Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks

Savin, Andrej

Document Version
Final published version

Publication date:
2014

Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks

Andrej Savin*

Introduction

The digital world of the 21st century is increasingly the world of automatic decision making. In such a world, an ever larger number of tasks are relegated to computers which gather and process data as well as suggest or make decisions silently and with little supervision. This situation has been made possible by a transfer of a staggering portion of our daily lives from the offline world to the Internet. It is a truism that automation would be impossible without our willing participation on the Internet. We freely take part in social networks, post on blogs, and send our emails. On the other hand, it is equally true that we are increasingly monitored by the state, by profit-maximizing corporations and by our fellow citizens and that these methods of monitoring are becoming smarter. Vast amounts of data which have become available and which we contribute, form what we today call "big data".[1] This is then harvested for connections and correlations and profiles created that can be used for commercial and other purposes. We fear this world but are also dependant on it. The creation of these profiles and their usage is an uncharted territory for the social sciences as much as it is a strange territory for the regulators.

Although often labelled "profiling", there are at least separate phenomena which are frequently but erroneously used concurrently. Profiling generally means extrapolation of information on the Internet by the process of computer-generated information gathering and subsequent construction and application of profiles.[2] Automated decision making, on the other hand, is the general ability to make decisions based on the generated profiles but without human actors . The difference lies in the fact that automated decision making is the process of reaching a decision (business, administrative, baking, etc.) based on the already created profile. In other words, a large collection of data is used as a source for creating a profile which is then put to use and on the basis of which a decision is made. Decisions can, however, also be made by humans on the basis of the very same profiles that machines use. Smart surveillance,[3] on the other hand, normally refers to a sub-set of automated

* Associate Professor, Copenhagen Business School

[1] Data of very large size and complexity that cannot be manipulated with usual database management tools. For an overview see Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (London: John Murray, 2013)

[2] On the complexities of profiling in the EU see Mireille Hildebrandt and Serge Gutwirth (editors). *Profiling the European Citizen* (Springer, 2008)

[3] Smart surveillance, which is only indirectly dealt with in this paper, is currently a subject of comprehensive studies funded through EU Seventh Framework Programme. While the SMART Project is a broad study of automated recognition technologies in the EU, the

decision making where individuals, companies and states use surveillance technologies (such as CCTVs, social networks, RFID and geo-tagging information, financial data) to gather information, create profiles and make decision based on them.

Profiling has been recognized as a problem in the Article 29 Data Protection Working Party (Article 29 WP).[4] A definition was proposed saying that profiling

> *means any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person's health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movements.*

Three important points will be apparent from the aforesaid. The first is that profiling (gathering of data and forming profiles based on this data) has the potential to be harmful even if no decisions are made on the basis of profiles. This is because the potential of this data to be harvested for information and its commercial value. Second, automated decision making is a much wider term than smart surveillance. A database of banking data may serve as a basis for decision on the customers' credit rating without any surveillance techniques being employed. Third, *smart* surveillance or smart decision making may be particularly sensitive due to data subject's lack of awareness that data are collected and used.[5]

Both automated decision making in general and smart surveillance as one of its aspects introduce a level of convenience and a level of risk. Both are useful and dangerous at the same time. Both are controversial. In 2014, both are ubiquitous. The risk has two faces. One is primarily economic – a subject fearful of monitoring will not easily share information and will not avail itself of information society services. The second is social and it has to do with our feeling that being monitored is morally and socially wrong. The public is aware of the potential negative sides with the European Barometer 2011 study demonstrating that 74% of Europeans desire the ability to give or refuse consent before collection or processing for online profiling purposes.[6]

RESPECT Project looks at convenient and cost-effective surveillance. Scalable Measures for Automated Recognition Technologies (SMART), Project No. 261727, 2011-2014. Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies (RESPECT), Project No. 285582, 2012-2105.

[4] Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, adopted on 13 May 2013

[5] Although the assumption that other data are less harmful simply because the subject had in one form or another "consented" to their use is questionable. For more details on the meaning and effect of consent online see EU FP7 project Consumer sentiment regarding privacy on user generated content services in the digital economy (CONSENT), Project No. 244643, 2010-2013

[6] European Commission, Special Eurobarometer 359, "Attitudes on Data Protection and Electronic Identity in the European Union", June 2011, pp. 74-75, available at http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

The purpose of this paper is to give a short overview of the present EU legal framework for automated decision making and to provide a brief analysis of the current proposals for reform. In the first part , we will look at the Data Protection Directive[7] and the Council of Europe Recommendation on Profiling.[8] In the second part, we will analyse the proposed General Data Protection Regulation.[9] In the final part, we will propose some general directions for the lawmakers.

