Determining Applicable Law pursuant to European Data Protection Legislation


Lee A. Bygrave

1. Introduction

In this paper, an examination is made of rules determining applicable law pursuant to European data protection legislation. The main point of departure for analysis is Art. 4 of the 1995 EC Directive on data protection. The provisions of Art. 4 constitute the first and only set of rules in an international data protection instrument to deal specifically with the determination of applicable law. These rules will become the norm for the data protection legislation of countries within the EU and EEA, and possibly also for the equivalent laws of other States. Somewhat surprisingly, the provisions in Art. 4 have so far been subjected to little academic analysis. Yet, as shown in this paper, these provisions could have a significant impact on the activities of e-commerce operators, including those operators established outside the EU/EEA.

Prior to adoption of the 1995 EC Directive on data protection, the rules governing territorial reach of national European data protection laws and concomitant jurisdictional and choice-of-law problems have tended to be complex and, to some extent, contradictory and unclear. Further, discussion about the most appropriate rules in this respect has been characterised more by disagreement than consensus.

A complicating factor is the nature of data protection law in relation to private international law. Data protection law straddles the boundaries between public and private law, criminal and civil law. This makes it difficult to firmly place data protection law within any one of the legal categories traditionally employed by the doctrines of private international law. It also complicates attempts to locate and/or assimilate suggested jurisdictional and choice-of-law solutions for the field of data protection within the broader field of interlegal rules.

1 This paper has been written as part of Phase 1 of the ECLIP project (Electronic Commerce Legal Issues Platform) funded by the EC Commission under the Esprit programme. General information on ECLIP is available at http://www.jura.uni-muenster.de/eclip. The conclusions reached in this paper, though, are entirely those of its author and do not necessarily reflect the opinions of other contributors to ECLIP nor the views of the EC Commission.


3 For relatively detailed analysis of these rules and the academic/policy discussions which have revolved around them, see inter alia Ellger, Der Datenschutz im Grenzüberschreitende Datenverkehr: Eine rechtsvergleichende und kollisionsrechtliche Untersuchung (Baden-Baden, 1990), chapter IV; Nugter, Transborder Flow of Personal Data within the EC (Deventer/Boston, 1990), chapter VII; Bergmann, Grenzüberschreitende Datenschutz (Baden-Baden, 1985), chapter 7. For a briefer treatment, see inter alia Bing, "Transnational Data Flows and the Scandinavian Data Protection Legislation" (1980) 24 Scandinavian Studies in Law, p. 65, 88–96; Hoeren, “Electronic Data Interchange: The Perspectives of Private International Law and Data Protection”, in Carr and Williams (eds.), Computers and Law (Oxford, 1994), p. 128 et seq.
Another complicating factor is the nature of the information systems that data protection law seeks to regulate. Many of these systems are increasingly difficult to link to one fixed geographical location, yet the doctrines of private international law tend to rely on an ability to make such links. Concomitantly, the ability of persons and organisations to identify the full parameters of the informational transactions surrounding and/or affecting them is being challenged by the increasing complexity of these transactions, yet interlegal doctrines tend, again, to presume such an ability.

2. The situation prior to adoption of the EC Directive on data protection

Prior to adoption of the EC Directive on data protection, each European country’s data protection law has applied, as an obvious point of departure, to the processing of personal data within the country’s borders (and, in some cases, its overseas territories). Application usually has not depended on the nationality or legal domicile of the data subject(s) – the person(s) to whom the data relate – but this has not always been the case, at least with respect to data protection laws outside Europe. Of typically more decisive importance has been the existence and character of the link between, on the one side, a data controller (the person/organisation who/which determines the purposes and means of data processing) and/or data-processing operation and, on the other side, the territory of the country concerned. If both the controller and the processing operation have been closely linked to the territory (e.g. the controller resides or is established in the territory and the processing is carried out within the latter) then the country’s data protection law has normally applied to the controller and the processing operation.

