Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling

[Published in *Computer Law & Security Report*, 2001, volume 17, pp. 17–24; also published in *Privacy Law & Policy Reporter*, 2000, volume 7, pp. 67–76]

Lee A. Bygrave

Abstract

In this paper, an analysis is carried out of Art. 15 of the 1995 EC Directive on data protection.[1] Article 15 grants persons a qualified right not to be subject to certain forms of fully automated decision making. It is one of the most intriguing and innovative provisions of the data protection Directive yet also one of the most difficult to construe properly. The central issue taken up in this paper concerns the extent to which Art. 15 may have a meaningful impact on automated profiling practices.

1 Introduction

Article 15(1) reads as follows:

"Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."

Up until very recently, provisions along the lines of Art. 15(1) have been rare amongst data protection instruments at both national and international levels. While their roots in data protection law go back to the late 1970s – more specifically to ss. 2–3 of the French data protection legislation enacted in 1978[2] – less than a handful of countries incorporated such provisions in their data protection laws *prior* to adoption of the EC Directive.[3] The inclusion in

---

1 Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (O.J. L 281, 23.11.1995, p. 31 *et seq*.) – hereinafter also termed simply "Directive".

2 *Loi no. 78-17 du 6. janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. Section 2 of this Act stipulates: "No judicial decision involving an appraisal of human conduct may be based on any automatic processing of data which describes the profile or personality of the citizen concerned. No governmental or private decision involving an appraisal of human conduct may be based solely on any automatic processing of data which describes the profile or personality of the citizen concerned". Section 3 states: "Any person shall be entitled to know and to dispute the data and logic used in automatic processing, the results of which are asserted against him". These translations are taken from Simitis, Dammann & Körner (ed.s), *Data Protection in the European Community: The Statutory Provisions* (Baden-Baden, 1992, loose-leaf, regularly updated).

3 In addition to ss. 2–3 of the French Act, see Art. 12 of the first Spanish data protection law (*Ley organica 5/1992 de 29. de octubre 1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*; replaced and repealed by Law 15/1999 of 13.12.1999) and Art. 16 of the first Portuguese data protection law (*Lei no. 10/91 de 12. de Abril 1991, da Proteccão de Dados Pessoais face à Informática*); replaced and repealed by Law no. 67/98 of 26.10.1998).

the Directive of the right provided by Art. 15(1) partly reflects a desire – as expressed in the Directive's preamble – to bring about a "high" level of data protection across the EU.[4]

Soon, a relatively large number of countries will have enacted provisions along the lines of Art. 15(1), mainly – though not exclusively[5] – as a result of the Directive. The overwhelming majority of these countries, however, will be European, at least for the near future. The extent to which non-European countries will enact provisions similar to Art. 15(1) remains unclear – an issue that is taken up in the concluding section of this paper.

As a data protection provision, Art. 15(1) is rather special in that, unlike the bulk of other rules in data protection instruments, its primary formal focus is on a type of *decision* as opposed to data processing. As such, Art. 15(1) is akin to traditional administrative law rules on government decision making. This characteristic, though, does not have large practical significance given that decisions inevitably involve the processing of data. Moreover, the impact of Art. 15(1) is likely to be considerably greater on the decision-making processes of the private sector than on the equivalent processes of the public sector, at least in jurisdictions with administrative law regimes that already provide broad rights of appeal against the decisions of government bodies (though not against private sector organisations).[6]

Article 15(1) is also rather special in that it is the only provision of the data protection Directive to grapple directly with particular aspects of automated profiling.[7] Generally speaking, profiling is the process of inferring a set of characteristics (typically behavioural) about an individual person or collective entity and then treating that person/entity (or other persons/entities) in the light of these characteristics. As such, the profiling process has two main components: (i) profile generation – the process of inferring a profile; (ii) profile application – the process of treating persons/entities in light of this profile. The first component typically consists of analysing personal data in search of patterns, sequences and relationships, in order to arrive at a set of assumptions (the profile) based on probabilistic reasoning. The second component involves using the generated profile to help make a search for, and/or decision about, a person/entity. The line between the two components can blur in practice, and regulation of the one component can affect the other component.[8]

On its face, Art. 15(1) only lays restrictions on the process of profile application. The same applies with earlier versions of the provision as contained in the first and amended proposals for the data protection Directive.[9] This is in contrast to the original proposal for the Directive on

---

4 See especially recital 9 (providing that EU Member States "shall strive to improve the protection currently provided by their legislation") and recital 10 (providing, *inter alia*, that the "approximation" of Member States' data protection laws pursuant to the Directive "must not result in any lessening of the protection they afford but must … seek to ensure a high level of protection in the Community").

5 Other (also non-legal) instruments could play a role here too. For instance, the Code of Practice on Protection of Workers' Data drafted by the International Labour Office (ILO) – see *Protection of Workers' Personal Data* (Geneva, 1997) – contains several principles restricting the use of fully automated decision making in the assessment of worker conduct. See *infra* n. 47.

6 This is not to imply that Art. 15(1) is necessarily limited to functioning as a right of appeal after a decision has been made.

7 See also, though, Art. 12(a) – presented in section 3 below.

8 For an extensive presentation and discussion of profiling practices, see Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Oslo, 1999), Part IV.