Data Protection Directive

The Data Protection Directive is the general instrument on privacy protection in the EU. It applies to collection of personal data except data concerning legal persons, data for purely personal purposes or public or national security and defence. Its basic premise is that data can be collected and processed if one of the prerequisites in Article 7 has been fulfilled. The main but not the only one is data subject's consent. The others refer to situation where data processing is necessary.

There is little doubt that data protection rules apply to creation of profiles in any situation where data used is *personal* data. There seems to be compelling evidence that they also apply in cases where data is anonymized, i.e. where data previously gathered about an identified or identifiable person had the identifying information removed.[10] This is because Article 2(b) emphasises that processing includes "erasure or destruction" of information.

The first relevant provision of the Directive refers to right of access to information. Among other things, it provides that data subjects shall have the right to obtain "knowledge of the logic involved in any automatic processing of data." Special emphasis is put on automated decisions referred to in Article 15 (1) (see below) which should be interpreted as meaning that data subjects always have the right to know the logic but this needs to be explained to them *in particular* in cases where there is automated decision making involved.

---

[7] Directive 95/46/EC of the European Parliament and 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, OJ L 281, 23.11.1995. d

[8] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23 November 2010

[9] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25.1.2011.

[10] See Wim Schreurs, "Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector" in *Profiling the European Citizen*, (ed.) Mireille Hildebrandt and Serge Gutwirth (Springer, 2008), p. 249

The key provision dealing with automated data processing is Article 15, entitled "Automated Individual Decisions". The first paragraph of the Article grants the right of every person not to be subject to a decision "which produces legal effect" or "significantly affects" and which is "based solely on automated processing of data". The paragraph specifically mentions that data needs to be intended to "evaluate" personal aspects and, by way of an example mentions performance at work, creditworthiness, reliability and conduct but leaves the list open.

Article 15(1) applies, therefore, only to situations which produce significant *or* legal effect (the assumption being that legal effect is by default of some significance). An automated decision by a bank not to grant credit falls under the provision as it produces significant (although usually not legal) effect. A decision by a local council to classify a property as falling under a particular tax regime falls under the provision due to its legal effect. A decision by a local sports club's computer system that a member is more likely to be interested in football than basketball and should, therefore, receive updates about the former produces neither legal nor significant effects.

If the *intention* is not to evaluate personal aspects, the article does not apply. The key to application of the article is the intention understood as the data processor's awareness of and desire to analyse personal information. If personal information analysis is not the intended but ancillary effect, the article would not apply. An example could be found in a number of situations where surveillance of public spaces (real or virtual) attempts to find patterns of public behaviour but gathers personal information (photos, addressed, etc.) in the course of that activity. A local council system monitoring whether public parking spaces are full could gather registration numbers in the process and forward them to other departments which may be in the position of making a decision (e.g. issue parking fines). This is not an ideal solution. It is submitted here that intention should not form part of the provision. The individual should be able to object to automatic decision making based on personal data whether the data controller's intention had originally been to analyse such data or not.

Article 15(1) does not demand consent in the meaning of Article 7. The data originally obtained may have been so on the basis of data subject's consent or any of the other bases. The obligation imposed is only to grant the right to prevent *automatic decisions* being made on the basis of data otherwise legitimately obtained. The original consent, if required, would therefore still be valid for the ordinary data processing that does not involve automated decisions. If data were originally obtained by consent, for instance because a user agreed to terms and conditions on a website, withdrawal of the consent automatically delegitimizes the data.

In derogation to the first paragraph, automated decisions may, according to Article 15(2) be taken in the course of the entering into or performance of a contract. The condition in both situations is that data controller can produce a log demonstrating that the data subject had himself initiated the contract or,

in the alternative, that "*there are suitable measures to safeguard his legitimate interests"*. By way of example for the latter, "*arrangements allowing him to put his point of view*" have been quoted. Whereas the first option is there simply to ensure that a subject, who willingly enters into a contract and transfers in the process some private information, must then expect that such information will be used, the choice of the second condition here is puzzling. It would seem that it means that data subjects can voice their objections *prior* to any decision being made.