Under many data protection Acts, the principal criterion for application has been the location of the data processing (or data file). However, this criterion has sometimes been waived, allowing the Act to be applied to data processing (or files) outside the country, and thereby creating a potential for conflict of laws.

The conditions under which waiver may occur have varied from law to law. The 1988 Netherlands’ Act on data protection, for example, could apply to personal data files not located in the Netherlands when: (i) the file is controlled by someone established in the Netherlands; and

---

4 Contrast the 1978 French Act on data protection (Loi no. 78-17 du 6. janvier 1978 relative à l’informatique, aux fichiers et aux libertés), which applies to France’s remaining overseas territories, such as Guadeloupe, with the UK Data Protection Act of 1984 which does not apply to British overseas territories, such as Bermuda and the Cayman Islands. Note too that by virtue of s. 2 of Norway’s 1985 Petroleum Act (Lov om petroleumsvirksomhet 22. mars 1985 nr. 11), the 1978 Norwegian Act on data protection (Lov om personregistre mm av 9. juni 1978 nr. 48) applies to offshore installations engaged in exploration, production and transport of petroleum products on the Norwegian continental shelf (and outside the Norwegian continental shelf if this is in accordance with international law or an agreement with a foreign State). However, the Norwegian data protection Act does not apply to the island of Spitzbergen.

5 See e.g. the US federal Privacy Act of 1974 which only protects data subjects who are citizens or legal permanent residents of the USA (s. 552a(a)(2)).

6 This is the case, for instance, with the 1990 German federal Act on data protection (Bundesdatenschutzgesetz – Gesetz zum Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990) – see Simitis, “§ 1”, in Dammann, Geiger, Mallmann, Simitis & Walz, Kommentar zum Bundesdatenschutzgesetz (Baden-Baden, 1992, 4th ed.), paragraph 74 et seq.; the 1992 Belgian Act on data protection (Loi du 8 décembre 1992 relative à la protection de la vie privée à l’égard des traitements de données à caractère personnel) – see Art. 3(1)(1); and the 1988 Netherlands’ Act on data protection (Wet van 28. december 1988, houdende regels ter bescherming van de persoonlijke levenssfeer in verband met personenregistraties) – see Nugter, supra n. 3, p. 187.

7 As graphically illustrated in, inter alia, Nugter, supra n. 3, p. 190 et seq.
(ii) the file contains data on persons who have the Netherlands as their domicile (s. 47(1)). By contrast, the 1992 Belgian Act on data protection could apply to automated processing of personal data abroad “where such processing is directly accessible in Belgium by means which are integral to the processing itself” (Art. 3(1)(2)). This rather ambiguous provision has been broadly interpreted such that the Belgian Act would apply to, say, a server located outside Belgium if either the information on the server is used in Belgium, originates in Belgium or is accessible from Belgium.\(^8\) As for Norway’s 1978 Act on data protection, this has been construed by the Norwegian Ministry of Justice as applying to a personal data register located abroad when the register can be “controlled” from Norway.\(^9\)

3. Determination of applicable law pursuant to Art. 4 of the EC Directive on data protection

The rules on applicable law laid down by the data protection Directive are found in Art. 4, which reads:

“Article 4: National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State’s territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself”.

As noted above, these provisions constitute the first and only set of rules in an international data protection instrument to deal specifically with the determination of applicable law. By contrast,\(^8\)