9 See Art. 14(2) of the Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data (COM(90) 314 final – SYN 287, 13.9.1990) (granting a person the right "not to be subject to an administrative or private decision involving an assessment of his conduct which has as its sole basis the automatic processing of personal data

telecommunications privacy which specifically restricted the creation of electronic subscriber profiles.[10] Nevertheless, the controls set by Art. 15(1) on profile application are likely to have an indirect effect on the process of profile creation. At the same time, there are no other provisions in the Directive specifically addressing the creation of profiles. This sort of situation is far from unique; the vast majority of data protection laws lack such provisions.

Article 15(1) does not take the form of a direct prohibition on a particular type of decision making (profile application). Rather it directs each EU Member State to confer on persons a right to prevent them being subjected to such decision making. Hence, a legally adequate implementation of Art. 15(1) may occur when national legislators simply provide persons with the opportunity to exercise such a right. This would leave the actual exercise of the right to the discretion of each person and allow, in effect, the targeted decision making to occur in the absence of the right being exercised (provided, of course, that the data-processing operation involved in the decision making meets the other requirements of the Directive and of national laws implementing the Directive).[11] This notwithstanding, national legislators are not prevented from implementing Art. 15(1) in terms of a prohibition on the targeted decision making.[12] However, such a prohibition cannot be absolute given that certain exceptions to the right in Art. 15(1) are mandated pursuant to Art. 15(2) and Art. 9. The scope and impact of these exceptions are dealt with in section 5 of this paper.

2 Rationale for Article 15

Article 15 derives from several concerns. The central concern is rooted in the perceived growth of automatisation of organisational decisions about individual persons. The drafters of the Directive appear to have viewed as particularly problematic the potential for such automatisation to diminish the role played by persons in shaping important decision-making processes that affect them. In relation to the forerunner to Art. 15(1) as contained in the 1990 Directive proposal, the EC Commission states:

"This provision is designed to protect the interest of the data subject in participating in the

---

defining his profile or personality"); and Art. 16(1) of the Amended Proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(92) 422 final – SYN 287, 15.10.1992) (granting a right to every person "not to be subjected to an administrative or private decision adversely affecting him which is based solely on automatic processing defining a personality profile").

10 See Art. 4(2) of the 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) ("The telecommunications organization shall not use such data [i.e. personal data on subscribers] to set up electronic profiles of the subscribers or classifications of individual subscribers by category"). The provision was deleted from later drafts "in order to take account of the principle of subsidiarity": see COM(94) 128 final – COD 288, 13.6.1994, p. 8.

11 As has been done, for instance, pursuant to s. 25 of Norway's Personal Data Act of 1999 (*lov om behandling av personopplysninger av 14. april 1999 nr. 31*).

12 As has been done, for example, pursuant to Art. 12bis of the 1998 Belgian data protection legislation (*Wet tot omzetting van de Richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de Bescherming van Natuurlijke Personen in verband met de Verwerkung van Persoonsgegevens en betreffende de Vrij Verkeer van die Gegegevens, van 11 december 1998; Loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlament Euroéen et du Conseil relative à la Protection des Personnes Physiques à l'égard du Traitement de Données à Caractère Personnel et à la Libre circulation des ces Données, du 11 decembre 1998*).

making of decisions which are of importance to him. The use of extensive data profiles of individuals by powerful public and private institutions deprives the individual of the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his 'data shadow'".[13]

A second expressed fear is that the increasing automatisation of decision-making processes engenders automatic acceptance of the validity of the decisions reached and a concomitant reduction in the investigatory and decisional responsibilities of humans. In the words of the Commission,

"the result produced by the machine, using more and more sophisticated software, and even expert systems, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities".[14]

One can also read into these comments a concern that, in the context of organisational decision making, the registered data-images of persons (their "data shadows") threaten to usurp the constitutive authority of the physical self despite their relatively attenuated and often misleading nature. A further concern is that this threat brings with it the threat of alienation and a threat to human dignity.[15]

There can be little doubt that the concerns outlined above should be taken seriously. While fully automated decision making in the manner described by Art. 15(1) still seems far from widespread, computers are frequently involved in executing assessments that have previously been the preserve of human discretion – e.g. in the context of determining persons' credit ratings, insurance premiums or social welfare entitlements. Up until recently, such assessments have tended to be based primarily on data collected directly from the data subjects in connection with the assessment at hand. It is likely, though, that these assessments will increasingly be based on pre-collected data found in the databases of third parties. Indeed, with effective communication links between the databases of large numbers of organisations, sophisticated software to trawl these databases, and appropriate adaptation of the relevant legal rules (i.e. an "automationsgerechte Rechtsetzung"),[16] it is easy to envisage computerised decision-making processes that operate independently of any specific input from the affected data subjects.[17]

---

13 COM(90) 314 final – SYN 287, 13.9.1990, p. 29.

14 COM(92) 422 final – SYN 287, 15.10.1992, p. 26.

15 See also Bygrave & Berg, "Reflections on the Rationale for Data Protection Laws", in Bing & Torvund (ed.s), *25 Years Anniversary Anthology in Computers and Law* (Oslo, 1995), p. 3, 32 ("the interest in non-automated decision making is founded not simply on the possibility of machines making mistaken judgements; penultimately, the interest embodies a concern for personal integrity, and ultimately a concern for human dignity"). Cf. recital 2 in the preamble to the Directive ("Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms … and contribute to … the well-being of individuals").