The second derogation exists in cases authorized by law, provided that such laws "safeguard the data subject's legitimate interests."

A difference has been made above between profiling and decision-making. Profiling, it will be recollected involves a computer-assisted search for patterns that help arrive at conjectures which, in turn, help form profiles. Decision making, on the other hand, involves making choices/conclusions based on profiles. Article 15 of the Directive in its present form applies to "a decision". In other words, it applies to profile *application* – not profile *making*. Whereas original drafts of the Directive had the same solution, original proposal for Directive on telecommunications privacy[11] had not.[12] Article 4(2) of that proposal (though not of the final Directive) specifically provides that "the telecommunications organization shall not use such data to set up electronic profiles of the subscribers or classifications of individual subscribers by category."

The result of this position is that profile *creation* is, by default, allowed but that persons who are unhappy with the profile being used for *automated* decision making may object according to Article 15. There are several reasons why this situation is not ideal. The first is that profiles, which play an increasingly important commercial role and are treated as commodities by modern companies, contain a significant potential for privacy violation irrespective of whose hands they are in. Data mining (computer-aided extraction of useful information from the Internet) and data aggregation (combining data from several sources) can constantly improve profiles and increase their commercial value. An example can be found in common social networking sites. A public profile (i.e. a profile being displayed to a general public and not just to "friends") is available to anyone who browses on a social network. The same profile can easily be connected to other social networking sites (containing photos, blog posts, etc). In fact, users themselves often volunteer this information. Contractual consent has, presumably, been obtained from the original poster for each of the sites used. It is not clear in the present regime whether such consent extends to profiles created by aggregation information obtained in the previous ones. If a hypothetical

[11] Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the Integrated Services Digital Network (ISDN) and public digital mobile networks (COM(90) 314 final — SYN 288, 13.9.1990)

[12] Lee Bygrave, "Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling", *Computer Law and Security Reporter* 7 (2000) 67-76

aggregator obtains such information by means of automatic computerized search and then displays it, the original contractual consent for each of the sites would not seem to cover the aggregator. Such aggregator would inevitably be both the processor and the controller within the meaning of Article 2 of the Directive. Furthermore, pursuant to Article 6 of the Directive, personal data can only be processed in a fair and lawful way and for specified, explicit and legitimate purposes. It can reasonably be assumed that an aggregator/profiler which gathers data in this way will fall foul of some of the criteria of "purpose limitation" in Article 6.

It is also necessary to add here that data processed in police and judicial matters fall under a separate regime.[13] The 2008 Framework Decision prohibits automated individual decisions in the manner similar to Directive. It is only allowed if authorised by a law which also lays down safeguard measures.

Council of Europe Recommendation on Profiling

The Council of Europe Recommendation on Profiling provides a significantly more detailed regulatory solution for profiling than the Data Protection Directive. The Recommendation, the first international attempt at regulating profiling, is meant as an application of data protection principles from Convention 108 to profiling.[14] It does not have a binding effect but can be considered soft law directed at all states which have adopted Convention 108.

The preamble to the Recommendation lists a number of reasons for its adoption. Nevertheless, a closer look demonstrates that the authors' primary worries were the following. First, profiles, when they are attributed to a data subject, make it possible to generate *new* personal data which are not those which the data subject has communicated to the controller or which can be presumed to be known to the controller. This is a justified fear, especially in light of the increasing data aggregation practices the sole purpose of which is to augment the value of the communicated data by way of connecting it to other data. The second prominent worry is the lack of knowledge that the individual is being profiled, the lack of transparency and the lack of accuracy. This fear is also justified as the user often has little or no control over what happens to data after he gives consent to its processing. The subsequent profiling may, therefore, continue without his knowledge and the original data may be degraded as they are combined with older or less accurate data or even data relating to a completely different individual. The final worry relates to children whose profiling may have serious consequences for their

[13] 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, OJ L 350, 30.12.2008, page 60

[14] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981

subsequent lives. Since children are not in the position to give consent, special protection measures need to be applied.

The Recommendation does make the important distinction between profile *generation* and profile *application*. Article 1(d) defines a "profile" as a set of data characterising an individual which is meant for "applying" to an individual. Furthermore, in Article 1(e) "profiling" is defined as applying the profile to an individual. The choice of words is somewhat unfortunate as profiling is often understood elsewhere as only the process of gathering information not the process of applying it. Elsewhere in the text, however, the recommendation does not have two different *regimes* for profile collection and profile application.