---


\(^9\) See letter of 25.09.1997 from the Ministry’s “Lovavdeling” to the Norwegian Data Inspectorate (ref. 97/02197KJR/HSD/bj). By “control” (“råderett”) is meant, as a minimum, that a person or organisation is able to gain access to, and register or store, data in the register. Otherwise, though, the Ministry refrains in its letter from delineating what other criteria are necessary in order that a person/organisation in Norway may be classified as having “control” over the register such that the latter falls within the licensing requirements of the data protection Act. According to the Ministry, these criteria can only be determined on a case-by-case basis. Cf. Djenne, Gronn & Haftli, Personregisterloven med kommentarer (Oslo, 1987), p. 156 (noting that a personal data register located abroad might be covered by the data protection Act if a person/organisation in Norway is able to change the data in it). For concrete instances in which the Norwegian data protection Act has been claimed to have extra-territorial application, see Jarbekk, Personvern og overføring av personopplysninger til utlandet (Oslo, 1996), p. 29 et seq.
the drafters of the 1980 OECD Guidelines on data protection\textsuperscript{10} were unable to reach agreement on appropriate rules, despite discussing interlegal issues extensively.\textsuperscript{11} The same problems appear also to have afflicted the drafters of the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

It can be seen that, under Art. 4, the principal criterion for determining applicable law is the data controller’s place of establishment, largely irrespective of where the data processing occurs. This criterion will therefore become the norm for countries governed by the Directive. It is a criterion that fits well with the equivalent rules found in several other Directives,\textsuperscript{12} along with the draft e-commerce Directive.\textsuperscript{13}

The choice of criterion advanced in Art. 4 can be contrasted with the criterion suggested in the 1990 proposal for the data protection Directive. The latter criterion for determining applicable law was stipulated as the location of the data file concerned. This criterion was subsequently changed due to the difficulty of determining such a location in an age of transborder computer networks. This difficulty would be even greater with the switch of the Directive’s regulatory focus to data-processing operations as opposed to data files.\textsuperscript{14}

Some idea of the rationale for the rules in Art. 4 can be gained from the \textit{travaux préparatoires} to the Directive. Of particular importance is the following commentary from the EC Commission in relation to the 1992 Amended Proposal for the Directive:

“[the intention of Art. 4 is] to avoid two possibilities:
– that the data subject might find himself outside any system of protection, and particularly that the law might be circumvented in order to achieve this;
– that the same processing operation might be governed by the laws of more than one country”.\textsuperscript{15}

The aim of avoiding the first-mentioned of the above possibilities is also manifest in recital 20 in the preamble to the Directive:

“Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice; …”.

There are four important terms in Art. 4 which beg definition. Two of these terms recur throughout the Directive and are pivotal for determining the field of application of the Directive generally. They are “personal data” and “controller”. The other two terms are largely unique to Art. 4. They are “establishment” and “equipment”.

\textsuperscript{10} Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Paris, 1980).
\textsuperscript{11} See further para. 74 et seq. in the Explanatory Memorandum to the Guidelines. The most that could be agreed upon is laid down in para. 22 of the Guidelines: “Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data”.
\textsuperscript{12} See generally the overview in Bing, \textit{The identification of applicable law and liability with regard to the use of protected material in the digital context}, ECLIP Research Paper, January 2000 (available at http://www.jura.uni-muenster.de/eclip), section 5.2.
\textsuperscript{14} See generally COM (92) 422 final – SYN 287, 15.10.1992, p. 13.
\textsuperscript{15} \textit{Id.}
Regarding the term “personal data”, this is defined in Art. 2(a) as

“any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.16

The focus of this definition on the criterion of direct or indirect identifiability (i.e. on the potential of information to facilitate identification of a person) makes it capable in theory of encompassing much data that prima facie have little direct relationship to a particular person. Thus, data may be “personal” even if they allow a person to be identified only in combination with other (auxiliary) data.17

At the same time, though, certain limitations are usually read into the identifiability criterion such that identification must be possible using methods that do not involve an unreasonably large amount of time, expense and labour. Recital 26 in the preamble to the Directive lays down what appears to be a broad and flexible criterion for identifiability:

“to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person”.