16 The phrase is taken from (German) literature dealing with adaptation of legal rules to facilitate automated decision-making processes: see e.g. Fiedler, "Automationsgerechte Rechtsetzung" (1974) 9 *Datareport*, no. 2, pp. 12–17. See also Bing, "Automatiseringsvennlig lovgivning" (1977) *Tidsskrift for Rettsvitenskap*, pp. 195–229. For a more recent analysis of what such adaptation entails, see Bing, "Three Generations of Computerized Systems for Public Administration and Some Implications for Legal Decision-Making" (1990) 3 *Ratio Juris*, pp. 219–236.

17 For a concrete example of an administrative decision-making system with a large, though not total, degree of such automation, see Bing, "The Emergence of a New Law of Public Administration. Research Issues Related to the Norwegian Housing Aid System", in Kaspersen & Oskamp (ed.s), *Amongst Friends in Computers and Law: A Collection of Essays in Remembrance of Guy Vandenberghe* (Deventer/Boston, 1990), pp. 229–240 (describing the decision-making system for assessment of benefits under the Norwegian Housing Aid Scheme).

Additionally, there is ongoing growth in the frequency, intensity and ambit of organisational profiling practices. Not only is profiling an emergent industry in its own right,[18] but the techniques upon which it builds (e.g. data warehousing and data mining)[19] are evermore sophisticated. Further, the efficacy of such techniques is now being enhanced through the use of artificial neural networks[20] and intelligent agents.[21] Part and parcel of the increasing sophistication of profiling techniques is their increasing automatisation as evidenced, for example, in cybermarketing practices.[22]

3 Related provisions

The right contained in Art. 15(1) is closely related to several other provisions in the Directive. To begin with, the right extends – and, to some extent, compensates for – the more general, albeit relatively weak right in Art. 14(a) of data subjects to object to the processing of data relating to them when there are "compelling legitimate grounds".[23] Secondly, Art. 15(1) helps to strengthen the right in Art. 14(b) of data subjects to object to data on them being processed for the purposes of direct marketing. Thirdly, Art. 15(1) contributes to reinforcing the rule in Art. 6(1)(a) that personal data be processed "fairly". Finally, note should be taken of Art. 12(a) which provides data subjects with, *inter alia*, a right to "knowledge of the logic involved in any automated processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1)". This last right is an important complement to the provisions of Art. 15 and helps to flesh out some of their requirements.[24]

---

18 For examples, see *Der Spiegel*, 5.7.1999, pp. 112ff.; Novek, Sinha & Gandy, "The value of your name" (1990) 12 *Media, Culture and Society*, pp. 526ff.; Froomkin, "Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases" (1996) 15 *University of Pittsburgh Journal of Law and Commerce*, p. 395, Part IV.

19 Data warehousing is the process by which an organisation gathers data from disparate sources and loads these data into a central, integrated database for subsequent analysis and (re)use. Data mining is the process by which data (e.g. those in the "warehouse") are examined through the use of various algorithms in order to uncover latent data patterns, connections, sequences, etc. that may be useful for the organisation. See generally the collection of articles in Fayyad & Uthurusamy (ed.s), "Data Mining and Knowledge Discovery in Databases" (1996) 39 *Communications of the ACM*, no. 11, pp. 24–68. See also *inter alia* Pipe, "The Data Mart: A New Approach to Data Warehousing" (1997) 11 *International Review of Law Computers & Technology*, pp. 251–261; Ontario, Information and Privacy Commissioner, *Data Mining: Staking a Claim on Your Privacy*, January 1998, <http://www.ipc.on.ca/english/pubpres/sum_pap/papers/datamine.htm> (last visited 29.8.2000). For a concrete example of the use of data mining to monitor employee behaviour, see *Computerworld Norge*, 28.4.1999, p. 5.

20 In short, artificial neural networks are computer algorithms that attempt to simulate the analytical operations of the human brain. For further description, see *inter alia* Bigus, *Data Mining with Neural Networks: Solving Business Problems from Application Development to Decision Support* (New York, 1996), especially chapters 2 and 4; Hubick, *Artificial Neural Networks in Australia* (Canberra, 1992), especially pp. 18ff.

21 In basic terms, intelligent agents are software applications which, with some degree of autonomy, mobility and learning capacity, execute specific tasks – e.g. data searches and filtering – for a computer user or computer system. For an introductory overview of various kinds of such agents, see Woolridge & Jennings, "Intelligent Agents: Theory and Practice" (1995) 10 *The Knowledge Engineering Review*, no. 2, pp. 115–152; Bigus, *supra* n .20, chapter 8.

22 For detailed description of such practices, see US Federal Trade Commission, *Online Profiling: A Report to Congress*, June 2000, <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf> (last visited 30.8.2000), pp. 2–8.

23 Article 14(a) expressly indicates that the right it provides may be overridden by national legislation. Hence, the practical impact of the right on national laws – and on profiling practices covered by these laws – is highly uncertain. Cf. the more narrowly formulated derogations in Art. 15(2) from the right provided by Art. 15(1): see further section 5 below.

