Data Protection in the Private Sector

Peter Blume

1	**Human Rights**	298
2	**Reasons to Regulate the Private Sector**	298
3	**The Purpose of Data Protection**	300
4	**Increased Interest**	302
5	**What Data Should Be Protected?**	303
6	**The Individual as Controller**	304
7	**Data as a Commodity**	306
8	**Marketing**	307
9	**Groups of Companies**	309
10	**Personal Identity Numbers**	312
11	**Surveillance**	313
12	**Actual Data Protection**	316
13	**The Future**	317

1 Human Rights

Data protection forms a part of the general protection of privacy as for example stated in article 8 of The European Convention on Human Rights. Data protection, or information privacy as we know it today, has evolved due to modern computer technology and was accordingly not at the center of attention when the basic right to privacy was originally determined.[1] Privacy concerns many different aspects and may broadly be divided into physical and psychological privacy. Data protection refers to the last mentioned although the division between the different aspects is not unambiguous. As an example, surveillance will in many cases affect both kinds of privacy. These may also be subdivided e.g. concerning communicational and territorial privacy. In any case the concept of privacy from a European perspective is a natural starting point when a legal protection of personal data is considered.

This is in particular interesting and maybe also surprising when the regulation of the private sector is considered. Traditionally human rights, including privacy, have been focused on the relationship between citizens and state. The purpose has been to protect citizens against different kinds of state abuse and this has mainly been achieved by stating negative rights. The rules determine what the state may not do. The object of regulation has accordingly been treatment of personal data in the public sector while human rights traditionally have not been seen as relevant with respect to data processing in the private sector, i.e. the relationship individual - corporation. This distinction between the two sectors is not quite as evident today. It has been recognized that human rights to some degree have a horizontal effect implying that for example a private enterprise can violate an individual's right to privacy. As a starting point the state has an obligation to ensure that this is not the case by making human rights positive. Even though it is not absolutely clear how far-reaching this obligation is and how it may be enforced, the important assumption seen from a data protection perspective is that human rights are relevant with respect to all parts of society. This is in some ways not a surprise as all European data protection statutes and directives cover the private sector. Data protection is a primary and in some sense vanguard example of the broad application of human rights.[2]

2 Reasons to Regulate the Private Sector

The close connection to human rights does not in itself explain why it is felicitous to impose data protection rules on the private sector and this is in particular not evident seen in a global perspective. It furthermore does not

1 The "sacred" text of information privacy, Warren, Samuel, Brandeis, Louis, *The Right to Privacy*, 4 Harvard Law Review (1890) p. 193-200, was among other things concerned with modern technology of that time, photography. This article has many different ingredients and it is interesting to note that its main focus is on information privacy issues in the private sector. *See* Blume, Peter, *Databeskyttelsesret (2.udg.)*, Jurist- og Økonomforbundets Forlag, København 2003 p. 25-28.

2 In ordinary human rights discourse this overall feature of data protection is surprisingly often neglected.

provide an answer to the question of whether the level of protection should be the same as in the public sector. This is a basic assumption in current European law. Accordingly, it is necessary to consider the features that make it expedient that data protection covers the private sector and to some extent this is best done by comparing this sector with the public sector. However, even though data protection emerges from the public sector there may be independent reasons sustaining a regulation of the private sector. There is not a necessary link between the two sectors.

As a beginning it may be observed that there is a fundamental difference with respect to the foundation of processing of personal data in the two sectors. In the public sector processing is primary based on statute and legal sources derived from statute. Administrative bodies must have a statutory foundation for their activities. In societies we recognize as democracies it may be argued that the link to statute diminishes the necessity for data protection law and this regulation may to a large extent be perceived as an extension of ordinary administrative law. It can be argued that it is only the close link to modern information technology that has made data protection a special branch of public law. In any case, processing of personal data must have authority in law. In the private sector legal regulation is basically founded on contract. The starting point is freedom of contract implying that individuals are free to agree upon extensive data processing. However, as it is well known total freedom is rarely accepted today as consumer law and competition law illustrate. It is recognized that there is no real equality on the market. Data protection law can sustain equality even though no distinction between strong and weak individuals is actually made in current law.[3] This is the first argument sustaining that there should be a data protection regime covering the private sector.

In general, the reason for processing data is not the same in the two sectors. In the public sector processing is aimed at making it possible for statutory law to function in accordance with its purpose. Statutes are of course very different and some may in themselves be perceived as intrusive with respect to privacy but such assumptions have at this level of analysis to be seen as part of legal policy considerations with no direct consequences with respect to the scope of data protection. Statutes correctly enacted by parliament form the basis of data processing in the public sector. In principle, the single public authority acting as data controller has no self-interest in the actual processing. Another way of phrasing this is to assume that the processing is always based on societal grounds. Viewed in isolation this could favor the view that data protection is not necessary in this sector.[4] There are quite different reasons for data processing in the private sector. First of all there is a commercial interest in processing. Data are commodities. In order to acquire commercial gains in the modern information society it is in a still increasing number of situations necessary that

3 The data subject has not been analyzed in any depth in data protection discourse. There are many different aspects that ought to be taken into account. *See* in this respect Bennett, Colin, Raab, Charles, *The governance of privacy*, Ashgate Publishing, Aldershot 2003, p. 35, 195.