Section 3 contains detailed conditions for collection. Article 3.1 provides that collection and processing must be "fair, lawful and proportionate" and that it must be for "specific and legitimate" purposes. The requirement that purposes should be specific is unrealistic. Modern profiles are often collected without specific purpose in mind or the purpose may become apparent at a later stage. Facebook "like" button, for example, was originally introduces without commercial purposes but these have subsequently been experimented with. Condition 3.2 demands that profiling be "adequate, relevant and not excessive" in relation to the purposes.

Collection and processing can be allowed in two situations only. The first (Article 3.4.a) is where they are *provided* for by law. This should be interpreted to mean where they are *demanded* by law, i.e. where a specific provision calls for profiling. In this case, no further conditions need be fulfilled. This will often be the case in laws involving administrative situations (ID cards and numbers, passports, insurance, police records, etc.) The second situation (Article 3.4.b) is where they are *permitted* by law and one of the five preconditions are met. The words *permitted* should here understood to mean that the purpose for the collection must not be illegal according to local law.

The first precondition for permitted collection and processing is a "free, specific and informed consent". This is a big advance over the solution currently given in Article 15 of the Data Protection Directive. The Recommendation demands a consent that specifically relates to profiling – a general consent given in the context of the ordinary data processing is not sufficient. Moreover, the consent must be "informed", meaning that data subject must be aware that data will be used for profiling and not for other purposes, however legitimate they may be. The second precondition covers performance of a contract and implementation of precontractual measures taken at data subject's request. An example can be found in any web store account used today. The third precondition relates to tasks carried out "in the public interest" or "in the exercise of official authority". The authority may be vested either in the controller or in a third party. The fourth precondition exists where the controller's or the third party's legitimate interests demand profiling. This can be overridden in the situation where data subject's own fundamental rights are at stake. The final precondition exists where the "vital

interests if the data subject" demand it. Profiling of persons incapable of demonstrating their own free consent is allowed only when protecting their own interest (Article 3.5).

The Recommendation shows acute awareness of one of the most common sources of profiling today – commercial profiling. In Article 3.7 it demands that "as much as possible", it should be able to access information about goods and services or access goods or services themselves without disclosing personal information, The article demands that providers of information society services (and this includes strictly commercial but also non-commercial or hybrid websites) should provide by default non-profiled access to their information. Sensitive data are the subject of a separate entry in Section C (Article 3.11). The default position here is the prohibition of profiling except where necessary for the "lawful and specific purposes" in the presence of adequate domestic safeguards.

In the course of profiling, the controller must provide the subject with a number of predetermined pieces of information (Article 4.1). When data is collected directly from the subject (and not transferred from a third party), this information needs to be given at the time of collection at the latest. The subjects need to be told that data will be used for profiling and need to know the purpose of profiling and the categories of personal data. The identity of the controller must be disclosed as well as the fact that safeguards exist.

A separate category (4.1.f) is designed to demonstrate the fairness of profiling to the subject. The subsequent list is given as a way of example. This includes the persons to whom data may be communicated, the possibility to refuse to give consent or to withdraw it subsequently, the right to object to or demand correction and others.

Of particular interest here is the "envisaged effects of the attribution of the profile to the data subject" which means that the data subject needs to learn not only about the fact that profiles are created about him or her but also the possible implications of these profiles being applied.

The fact that data is not collected from the data subject but obtained from the third party (by way of purchase, for example) does not exonerate the controller from providing the information to the data subject at the time of transfer (i.e. when the controller receives the data). It is interesting to note that Article 4.4 is aware that data is often not collected for the purposes of profiling but only become its subject later. The obligation to inform arising out of Article 4.1 is then extended to such a situation.

Data subjects have the right, according to Article 5.1 to learn not only about the fact that they are being profiled but also the logic underlying the profiling. They are entitled to correction, deletion or blocking only in the cases where profiling is performed contrary to domestic law. The right to correction, deletion or blocking does not exist purely because the data subject had changed its mind about the profiling. A separate right of objection is inserted

in Article 5.3 which entitles the data subject to complain on "compelling legitimate grounds".