24 See further section 4.3 below.

4 Applying Article 15(1)

For the right contained in Art. 15(1) to apply, four cumulative conditions must be satisfied:

1. A decision must be made;
2. The decision concerned must have legal or otherwise significant effects on the person whom the decision targets;
3. The decision must be based solely on automated data processing;
4. The data processed must be intended to evaluate certain personal aspects of the person who is targeted by the decision.

A considerable amount of ambiguity inheres in these conditions. This ambiguity is scarcely mitigated by the Directive's recitals or *travaux préparatoires*.

4.1 Condition 1

Neither the Directive nor its *travaux préparatoires* specifically address what is required for a decision to be made. Nevertheless, it is fairly obvious that making a decision about an individual person ordinarily involves the adoption of a particular attitude, opinion or stance towards that person. Such an attitude/stance can be of numerous kinds. For example, it can require the person to act or refrain from acting in a certain way. Or it can involve acceding to or denying a particular request from the person. Alternatively, it can result in action being taken to influence the person with or without his/her knowledge.

Difficulties may arise sometimes in distinguishing decisions from other processes (e.g. plans, suggestions, advice, mapping of options) that can prepare the way for, or head off, formal decision making.[25] At the same time, it is important to note that Art. 15(1) does not operate with any *prima facie* requirement that a decision be of a certain form. Further, the notion of decision in Art. 15(1) is undoubtedly to be construed broadly and somewhat loosely in light of the provision's rationale and its otherwise detailed qualification of the type of decision it embraces. Thus, the mere fact that a process is formally labelled or perceived as a plan or an advice would not be sufficient in itself to bring the process outside the ambit of Art. 15(1). Nevertheless, if a decision is to be caught by Art. 15(1), it must have some degree of binding effect on its maker (such that the latter is likely to act upon it). This follows partly from the very concept of a decision and partly from the requirement that the decision must have legal or otherwise significant effects on the person whom the decision targets (see condition 2 below).

Some uncertainty as to whether a decision is made could pertain to situations in which a human decision maker is apparently absent; i.e. when the process at hand consists of a response on the part of computer software (e.g. an intelligent agent) to particular constellations of data and data input. This issue is actualised by certain profiling practices in the context of cybermarketing. For instance, the advertising banners on Internet websites are frequently programmed to adjust

[25] For elaborations of these difficulties in the field of Norwegian public administrative law, see e.g. Eckhoff & Smith, *Forvaltningsrett* (Oslo, 1997, 6th ed.), pp. 403–404; Woxholth, *Forvaltningsloven med kommentarer* (Oslo, 1993, 2nd ed.), p. 31; Frihagen, *Forvaltningsrett* (Oslo, 1991), vol. 1, espec. p. 282 *et seq*.

automatically their content and/or format according to the net-browsing data about the site visitor which are stored as "cookies" on the visitor's computer.[26] Does such adjustment involve a decision being made?

In support of a negative answer, it could be argued that the term "decision" ordinarily connotes a *mental* action (the adoption of a particular *opinion* or *belief*). An affirmative answer, though, has stronger foundations. On the one hand, it can be plausibly argued that the term "decision" should be construed broadly for the reasons set out above. In light of this, the logical processes of computer software would seem to parallel sufficiently the processes of the human mind to justify treating the former as analogous to the latter for the purposes of Art. 15(1). On the other hand, it can be plausibly argued that a human decision maker will still exist even if he/she is not directly involved in the process concerned. That decision maker will be the person who is responsible for programming the software.[27]

4.2 Condition 2

Regarding condition 2, it is relatively clear what "legal effects" involve. These are effects that are able to alter or determine (in part or in full) a person's legal rights or duties.

Ambiguity with respect to condition 2 inheres mainly in the notion of "significantly". Does the notion refer only to effects that are significant for the data subject in an objective sense (i.e. relatively independent of the data subject's own perceptions)? Does it refer only to effects of a material (e.g. economic) nature? Does it require the decision concerned to be *adverse* to the interests of the data subject?

Given the thrust of recitals 9 and 10,[28] together with the likelihood that the Directive requires recovery for both material and immaterial damage pursuant to Art. 23,[29] it is doubtful that "significantly" refers exclusively to material effects. Arguably, therefore, a significant effect might lie merely in the insult to a data subject's integrity and dignity which is occasioned by the simple fact of being judged by a machine, at least in certain circumstances (e.g. when there is no reasonable expectation of, or reasonable justification for, the sort of decision making described in Art. 15(1)). Moreover, if we accept that an important part of the rationale for the right in Art.

---

[26] See e.g. the report by the Federal Trade Commission, *supra* n. 22.

[27] While this argument is highly plausible for computer software processes today, we should not overlook the future possibility of intelligent agents becoming so autonomous in their actions and learning capabilities that it is *logically* difficult to link their behaviour with any particular human(s). Even in such a situation, though, we could probably still find humans to whom the decisions could *legally* be linked.

[28] Set out *supra* n. 4.