Usually, data must be capable of being linked to a particular individual person before they are to be regarded as “personal” pursuant to data protection laws. Thus, data which can only be linked to an aggregate of persons will normally fall outside the ambit of such laws. However, some countries (e.g. Italy, Austria, Luxembourg and Norway) have data protection legislation that expressly covers data on collective entities such as corporations, partnerships and citizen initiative groups; nevertheless, such data are only covered if they can be linked back to one particular entity as opposed to a multiplicity of entities.

In an e-commerce environment, it is of particular importance to determine the extent to which “clickstream” data attached prima facie to an Internet Protocol address are personal data for the purposes of data protection law. The issue cannot be resolved in the abstract. Nevertheless, it is probable that such data could be personal data if, for instance, there is a readily accessible directory listing one particular person against one particular address.18

Regarding the term “controller”, this is defined in Art. 2(d) as the

“natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data”.

This definition envisages the possibility of there being more than one controller per data-processing operation (i.e. control can be shared). It also implies that a controller need not be in possession of the personal data concerned. Further, it envisages that who is controller may

---

16 Recital 14 in the Directive’s preamble makes clear that this definition also encompasses sound and image data on natural persons.
change from one data-processing operation to another, even within one information system. Finally, it indicates that determination of who is controller hinges not on the formal allocation of control responsibilities (as set down in e.g. contractual provisions) but on the factual exercise of control.

Regarding electronic communications networks, the person or organisation providing the transmission services is normally not to be regarded as the controller of personal data contained in a transmitted message; rather, the controller will be the person or organisation “from whom the message originates”.19 Nevertheless, transmission service providers “will normally be considered controllers in respect of the processing of the additional personal data necessary for the service”.20

A controller is to be distinguished from what the Directive terms a “processor”. The latter is defined in Art. 2(e) of the Directive as a person or organisation engaged in processing personal data “on behalf of” a controller. Controllers must ensure, through appropriate contractual or other arrangements, that processors carry out their tasks in compliance with the laws enacted pursuant to the Directive (Art. 17). In the event of a processor not complying with such laws, it will be the controller that is primarily liable (Arts. 23 & 17(2)). Moreover, as noted above, applicable law is determined by reference to the place of establishment of a controller as opposed to processor. Thus, for e-commerce operators, determining which actors are controllers is more important than determining which actors are processors.

The importance of the distinction between controllers and processors for determining applicable law can be highlighted using an actual case related to the application of Norwegian data protection legislation. In that case, the 1978 Norwegian Act on data protection was held by the Norwegian Ministry of Justice to apply to a register over the personnel of a cruise ship owned by a Norwegian company, despite the fact that the personnel were not Norwegian, the company directly employing the personnel was neither Norwegian nor established in Norway, and the ship only ever sailed in the Caribbean (as opposed to Norwegian territorial waters).21 Applying Art. 4 of the Directive to the facts of this case, if the company directly responsible for employing the personnel were classified as the controller in relation to data on the personnel, Norwegian data protection law would not apply to the processing of these data unless the ship-owner could also be classified as a (co-)controller of the data in question. In such a situation, two different data protection laws might apply to the same data-processing operation, resulting possibly in a positive conflict of legal authority.

However, a different (and less problematic) result would arise were the country in which the personnel company is established, to have no data protection legislation whatsoever, or the personnel company were properly to be classified as merely a processor of the data for purposes determined by the Norwegian ship-owner. In the latter case, Norwegian data protection law would apply if either the ship-owner was established in Norway (cf. Art. 4(1)(a)) or the data was being processed using computer equipment located on board the ship and the ship sailed under a Norwegian flag, thus qualifying as Norwegian territory (cf. Art. 4(1)(c)).

19 Recital 47 in the preamble to the Directive.
20 Id.
21 See further Jarbekk, supra n. 9, pp. 29–30 and references cited therein.
Turning to the notion of “establishment”, this is left undefined by the Directive save for some explanatory comments given in recital 19 in the Directive’s preamble. Recital 19 states that the criterion of establishment “implies the effective and real exercise of activity through stable arrangements”. Moreover, recital 19 continues, “the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect”. Hence, take the situation of company A which is established in Greece and which has a subsidiary, B, established in Portugal: the statements in recital 19 imply that if A processes data for purposes determined by B, Portuguese law will apply to the processing even if B is only a subsidiary of A.