4 The same line of thought may be applied with respect to ordinary administrative law. Data protection ensures that the consideration to information privacy is taken into account in the application of statutory law.

personal data are stored and used. It is not statute but capital that constitutes the background for data processing. In the private sector there is a self-interest in processing implying that there is a temptation to process to a greater extent than may be viewed as reasonable. For this reason a regulation is necessary.

The organization of the two sectors also differs. The public sector is composed by a limited number of central and local government bodies. It is fairly easy to determine who can act as data controllers and thereby to know towards whom data protection obligations should be directed. In contrast, the private sector is diversified and composed of some large enterprises and a huge amount of small firms etc. It is much more difficult to locate the data controllers and it is also difficult to establish a common position as to how the data protection level should be. This situation favors a varied regulation of the private sector but it also makes it clear that such a regulation is a difficult task. Furthermore it should be observed that against this background it is not evident that the rules ought to be the same in both sectors.

It follows from the observations made above that in many ways there are stronger reasons for a specific data protection regulation in the private sector than in the public sector. Tradition is opposite due to the starting point in human rights. However, with respect to the private sector it must always be considered whether the state should intervene and impose conditions concerning how private enterprise may be conducted. General political beliefs favor both positions. However, the development of the information society with the increased importance of personal data sustains together with the reasons mentioned above that the private sector is regulated.

This conclusion is in accordance with long standing European opinion and there has been increasing international understanding for the necessity of such a regulation. However, this does not imply a specific regulation neither with respect to content or scope. These issues are discussed in the following.

3 The Purpose of Data Protection.

Before confronting specific issues it is expedient to consider the purpose of data protection law.[5] Such a consideration is necessary in order to determine how the private sector ought to be regulated with respect to specific questions. Clarifying the purpose is not quite easy because current formal rules do not seem to be quite honest in this respect and tend to promise more than they are willing to deliver.[6] A natural starting point is Directive 95/46 EC[7] that is the basic European legal text determining national acts, including those of the Nordic countries. In article 1 two purposes are stated. These are free flow of personal

5 A distinction between data protection and data protection law may be made. It is feasible that not all the general and ideal ideas sustaining the notion of data protection actually have been taken into account in the legal regulation. Such a dividing line is rarely drawn and whether this is advisable ought to be considered in the future.

6 See in this respect, Blume, Peter, *Behandling af persondata*,(København 2003) p. 8-11 concerning the Danish act.

7 In the rest of the article referred to as the Directive.

data within the Community and protection of basic rights, in particular privacy. One might say, a technical/economic and an ideal purpose. According to the European Court of Justice[8] it is free flow of data that is the determining purpose as the Directive has its authority in article 100A of the Treaty concerning the single market. This assumption implies that at least at the EU level it is mainly economics that have led to an interest in data protection. Although free data flow is relevant in the public sector such flows are in practice mainly of interest in the private sector. According to this understanding of the Directive, information privacy merely seems to be an instrument used in order to make free data flow possible. Privacy serves an economic purpose and this favors the inclusion of the private sector in the legal regulation. Such a narrow and in some sense pragmatic interpretation is possible and the history of the Directive actually makes it quite feasible.

However, maybe free data flow is mainly an internationally oriented aim[9] because in most national acts this purpose is not visible. With the exception of the Danish act, all Nordic acts include a rule on their purpose and none of these mention free flow of data. Their wording differs somewhat but they all center on ideal aspects of privacy. According to these rules the purpose is in particular to protect citizens against violations of personal integrity. Although they have major importance, the economic implications of data protection are not made explicit on this level. This is probably in accordance with the general popular belief as it is often assumed that data protection restricts the possibilities of data processing thereby protecting citizens.

The basic question is whether data protection acts actually protect privacy. In this respect mainly two observations are presented. First, data protection rules almost always concern procedure and normally no kind of processing is totally prohibited. The theme is not the extent but the way in which personal data may be processed. This is a truth with certain modifications in particular in respect to the private sector as some of the rules although not being absolute in practice restrict types of data processing.[10] However, also with respect to such rules the main focus is on procedure and not on extent. A rule that makes processing dependent on data subject consent has this nature. Such a rule may be demanding on the resources of the controller especially with respect to data concerning many data subjects but it does not prevent processing entirely. Furthermore, it should be noticed that consent corresponds with the basic principle of freedom of contract.[11]

Against this background the relationship between data protection rules and other legal regulation becomes interesting. It should in this respect be noticed

---

8 Decision C-101/01 (Lindqvist).

9 This purpose is also decisive in other international instruments such as the 1980 OECD guidelines and the 1981 Council of Europe convention.

10 The rules (Directive article 8) on processing of sensitive data may especially in this sector make processing impossible. A simple example is that as a consequence of the Directive a trade union cannot publish a directory of its members. Consent is possible but in practice impossible.