[29] Admittedly, the Directive does not clearly specify whether or not the notion of "damage" in Art. 23 covers both material and immaterial loss. Nevertheless, recitals 9 and 10 weigh in favour of a broad interpretration of the damage concept in Art. 23. Further, the Commission's intention with respect to the equivalent provisions in its 1990 Directive proposal was that "[t]he concept of damage covers both physical and non-physical damage": COM(90) 314 final – SYN 287, 13.9.1990, p. 40. There is nothing to indicate that this intention changed in the subsequent drafting process leading to the Directive's adoption (see especially COM(92) 422 final – SYN 287, 15.10.1992, p. 33 ("Article 23(1), like Article 21(1) in the initial proposal, places a liability on the controller to compensate *any* damage caused to any person ...": emphasis added) and nothing to indicate that this intention has not been shared by either the European Parliament or Council. Cf. recital 55 which states that "any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller". However, one cannot place much weight on the presence of "any" in the English text of the recital since other texts, such as the French, German, Danish and Swedish, omit the adjective altogether.

15(1) is protection of human integrity and dignity in the face of an increasingly automated and inhuman(e) world, some consideration must be given to how the data subject perceives the effect(s) of the decision concerned. Nevertheless, the criterion "significantly" also has objective (inter-subjective) connotations. Thus, a data subject's perception of what constitutes a significant effect on him/her is very unlikely to be wholly determinative of the issue; the legal weight of the perception will depend on the extent to which it is regarded by a considerable number of other persons as having a reasonable basis.

Safeguarding the interests of the data subject requires that assessment of what is a significant effect is not based solely on the data subject's own reactions. Consider, for example, a situation in which a person who is considering whether to apply for a bank loan interacts with a fully automated loans assessment service offered by a bank. As a result of this interaction, the person is informed that he/she qualifies for a loan of a certain sum under certain conditions. The terms of this assessment could be viewed by the person as favourable yet fail to give an objectively accurate depiction of how much and under what conditions the person would be able to loan because, for instance, the programme steering the assessment does not take into account certain details about the person's life situation. Indeed, were the latter details taken into account, the person would qualify for a higher loan with more favourable repayment conditions (for him/her). In such a situation, the data subject might well experience the assessment decision as unproblematic despite its objective faults. Paradoxically, however, this sort of situation could fall outside the scope of Art. 15(1) on account of the provisions in Art. 15(2), which are described in section 5 below.

As for the issue of whether the criterion of "significant(ly)" requires the decision concerned to be *adverse* to the interests of the data subject, an earlier draft of the Directive expressly limited the right in Art. 15(1) to such decisions.[30] However, this fact alone does not mean we should read the same limitation into the final version of Art. 15(1). Indeed, the very fact that the term "adversely" has been dropped from Art. 15(1) might suggest an intention not to limit the scope of the right in such a way. Still, it is extremely doubtful that Art. 15(1) may apply when a decision has purely beneficial effects for the data subject. This follows partly from Art. 15(2), described in section 5 below. At the same time, there exists a large amount of conceptual (and practical) overlap between the notions of "significantly" and "adversely". This overlap notwithstanding, the criteria cannot be read as fully commensurate with each other. Some adverse effects can be too trivial to be significant. In other words, the fact that a decision has adverse effects is merely a necessary but not sufficient condition for finding that the decision has significant effects. Thus, what is required is a decision that is *significantly adverse* in its consequences.

On the latter point, the EC Commission seems to have been of the opinion that simply sending a commercial brochure to a list of persons selected by computer does not significantly affect the

[30] See Art. 16(1) of the 1992 Amended Proposal for the Directive, set out *supra* n. 9. See also the commentary on this provision in COM(92) 422 final – SYN 287, 15.10.1992, pp. 26–27: "The person must be subject to an adverse decision. The decision must be one which can be invoked against him, one which has consequences for him; thus the simple fact of sending a commercial brochure to a list of persons selected by computer is not a decision adversely affecting them for these purposes. […] Thus the use of scoring techniques with a view to the lending of money to an individual is possible, if positive decisions to lend are based solely on an automatic assessment of risks; but where the score is negative the legitimate interests of the data subject must be safeguarded, for example by deferring a final answer until the organisation has been able to carry out a 'flesh and blood' study of the case".

persons for the purposes of Art. 15(1).[31] Also other commentators view advertising (or at least certain forms of advertising) as too trivial to be significant.[32] Nevertheless, some forms of advertising have at least a potential to significantly affect their targets. For instance, the cybermarketing process outlined above in section 4.1 could plausibly be said to have a significant (significantly adverse) effect on the persons concerned if it involves unfair discrimination in one or other form of "weblining" (e.g. the person visiting the website is offered products or services at a higher price than other, assumedly more valuable consumers have to pay, or the person is denied an opportunity of purchasing products/services that are made available to others).[33]

Finally, there can be little doubt that a decision may have a significant effect on the data subject even if it does not result in a manifest/positive alteration of his/her situation *vis-à-vis* other persons. In other words, Art. 15(1) may apply even if the decision concerned is used to *refrain* from changing the *status quo* (e.g. psychometric testing of job applicants results in none of them being offered jobs).