The next phrase in need of interpretation is “makes use of equipment” in Art. 4(1)(c). This phrase is not defined in the Directive. The reference to “equipment” gives an impression that something materially substantial and solid must be used. Such an impression, however, is somewhat misleading. Recital 20 in the preamble to the Directive mentions simply “means used”; i.e. it drops the more technical term “equipment”. Other language versions of the Directive tend to refer simply to “means” (French “moyens”; German “Mittel”). In other words, the term is to be construed broadly and somewhat loosely.

4. Problematic aspects of Art. 4

The following discussion of problematic aspects of the rules in Art. 4 is necessarily tentative. There is, as yet, little experience of how the rules work in practice. At the same time, there is also a surprising paucity of in-depth discussion of the rules by legal academics and practitioners. With respect to the Directive’s international impact, the attention of most commentators has been directed towards the provisions in Arts. 25–26 of the Directive which attempt to regulate the flow of personal data from States within the EU to other States (so-called third countries). Nevertheless, for reasons set out below, the rules in Art. 4 could very well have an explosive impact on relations between the EU and other countries.

To provide a framework for the comments in this section, it is pertinent to recall the aims of Art. 4 as set down in the travaux préparatoires and preamble to the Directive. These aims are twofold: to avoid a situation in which the data subject finds him-/herself outside any system of protection; and to avoid a situation in which the same data-processing operation is governed by the laws of more than one country. As elaborated upon in the following, Art. 4 is likely to fulfill the first-mentioned of these aims, though to such an extent, perhaps, as to result in regulatory overkill. As for the second-mentioned aim, this is unlikely to be met in some instances.

---

22 This description appears to build upon case law of the European Court of Justice. See especially Case C-221/89, The Queen v. Secretary of State for Transport, ex parte Factortame Ltd and others [1991] ECR, p. 1-3905, para. 20: “the concept of establishment within the meaning of Article 52 et seq. of the Treaty [of Rome] involves the actual pursuit of an economic activity through a fixed establishment in another Member State for an indefinite period”.

23 In this regard, note also the Explanatory Memorandum for Belgium’s Act of 11.12.1998 to amend the country’s 1992 Act on data protection in line with the EC Directive. The Memorandum defines “means” as “every possible equipment, such as computers, telecommunications machinery, print units, etc. with explicit exclusion of means that are uniquely used for the transmission of personal data over the territory, such as cables, routers, etc.” (p. 27).

24 See supra n. 15 and accompanying text.
To take the last point first, while there will normally be just one controller for each data-processing operation, there could be occasions when there are found to exist two or more controllers, each established in different Member States, with respect to the one operation. This possibility is envisaged by the Directive’s definition of “controller” in Art. 2(d) – i.e. a controller is a body “which alone or jointly with others determines the purposes and means of the processing of personal data” (emphasis added). In such cases, application of Art. 4 would mean that the one data-processing operation is subject to different national laws. This will not be a problem if the various laws are in harmony with each other – which is the assumption and hope of the drafters of the Directive – but we cannot be certain that harmony will eventuate in all cases, particularly in light of the considerable margin for manoeuvre that Member States have been given in implementing the Directive.25

A related issue is whether Art. 4 requires EU Member States to drop their older rules allowing for extra-territorial application of their respective data protection laws in certain cases. It could be argued that Art. 4 does not regulate the extent of territorial application of Member State’s national data protection laws; Art. 4 just ensures that a particular law applies in a particular situation. If the argument is accepted,26 one will clearly run into problems of jurisdictional collision. However, it can scarcely be held that the drafters of the Directive did not intend to reduce, if not eliminate, such problems,27 and Art.4 should probably be construed in the light of this. Nevertheless, it would have been desirable in terms of legal certainty for the drafters of the Directive to have been more explicit on this point.

