the GDPR and the EU. The former takes full benefit here from its position as a body of international law that mainly addresses its legal output to 'Member States' that have to follow up in domestic law. The EU does everything but this. In fact, it has opted for a Regulation to bypass the domestic regulators. The GDPR is binding European law in no need of implementation, at least at the formal legal level. The downsides of 'more Europe' and 'more internal market harmonisation' are evident: An important actor in our human rights system, the state, is left out the legal equation. It therefore feels reassuring to find a list of 'to-dos' addressed to state authorities in the Council of Europe documents. In this way states undertake the role to protect individuals from AI and Big Data risks. Human rights protection is more than just guaranteeing enforcement by providing resources to administrative enforcement bodies. States should not only 'enforce the GDPR' but take the lead in making the Big Data and the AI world human. In this context, a small recommendation by the Council of Europe to improve public procurement procedures is in fact a loud reminder of the old wisdom that governments should teach by example. [59]

8. Conclusion

Because a great number of the member states of the Council of Europe are at the same time EU Member States, a careful act of legal balancing is necessary at all times. The main concern in this case is for the same country not to be brought to the impossible position of having to choose which legal system to break; In order to accomplish this, particularly in these fields where legal powers entrusted to the Council of Europe and the EU are concurrent, great care is taken that legal obligations are not contradictory, or even competing. Most pertinently, this is the case in the field of personal data protection: Because both the Council of Europe and the EU have long established by now personal data protection legal systems, great care has been given so as for their main rule-setting instruments, Convention 108+ and the GDPR respectively, to be compatible. This is evidenced, above all else, in the long time that lapsed between technical finalisation and final formal adoption of Convention 108+ within the Council of Europe.

However, compatibility does not necessarily mean stifling of initiative. Neither does it mean that the more detailed document (in this case, the GDPR) applies at the expense of the more general one (in this case, Convention 108+). In fact, quite the contrary is true: For decades, the Council of Europe's immeasurable contribution to personal data protection in Europe was regulation also of security-related personal data processing. On top of that, the international influence of Convention 108 has been far more prevalent than that of the EU Data Protection Directive of 1995 (as evidenced by number of ratifications of the former if compared to countries having acquired "adequate" status as per the EU data protection system requirements). These traits are not expected to retreat under the new regulatory environment, posed by Convention108+ and the GDPR respectively: The Council of Europe's personal data protection mechanism has dared to dwell into territory avoided until now by its EU equivalent, as after all evidenced by the 2017 Guidelines on Big Data that formulate the basis of this paper. In addition, the rate of ratifications by non-European countries of Convention 108+ has continued with the same, if not increased, pace as in the past.

Given that the basic texts of reference, Convention 108+ and the GDPR, are compatible, the Council of Europe's Guidelines on Big Data and AI may be directly used by EU Member States. Complementarity is thus achieved, further strengthened by the lack of any similar guidance to the same countries from the EU personal data protection mechanism. The approach and the solutions provided in both Guidelines are, to the authors' opinion at least, compatible with the GDPR system, and therefore Member States in the EU can apply them reassured that they do not breach any other (EU) personal data protection obligations. As such, in the sense of the only data protection soft law on Big Data available today at a supranational level in Europe, the Guidelines' contribution is already important.

The choice of instrument is also deemed successful: Soft law in the place of hard, formal legal provisions. As seen, both the EU and the Council of Europe have avoided to refer to Big Data in their basic data protection regulatory texts. Given the prevalence of the term at the time these were drafted, this must have been an intentional omission. However, guidance is indeed needed, and it may well come in the form of soft law. The Council of Europe has taken the lead in this – and, given the complementarity factor discussed above, the EU has no practical reason to become engaged and also issue guidance on the same topic at least in the near future.

A basic advantage of a soft law instrument is that it can be easily amended – or withdrawn, for the same purposes, if deemed no longer relevant. To our mind this may well be the case in the near future as regards Big Data. The term has receded from the spotlight, being replaced by other technology marketing catchwords. In addition, ever-increasing processing capabilities mean that what was perceived as "Big" then years ago, when the term was coined, is routine and mainstream today. Things are expected to continue in the same manner. Consequently, it may well be the case that at the time of drafting this paper, in early 2020, its title

may already be (or fast becoming) obsolete: One cannot but wonder whether Big Data, five years after its peak in global interest, has not become simply "Data" by now. The Council of Europe did well to spot the wave and ride it in a timely manner since the release of its 2017 Guidelines: It only remains to be seen for how much longer, and in which exactly format and content, their valuable contribution will remain timely and relevant.