4.3 Condition 3

Moving to condition 3 (i.e. the decision is based solely on automated data processing), the main problem here is to determine the proper meaning of the criterion "solely". If the criterion is read very strictly, one could argue that few, if any, decisions are or can be wholly the result of automated processes because the programmes steering these processes are initially created by human beings.[34] But such an argument deprives Art. 15(1) of any practical effect. Thus, it is necessary to operate with a relative notion of "solely". What the notion seems intended to denote is a situation in which a person fails to *actively* exercise any *real* influence on the outcome of a particular decision-making process. Such a situation would exist if a decision, though formally ascribed to a person, originates from an automated data-processing operation the result of which is not actively assessed by either that person or other persons before being formalised as a decision.[35]

At the same time, it is important to note that if a data subject successfully exercises his/her right to object pursuant to Art. 15(1), the data controller is simply required to review critically the criteria or factors forming the basis for the fully automated decision. The controller is not required to change these criteria or factors, nor to supplement them with other criteria/factors.

---

[31] *Ibid*. It should not be forgotten, though, that the Commission's opinion relates to a draft provision expressly requiring an *adverse* effect.

[32] See e.g. Damman & Simitis, *EG-Datenschutzrichtlinie: Kommentar* (Baden-Baden, 1997), p. 220 ("Die Einbeziehung oder Nichteinbeziehung in eine Direktwerbung ist … keine erhebliche Beeinträchtigung").

[33] Further on weblining, see Stepanek, "Weblining: Companies are using your personal data to limit your choices – and force you to pay more for products", *Business Week Online*, 3.4.2000, <http://www.businessweek.com/2000/00_14/b3675027.htm> (last visited 5.9.2000); FTC, *supra* n. 22, p. 13.

[34] An argument also broached in Korff, "The Effects of the EC Draft Directive on Business", in Dumortier (ed.), *Recent Developments in Data Privacy Law* (Leuven, 1992), p. 43, 50.

[35] See also COM(92) 422 final – SYN 287, 15.10.1992, p. 26: "what is prohibited is the strict application by the user [data controller] of the results produced by the system. Data processing may provide an aid to decision-making, but it cannot be the end of the matter; human judgement must have its place. It would be contrary to this principle, for example, for an employer to reject an application from a job-seeker on the sole basis of his results in a computerized psychological evaluation, or to use such assessment software to produce lists giving marks and classing job applicants in order of preference on the sole basis of a test of personality".

Nevertheless, the review process might well involve these sorts of amendments being made.

Such a review process will be partly facilitated by the data subject's right under Art. 12(a) to knowledge of the logic behind decisions of the kind embraced by Art. 15(1). The existence of this right means, in effect, that decision makers themselves must be able to comprehend the logic of the automated steps involved. This further means, in effect, that the logic be documented and that the documentation be kept readily available for consultation and communication (both inside and outside the decision maker's organisation).[36] The documentation must set out, at the very least, the data categories which are applied, together with information about the role these categories play in the decision(s) concerned.

4.4 Condition 4

As for condition 4 (i.e. the data processed are intended to evaluate "certain personal aspects" of the data subject), this does not necessitate, on its face, the construction of a formalised profile of the data subject.[37] In practice, however, the use of profiling techniques and the creation of some sort of personality profile will be required, though the profile need not be formalised as such.

It would seem that Art. 15(1) indirectly covers some use of abstract profiles,[38] as the term "data" is not directly qualified by the adjective "personal". The latter fact means that the profile could be derived from "clickstream" data (e.g. domain names, websites visited, keywords used in search programs) that are somewhat difficult to classify as "personal" data pursuant to data protection legislation because they are linked primarily to an Internet Protocol address of a computer, not an individual person. Ultimately, though, the decision to which a person may object must be based on a profile of that person. At the same time, there is no requirement that the profile casts the person in a particular (positive or negative) light.

The chief point of uncertainty with condition 4 is the scope of the phrase "certain personal aspects". There is no doubt that the phrase "personal aspects" refers to aspects of the data subject's person or personality.[39] Moreover, there is little doubt that inclusion of the word "certain" means that not all "personal aspects" are legally relevant for the application of Art. 15(1). The question arises as to where and how the line is to be drawn between legally relevant "personal aspects" and those aspects that are not legally relevant. Some aid is provided by the non-exhaustive exemplification in Art. 15(1) itself ("work performance", "creditworthiness",

---

[36] Recital 41 of the Directive, however, places some limits on such communication to data subjects (and to other persons external to the organisation of the data controller or decision maker). The recital states, *inter alia*, that the right to knowledge of the logic behind automated decision making "must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software". Yet the recital also states that "these considerations must not … result in the data subject being refused all information". It remains to be seen just how difficult achieving the right balance here will be.

[37] Cf. Article 16(1) of the 1992 Amended Proposal for the Directive which specifically refers to "personality profiles". By contrast, Art. 14(2) of the 1990 Directive Proposal refers to "data defining his [the data subject's] profile or personality". See *supra* n. 9.

[38] By "abstract profile" is meant a set of characteristics linked primarily to a relatively abstract category of persons or collective entities (e.g. female university students; large multinational corporations). This sort of profile is to be contrasted with a set of characteristics connected primarily to a specific person or collective entity. See further Bygrave, *supra* n. 8, chapter 17 (section 17.2).