Regulation Proposal

The current data protection regime is almost 20 years old. A need for reform was recognized and a new proposal saw light in 2012. The new Regulation is meant as a shift from bureaucratic requirements to compliance in practice.[15]

The Regulation has a significantly more coherent protection of profiling. Recital 24 recognizes the danger of online identifiers such as cookies or IP numbers which their "devices, applications, tools and protocols" may leave behind. This, combined with unique identifiers and other information may lead to profile creation. The Commission concludes, however, that identification numbers, location data, online identifiers or other specific factors are not personal data as such. It is puzzling why this conclusion had been reached as this data is not anonymous by default. On the contrary, IP numbers and cookies are by default connected to particular machines which are , more often than not, accessed by particular users. Amendment 15 of the Albrecht Report (see below, note 25) changes the text, saying that the default position is Regulation application "unless those identifiers demonstrably do no relate to natural persons", giving as a way of example company IP addresses.

The main provision on profiling, Article 20, is entitled "Measures based on profiling". This may suggest that the article is only regulating *decision making* based on profiles and not the actual profile creation. The word "decision", however, prominently featuring in Article 15 of the Directive has been removed. This has to be interpreted to mean that the new regime applies to profile *creation* as well as to *decision making*, automatic or other, resulting from the application of the profile to an individual.[16] Another difference from the Directive is that "natural person" replaces the "data subject". This is a significant change. In the Directive Article 2, a "data subject" is "an identified or identifiable natural person". The fact that Regulation would apply to natural person means that profiling is covered in the Regulation, in principle at least, irrespective of whether the data is anonymized or not.

Recital 58 outlines the bases for lawful profiling. Such measure should be allowed when expressly authorised by law (and proper safeguards exist), when it is carried out in the course of entering or performance of a contract, or when the data subject has given his consent. These requirements are

[15] See Christopher Kuner. "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law". *Privacy & Security Law Report*, 11 (2012): 6

[16] See Mathias Vermeulen, . "Regulating Profiling in the European Data Protection Regulation: An Interim Insight into the Drafting of Article 20". EMSOC Working Paper. Available at SSRN: http://ssrn.com/abstract=2382787 or http://dx.doi.org/10.2139/ssrn.2382787 accessed 28.2.2014.

repeated in Article 4(8) of the main body of the Regulation (as is also the case in Recommendation).

Article 20 applies to measures which produce legal effect or which "significantly affect" natural persons. The measures must be "based solely on automated processing" and "intended to evaluate certain personal aspects". This part is worded in the same manner as the Directive. The first addition is that the measure may also be intended "to analyse or predict" various factors. This is a small but important clarification of how profiles may be applied. By way of example, performance at work, economic situation, location, health, personal preferences, reliability and behaviour are quoted. It will be recollected that the Directive only provided three examples: performance at work, creditworthiness, reliability and conduct.

Paragraph 2 allows profiling in the course of conclusion or performance of a contract, where it is expressly authorized either by EU or national law or is based on consent. The latter provision points to new Article 7 which is an updated and more precise definition of consent. That article demands that the controller bears the burden of proof. Paragraph 2 furthermore demands that consent which is in a written declaration containing other matters (e.g. 'terms of use') be distinguishable. Consent can be withdrawn, which has the effect of making processing unlawful from the moment of withdrawal but not before. Consent is not a valid basis where there is an imbalance between the data subject and the data controller.

Article 4(8) of the proposal defines consent as "freely given specific, informed and explicit indication". This indication can be given by a statement or affirmative action. Article 4(8) is an improvement on the situation in the Directive. FP7 CONSENT project, looking into consent and privacy on user-generated websites, demonstrated[17] that users often give consent lightly, without properly understanding its implications. The most common situation is where an individual is presented with lengthy 'privacy policy' or 'terms and conditions'. The users are unlikely to read those due to their length or the fact that they change frequently. Even popular sites like Facebook, which have simplified both their privacy policies and terms of use, prove complicated. Facebook "Data use policy"[18] lists six different headings. Among these are titles "Information we receive and how it is used", "Other websites and applications" and "Cookies, pixels and other similar technologies" all of which relate to profiling to larger or smaller effect. In addition to this, there exists a separate "Privacy Page",[19] "Safety Page"[20] and "Minors and Safety" page. All of this is in addition to what the site calls "Complete Data Use Policy".[21] It is submitted that an average user is not capable of making an informed decision

[17] CONSENT Project, see footnote 5. In particular work packages 3 (privacy polices) and 7 and 8 (quantitative and qualitative analysis).
[18] https://www.facebook.com/about/privacy/ accessed 28.2.2014.
[19] https://www.facebook.com/fbprivacy
[20] https://www.facebook.com/safety
[21] https://www.facebook.com/full_data_use_policy

about profiling in the situation described here. Similar conditions are found on other websites.