A further problem is that Art. 4(1)(c) gives rise to the possibility of regulatory overreaching in an online environment. By “regulatory overreaching” is meant a situation in which rules are expressed so generally and non-discriminatingly that they apply prima facie to a large range of activities without having much of a realistic chance of being enforced. To take a simple example, it is very common for the operators of websites to set “cookies” on to the browser programs of those visiting their sites. Such a mechanism operates automatically once established. If a website operator based in, say, India were to set cookies on to the browser programs of persons situated within the EU, then the operator’s actions would arguably meet the criteria in Art. 4(1)(c) – i.e. the operator would be processing personal data making use of equipment (broadly construed) situated on the territory of an EU Member State. This would mean that the processing would be governed by the data protection law of the EU Member State concerned. It is assumed, of course, that the cookies are properly to be classified as personal data pursuant to the Directive (there are solid arguments for viewing them as such).28

Thus, in an online environment, the strict application of Art. 4(1)(c) is likely to create a situation in which large numbers of data controllers outside the EU/EEA are supposed to comply with at least two sets of data protection rules that may not be harmonised (i.e. the rules of the EU/EEA Member State and the rules of the respective countries in which the controllers are established), and in which the duty of compliance with what are for the controllers foreign rules can arise on the basis of using relatively common, highly automated data-processing mechanisms. Indeed,

25 Obvious instances of this margin are found in Arts. 5, 7(f), 8(4), 10, 11, 13 and 14(a).
26 The argument is implicitly embraced in Bing, supra n. 12, section 5.2.2. In another paper, however, Bing distances himself from the argument: Bing, “Data protection, jurisdiction and the choice of law” (1999) 6 Privacy Law & Policy Reporter, p. 92, 95.
27 See supra n. 15 and accompanying text.
28 See references cited supra n. 18.
since the notion of “equipment” is a loose and disparate one, such that equipment used in one
data-processing operation can be dispersed over several countries, then controllers might have to comply with a considerable multiplicity of national laws. Complicating matters is the likelihood that many controllers (especially those situated in countries lacking national data protection authorities) will be unaware of these compliance duties. Who is to draw the attention of data controllers in third countries to the provisions of Art. 4(1)(c)?

Another problem is that, in an online environment, it will often be difficult for a data subject or data protection authority to determine the location of the controller, let alone to work out where the latter is “established”. Moreover, given that the exact legal parameters of the concept of establishment are far from clear – at least in the context of online networks – there will be difficulties in working out if an establishment exists.

One issue in this regard is the extent to which a website itself may be classified as an establishment pursuant to the Directive. This issue is not dealt with in detail here. For present purposes, it suffices to note that there is, as yet, a paucity of case law directly concerned with the issue. Moreover, at first sight, although it can be argued with some force that “effective and real exercise of activity” (recital 19) can be carried out through a website (at least if the site is interactive), it would seem difficult to argue that a website can satisfy the need for “stable arrangements” (recital 19 again).29

Yet another problem is that the Member State in which a data controller is established will not necessarily be the Member State in which the data subject affected by the processing is domiciled or resident. Thus, in an era of evermore extensive transborder data processing, data subjects are likely to be increasingly forced to seek remedies under foreign law for interferences with their data protection rights. In such a situation, data subjects may frequently face difficulties that they would not otherwise experience in seeking remedies pursuant to their own national laws.30

No doubt the intention of the Directive’s drafters is that such difficulties will be obviated by harmonisation of the respective Member State’s data protection laws, increased cooperation between the various national data protection authorities and increased possibilities for cross-jurisdictional court enforcement of data protection laws.31 But the extent to which these difficulties will be lessened in practice is unclear.