[39] See also the French version of the Directive which refers to "certain aspects of his [the data subject's] personality" ("certains aspects de sa personnalité"), while the German version refers to "certain aspects of [the data subject's] person" ("einzelner Aspekte ihrer Person").

"reliability" and "conduct"). This exemplification indicates that legally relevant "personal aspects" must concern a person's abilities, behaviour, preferences or needs; i.e. they must concern a person's *character*. They must concomitantly have a degree of complexity.[40] Thus, quantitative data on purely physiological traits (e.g. a person's physical speed of reaction or blood type) are unlikely in themselves to constitute "personal aspects" unless they are combined with other data that connect them more directly to a person's character (e.g. the data are applied to evaluate a person's degree of diligence/negligence in a particular context).[41]

The exemplification in Art. 15(1) further indicates that "personal aspects" need not relate primarily to the private (non-public) or domestic (non-professional) sides of a person's character. There would also appear to be no necessity that these aspects are unique to the person. It is otherwise difficult at this stage to make reasonably determinative statements about the reach of the phrase "certain personal aspects".

Nevertheless, there can be little doubt that Art. 15(1) will not apply to a fully automated decision by a bank to refuse a person cash simply because the person lacks the necessary credit in his/her bank account.[42] A different result would arise, however, if the decision concerned were grounded on a fully automated analysis of the person's payment history; this would involve an evaluation of creditworthiness in the more personal sense envisaged by Art. 15(1). Less certain is whether Art. 15(1) would apply to a fully automated decision about a person's eligibility for a retirement pension, when the decision is grounded simply on the level of the person's income and financial assets. There is no obvious answer to the question.[43] At first glance, these data types appear relatively neutral in terms of what they indicate about a person's character. Yet they are sufficient to constitute a rudimentary personality profile when linked together and it might well be possible to derive latent aspects of a person's character from their linkage. Moreover, they are sufficient to give a reasonable indication of a person's creditworthiness. Thus, solid grounds exist for arguing that Art. 15(1) embraces the above type of decision on pension eligibility.

5 Derogations from Article 15(1)

The right in Art. 15(1) may be derogated from pursuant to Art. 15(2) and Art. 9.[44]

Article 15(2) allows a person to be subjected to a decision referred to in Art. 15(1) in the following situations:

---

40 A point emphasised particularly in Dammann & Simitis, *supra* n. 32, p. 219.

41 See also Dammann & Simitis, *supra* n. 32, pp. 219–220 ; Ehmann & Helfrich, *EG Datenschutzrichtlinie: Kurzkommentar* (Köln, 1999), p. 230.

42 The same line is taken in, *inter alia*, *Behandling af personoplysninger*, Betænkning no. 1345 (Copenhagen, 1997), p. 494. See also COM(92) 422 final – SYN 287, 15.10.1992, p. 26: "The processing must apply variables which determine a standard profile (considered good or bad) to the data concerning the data subject; this excludes all cases where the system does not define a personality profile: for example, the fact that a person is unable to obtain the sum of money he wants from an automatic cash dispenser because he has exceeded his credit limit would not fall inside this definition".

43 Cf. *Et bedre personvern – forslag til lov om behandling av personopplysninger*, Norges Offentlige Utredninger 1997:19, p. 69 (answering this question in the negative, though subsequently noting that delineation of what shall be classified as "certain aspects of personality" is relatively unclear).

44 The relatively large list of derogations provided for under Art. 13(1) does not apply to Art. 15.

1. where the decision is taken in the course of entering into or executing a contract, *and* either the data subject's request for the entering into or execution of the contract has been fulfilled *or* provision is made for "suitable measures" to safeguard the person's "legitimate interests" (Art. 15(2)(a)); or
2. where the decision "is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests" (Art. 15(2)(b)).

Article 15(2) stipulates that both its sets of derogations must be incorporated into the legal regimes of EU member states, though "subject to the other Articles of this Directive". How problematic this is from a data protection perspective will depend partly on the nature of the "suitable measures" for safeguarding the interests of data subjects.

An example of a "suitable measure" in the first situation delineated by Art. 15(2) is described as "arrangements allowing [the data subject] … to put his point of view" (Art. 15(2)(a)). Given the rationale for Art. 15, it is to be presumed that these arrangements must not only allow for the data subject to put his/her point of view but also ensure that this point of view is received and taken into account by those who are formally responsible for the decision concerned.[45] It is further to be presumed that the arrangements must allow for the data subject's viewpoint to be expressed *before* any final decision is made.[46]

This example of a "suitable measure" is undoubtedly pertinent for Art. 15(2)(b) as well. At the same time, the example is not intended to delineate the entire range of "suitable measures" in both situations.

Independent of the issue of "suitable measures", there is a significant problem from a data protection perspective in one of the assumptions that apparently underlies Art. 15(2)(a): this is that the derogation which Art. 15(2)(a) provides from the operation of Art. 15(1) seems to assume that fulfilment of a person's request to enter into or execute a contract will always be unproblematic for that person. Such an assumption, however, is fallacious – as indicated by the bank loan example set out in section 4.2 above. To take another example, Art. 15(2)(a) would seem to allow a person's application for employment to be decided solely on the basis of psychometric testing if he/she is given the job (i.e. his/her request to enter into a contract is met). Yet such testing can have detrimental consequences for the person concerned (and for the quality of employment application processes generally). For instance, the person could well regard such testing as demeaning to his/her dignity, or the testing could fail to reveal that the person is qualified for another, more favourable position.