In light of the foregoing, Article 4(8) is a step forward. The consent required there, coupled with the clarification of Article 20 can be interpreted to mean that consent regarding profiling and automated data processing needs to be obtained separately. Nevertheless, it would have been better had the solution in the Recommendation been adopted where consent is specifically related to profiling.[22]

An important addition to the old regime is paragraph 3, which says that decisions cannot be made solely on Article 9. This article deals with special categories of data (racial, ethnic, political, religious, trade union-related and others). If a commercial entity engages in, for example, racial profiling, assigning their clients into groups based on racial criteria would be illegal.

Reaction, Albrecht Report and Proposed Amendments

The business communities reacted aversely to the proposal believing that extra burden is being placed on them.[23] In particular they objected to potential requirement to consent to cookies, the potential to apply the proposed Regulation to behavioural advertising and to consent as a basis in general.[24] They emphasized that comprehensive and wide-ranging clause would not be risk-based and would unduly restrict a number of useful practices. Some of the criticism is directed at the individualized/anonymized dichotomy which the Regulation operates on but which does not necessarily coincide with the reality.

The Opinion of the Committee on Industry, Research and Energy[25] proposes through Amendment 182 a new industry friendly solution which would apply to "advertising, market research or tailoring telemedia". In such cases, user profiles can be created using pseudonymised data, in cases where the person concerned does not object. To make sure that problems do not arise, the amendment suggest that user profiles may not be combined with data about the bearer of the pseudonym.

Article 29 WP, consisting from EU data protection authorities, suggested, contrary to the industry views summarized above, that the Regulation could do more to protect individuals against profiling. It objected to the fact that stronger differentiation had not been made between the collection of data for

[22] See Article 3.6
[23] UK House of Commons Justice Committee, The Committee's opinion on the European Data Protection Framework proposals. Volume II, Additional Written Evidence, September 2012. Written evidence from the Advertising Association, Ev w28. 13.1 – 13.2.
[24] See Mathias Vermeulen, op. cit. p. 11-12
[25] 26.2.2013. COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

the purposes of profiling on one hand and the creation of profiles as such.[26] The Working Party suggested that provisions ensuring greater transparency and control for data subjects be introduced.

In a somewhat similar line but producing a more detailed revision, the main rapporteur for the Regulation, Jan Albrecht, proposed significant amendments that change the picture of the Proposal.[27]

In respect of controllers not established in the Union, the Regulation proposes its application in Article 3 to such controllers where they offer goods or services to data subjects in the EU or where they monitor their behaviour. Albrecht Amendment 83 recommends that monitoring of *behaviour* be replaced with monitoring of data *subjects*. This is widening of the scope of the Regulation's application as monitoring of subjects may not simultaneously be monitoring of their behaviour.[28] A data subject becomes, in Amendment 84, a person who can be singled out alone or "in combination with associated data."

The Albrecht Report changes the article structurally, moving definition to Article 4 (Amendment 87) and information requirements to Article 14 (Amendments 130-132). It streamlines and tightens the requirements for lawful profiling. The title is changed from "Measures based on profiling" to "Profiling" signifying that the regime applies to profile *generation* as well as to *decision making* based on profiles. It adds a new and significant paragraph 2(a) which says that:

> *Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited.*

The Albrecht Report has as a basis four important principles. The first is that monitoring of data in the sense of Article 3 (as amended) would take place depending on how comprehensive the tracing efforts were.[29] Offline use or sporadic aggregation would not be considered monitoring. Second, protection would apply to information concerning an identified or identifiable person.[30] If data cannot be related in any way to such a person, the Regulation would not apply. Third, processing relating to identifiers which leave traces should be covered by Regulation.[31] Fourth, consent is only valid where the choice made is genuinely free and valid.[32]

---

[26] See note 4 above, p. 3

[27] Jan Albrecht, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM (2012)0011 – C7 - 0025/2012 – 2012/0011 (COD)). European Parliament, Committee on civil liberties, justice and home affairs. 17 December 2012.