5. Possible remedies

A great number of problems have been identified above. Most, if not all, of them are likely to be mitigated (though not necessarily extinguished) in the coming years as a body of case law and practice develops in the wake of national implementation of the Directive.

29 Cf. Article 2(c) of the Amended proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the Internal Market (COM (1999) 427 final, 17.08.1999). This defines an “established service provider” as someone who “effectively pursues an economic activity using a fixed establishment for an indeterminate duration”, and also stipulates that the “use of the technical means and technologies required to provide the service does not constitute an establishment”.

30 For a plausible scenario demonstrating such problems, see Benno, The “anonymisation” of the transaction and its impact on legal problems, The IT Law Observatory Report 6/98 (Stockholm, 1998), p. 16.

31 See especially Art. 28(6) of the Directive.
In this section, attention is devoted to what are arguably the two major problems; that of regulatory overreaching and that of data subjects having to cope with foreign legal systems.

Regarding the first-mentioned problem, it has been suggested by some commentators that the possibility of regulatory overreaching could be reduced if Art. 4(1)(c) is read down such that its application is limited to two situations:

1. where the controller attempts to circumvent the law of an EU Member State by relocating his/her/its establishment to a third country (but still uses means situated in the EU);

2. where the controller him-/her-/itself (who is located in a third country) transmits data to a third country for further processing (again using means situated in the EU).\(^{32}\)

All in all, the above proposal seems to be a sensible solution. Although it is by no means certain that implementing the proposal would cut out all possibilities of regulatory overreaching, these possibilities would be reduced significantly.\(^{33}\)

Turning now to the second major problem, this could be remedied if applicable law were to be made the law of the State in which a data subject has his/her domicile. Such a rule would parallel existing European rules on jurisdiction and choice of law in the case of consumer contracts.\(^ {34}\)

Given the problems for data subjects in seeking remedies under foreign law, it is somewhat surprising that no consideration has been expressly given in the travaux préparatoires to the Directive for applying such a rule. The adoption of such a rule has been championed by some scholars,\(^ {35}\) and it deserves serious consideration, particularly in light of the close relationship between the concerns of data protection law and consumer protection.

No doubt, the drafters of the Directive refrained from adopting such a rule because it would ostensibly require data controllers to familiarise themselves with, and take into account, a multiplicity of national data protection laws. Nevertheless, one is entitled to ask:

(i) do these problems for data controllers outweigh the problems identified above for data subjects, especially in light of the increasing difficulties in identifying and defining the parameters of electronic (particularly online) transactions?\(^ {36}\)

(ii) what is the rationale for the discrepancy between the criteria for applicable law adopted in the field of data protection and the equivalent criteria adopted in the field of consumer protection?

---


\(^{33}\) As Terwangne and Louveaux correctly point out (id.), another advantage of the proposal is that the second of the two listed situations falls outside the rules of Arts. 25 and 26 of the Directive; hence, a gap in protection would arise if that situation were not covered by Art. 4(1)(c).


\(^{35}\) See e.g. Rigaux, “La loi applicable à la protection des individues à l’égard du traitement automatisé des données à caractère personnel” (1980) 69 Revue critique de Droit International Privé, p. 443 et seq; Benno, supra n. 30, p. 17 et seq.

\(^{36}\) Further to this point, see Benno, supra n. 30, p. 17 et seq.
(iii) again, is this rationale justified in light of the emerging realities of electronic transactions?

These questions deserve to be subjected to serious consideration by policy makers.

A possible compromise solution, which has been suggested by at least one commentator, is to adopt a qualified version of the data subject domicility criterion. This would stipulate that the data protection law of the country in which a data subject is domiciled will apply if the data controller should have reasonably expected that his/her/its processing of data on the data subject would have a potentially detrimental impact on the latter. On its face, such a rule seems attractive, though arguably it probably would not significantly lighten the burdens of data controllers. Nevertheless, the viability and practical implications of such a rule deserve further study.

---

37 Id.