Turning to Art. 9, this requires certain derogations from Art. 15(1) – and from other provisions in Chapters III, IV and VI of the Directive – in the interests of freedom of expression. More specifically, Art. 9 requires derogation from these provisions insofar as the processing of personal data "is carried out solely for journalistic purposes or the purpose of artistic or literary expression" and the derogation is "necessary to reconcile the right to privacy with the rules governing freedom of expression".

---

[45] See also Dammann & Simitis, *supra* n. 32, pp. 221–222.
[46] See also Ehmann & Helfrich, *supra* n. 41, p. 233.

It is difficult to see how Art. 9 can have any extensive practical relevance for the sort of decision making dealt with by Art. 15(1). One can envisage, though, the emergence of a kind of automated journalism that bases its portrayals of the character of particular persons exclusively on the automated searching and combination of data from, say, various Internet sources. This sort of activity might have a chance of falling within the scope of Art. 15(1), though its ability to meet the decisional criteria of the provision is uncertain.

6 Article 15 – "all dressed up but nowhere to go"?

At first glance, Art. 15 shows much promise in terms of providing a counterweight to fully automated profiling practices. On closer analysis, however, we find that this promise is tarnished by the complexity and numerous ambiguities in the way the provisions of Art. 15 are formulated. These problems are exacerbated by a paucity of authoritative guidance on the provisions' scope and application. The efficacy of Art. 15 as a regulatory tool is further reduced by the fact that its application is contingent upon a large number of conditions being satisfied; if one of these conditions is not met, the right in Art. 15(1) does not apply. As such, the right in Art. 15(1) resembles a house of cards. In the context of *currently common* data-processing practices, this house of cards is quite easy to topple. Nevertheless, this situation might well change in the future if, as is likely, automated profiling becomes more extensive.

Even now, Art. 15 is normatively important in terms of the principle it establishes and embodies. This principle is that fully automated assessments of a person's character should not form the sole basis of decisions that significantly impinge upon the person's interests. The principle provides a signal to profilers about where the limits of automated profiling should roughly be drawn. We see also that this principle is beginning to be elaborated upon in concrete contexts, such as the assessment of worker conduct.[47]

At the same time, though, the "safe harbour" agreement which has been concluded recently between the USA and EU,[48] and which stipulates conditions for permitting the flow of personal data from the EU to the USA, puts a question mark over the status of the Art. 15 principle for non-European jurisdictions. The principle is nowhere to be found in the terms of the agreement.[49]

---

47 See here the ILO Code of Practice on Protection of Workers' Data (*supra* n. 5), particularly principles 5.5 ("Decisions concerning a worker should not be based solely on the automated processing of that worker's personal data"), 5.6 ("Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance"), 6.10 ("Polygraphs, truth-verification equipment or any other similar testing procedure should not be used") and 6.11 ("Personality tests or similar testing procedures should be consistent with the provisions of this code, provided that the worker may object to the processing").

48 See Commission decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (O.J. L 215, 25.8.2000, p. 7 *et seq*.).

49 This is despite the opinion of the Working Party established pursuant to Art. 29 of the data protection Directive (Working Party on the Protection of Individuals with regard to the Processing of Personal Data) that the safe harbour agreement should make provision for the principle. See especially *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, Working Document adopted 24.7.1998, <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp12en.pdf>, pp. 6–7 (cf. p. 17). This standpoint is followed up (though rather obliquely) by the European Parliament in its Resolution of 5.7.2000 on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Principles and related Frequently Asked Questions issued by the US Department of Commerce (A5-0177/2000), Point B(d) (stating that the data protection regimes of third countries should provide a data subject with a right to object to the processing of data on him/her "in certain situations").

Hence, other non-European countries will probably not be required by the EU to implement the principle either. So far, legislators in these countries have shown little willingness to implement the principle of their own accord.[50]

This situation is unfortunate. Despite its special character relative to the bulk of other data protection rules, the principle laid down by Art. 15 should be regarded as a *core* data protection principle; i.e. a principle that is indispensable for defining the future agenda of data protection law and policy, and one that should therefore be embodied in most, if not all, future data protection instruments around the globe.[51] Otherwise, data protection instruments risk being deprived of a significant (albeit imperfect) counterweight to the ongoing expansion, intensification and refinement of automated profiling practices.

[50] For instance, no specific provision has been made for the principle in the proposed new federal data protection laws for the private sector in Canada and Australia. See further Canada's Personal Information Protection and Electronic Documents Act 2000 (Bill C-6) and the Privacy Amendment (Private Sector) Bill 2000 introduced into the Australian Federal Parliament on 12.4.2000.

[51] Cf. the Art. 29 Working Party which does not count the principle as a "basic" data protection principle – at least for the purposes of determining what is adequate protection in the context of data flows to non-EU countries – but rather as an "additional principle to be applied to specific types of processing". See *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, *supra* n. 49, pp. 6–7 (cf. p. 17).