[28] For example, ID numbers, photos and voice samples are normally not behaviour-related

[29] Item 21

[30] Item 23

[31] Item 24

[32] Item 33

It is worth adding here that the Report created a category of "pseudonymous data." This category, introduced in Amendment 105 which modifies Article 7 on consent by adding a new paragraph – 2a, is subject to less strict treatment. The article provides that data which is processed only in the form of pseudonyms allows consent "by automated means using a technical standard with general validity in the Union."

Concluding Remarks

While a reader may quickly agree with the idea that profiling and automated decision making are widespread and important, it is more difficult to reach generalized conclusions concerning any future direction in which law should move. Whereas it may be tempting to look at the situation in black or white, depending on whether one stands on the industry or the user side, we believe the reality to be somewhat more complex. Three general conclusion may nevertheless be drawn:

First, while the existence of protection in the present regime is positive, it is equally true that current laws are in need of change. The present regime has simply become too dated for the modern realities of big data, data mining, data aggregation, profiling and automated decision making. On the other hand, future profiling and automated decision need to be regulated carefully. National data protection authorities (represented in Article 29 WP) have sometimes radically different solutions than those offered by the industry or the Commission. It is a misapprehension to believe that these differences can be overcome without a constructive political dialogue or by strong-arm tactics. In that sense, the Council of Europe Recommendation should be a welcome and useful instrument for the European lawmakers.

Second, there is no doubt that regulatory models in Europe and in the United States are different. The United States have traditionally been more "parsimonious" while the EU has been more proactive.[33] It is illusory, however, to believe that solutions which are more widely accepted by the industry while granting significant individual rights can be achieved without a long-lasting and effective transatlantic dialogue.

Third, data mining and big data have led to creation of an information environment that brings many advantages to modern users. Ignoring these advantages is dangerous. At the same time it brings the risk of invasion and discrimination. Ignoring these is equally dangerous. Having this ambiguity in mind, Custers and others have suggested that *a priori* limiting measures such as access controls, anonymity and purpose specification are increasingly failing in the fight against privacy violation and discrimination and argued for a focus on *a posteriori* accountability and transparency.[34] While these ideas are yet to be tested, it is possible to say that lawmaking alone will not give the

[33] See Schwartz., Paul. M. "The E.U.-U.S. Privacy Collision: A Turn to Institutions and Procedures" 126 (2013) Harvard Law Review 1966

[34] Bart Custers, et al. (eds.) *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases* (Berlin: Springer, 2013), p. 342

answer and that traditional lawmaking, in particular, may have to be complemented by modern and less traditional approaches.

Bibliography

Jan Albrecht, *Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (COM (2012)0011 – C7 - 0025/2012 – 2012/0011 (COD)). European Parliament, Committee on civil liberties, justice and home affairs. 17 December 2012.

Bygrave, Lee. "Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling", *Computer Law and Security Reporter* 7 (2000) 67-76

Bart Custers, Toon Calders, Bart Schermer and Tal Zarsky (editors) *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases* (Berlin: Springer, 2013)

Hildebrandt, Mireille and Gutwirth, Serge (editors). *Profiling the European Citizen*. Springer, 2008

Richard Jones, Dalal Tahri."An overview of EU data protection rules on use of data collected online". *Computer Law & Security Review.* 27 (2011) 630–636

Kuner, Christopher. "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law". *Privacy & Security Law Report*, 11 (2012): 6

Schermer, Bart. "The limits of privacy in automated profiling and data mining" 27 (2011) Computer Law & Security Report 45-52

Mayer-Schonberger, Viktor and Cukier, Kenneth. *Big Data: A Revolution That Will Transform How We Live, Work and Think*. London: John Murray, 2013

Schreurs, Wim. "Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector" in *Profiling the European Citizen*, edited by Mireille Hildebrandt and Serge Gutwirth. (Berlin: Springer, 2008)

Schwartz., Paul. M. "EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation". *Privacy & Security Law Report*, 12 (2013): 718

Schwartz., Paul. M. "The E.U.-U.S. Privacy Collision: A Turn to Institutions and Procedures" 126 (2013) *Harvard Law Review* 1966

Vermeulen, Mathias. "Regulating Profiling in the European Data Protection Regulation: An Interim Insight into the Drafting of Article 20". *EMSOC Working Paper*. Available at SSRN: http://ssrn.com/abstract=2382787 or http://dx.doi.org/10.2139/ssrn.2382787 accessed 28.2.2014.