11 It should be recalled that the basic principles stated in article 6 of the Directive have to be respected even when a valid consent is given.

that both in the Directive and in the national statutes there are close links to other rules that are not concerned with data protection. Such links are often overlooked. The real authority for a certain kind of processing is often found in other legal regulation and this fact often makes it extremely difficult to determine the full extent and impact of data protection regulation.[12] With respect to the theme of this article this relationship should be recalled in the following in connection with the assessment of specific data protection rules. Broadly this section can be concluded with the assumption that the interest of data protection law is procedure, not the volume or extent of data processing. This does not imply that data protection is worthless but that its importance is more limited than normally indicated.

4 Increased Interest

As previously mentioned data protection rules have traditionally been stricter in the public than in the private sector. It has been assumed that data protection should not intervene too much in the practice of private enterprise. As a starting point this is no longer the case in European law as the Directive makes the same rules applicable in both sectors. The basic argument sustaining this approach is that the level of protection ought not to be dependent on the sector the data are being processed. It can be observed that also in other parts of the world there has been an increased interest in regulating the private sector.

There is little doubt that this international development is due to the information society becoming a practical reality. This has meant that the scale of personal data processing in the private sector has increased and become more widespread. Citizens are more aware of the fact that this processing can violate their integrity. In particular the many options of dubious and in some cases concealed processing that the Internet has made possible document that a regulation is necessary. The Internet has enhanced the possibilities of privacy violations. Although few citizens really understand cyberspace they witness how their data are being treated and feel that something should be done about it. As demonstrated by rules on retention and preservation of data in order to combat crime and terrorism the state can also violate privacy through the Internet but it is mainly with respect to the private sector that the Internet has posed a new threat.

It is generally agreed that there has to be a certain level of protection but this does not necessarily imply that this level ought to be the same as in the public sector. It may still be argued that the private sector should be regulated in a special way taking opposing commercial interests into account. There are still many both theoretical and practical problems unsolved but the important starting point is that there is wide-spread agreement as to the necessity of a regulation in the private sector. This is not in dispute today while there are still important legal culture differences with respect to the choice of regulatory method. It is not necessarily statute that should be preferred as self-regulation and contract in some jurisdictions as in the US is seen as a useful alternative.

12 In this connection *see* Blume, Peter, *Databeskyttelsesret og anden ret*, Juristen 2004 p. 28-35.

5 What Data Should Be Protected?

While in principle anybody in the private sector can be a data controller, it is less evident who should be protected by data protection; how should the category data subject be defined. The starting point is simple. Data protection is concerned with information related to physical persons. It is their informational privacy that is protected. It is evident when reading the actual rules that they have been drafted with this perspective in mind. This is the basic rationale of the rules and although there are many disputed details, the protection of the individual is not in doubt. This is what data protection is mainly about.

In particular with respect to the private sector it is often discussed whether the regulation should have a broader scope. It is considered whether data concerning collective entities should also be protected by data protection rules.[13] At the outset it must be emphasized that this is a legal policy issue and there is no correct answer as such. It can be observed that the Directive only covers data on physical persons but it does not exclude that others may be protected under national law. According to the ECJ such a protection is possible provided that it does not violate EU law.[14] It can furthermore be observed that there in some national laws is a limited protection of corporations. This is e.g. the case in Danish law where the data protection act (429/2000) provides such a protection with respect to data processing by credit rating agencies and in the special case when a file or database is used to warn others against entering into business relationships. The former act on private registers (293/1978) in general included data on corporations but was rarely applied in this respect.

There are situations where a corporation, an association, etc. has a legitimate interest in its information being protected.[15] This is not disputed here but the question remains whether such a protection should be included in data protection law or whether it is better placed within other parts of the legal system. There are good reasons to prefer the last mentioned solution. First and foremost there is a risk that the inclusion of collective entities will blur the basic intentions of data protection. The privacy of an individual and of an entity are two different issues. In contrast to collective entities, an individual is generally more vulnerable and can feel shame, guilt, and other human feelings. There is a specific kind of integrity related to human beings and this integrity ought to be protected in a specific way. If there is any strength connected to data protection it is exactly that it is related to physical persons. It can also be observed that the data protection rules are drafted from this perspective and in practice it is often very difficult to apply those rules to collective entities. It could be argued that the rules could be drafted in another way but this is in many cases not possible without changing the actual protection. For example, there is a major difference

13 Under the Directive and national acts data concerning personally owned companies are regarded as personal data. This is not obvious but the issue will not be discussed here. *See* Bygrave, Lee A., *Data Protection Law* (The Hague 2002) p. 211-15.

14 ECJ Lindqvist decision, finding 98.

15 In general *see* Bygrave, Lee, p. 173-282. It is on p. 175 emphasized that account must be taken of other legislation, of practical experience and of whether corporations want such a protection.

between a right of access for an individual and for a corporation. Of importance is also that data protection authorities in general are not well suited to handle issues relating to data on enterprises. They lack the necessary expertise and although this is a practical consideration it points in the same direction. All in all, data protection should be reserved for physical persons.

In current law this means the protection of a specific identified or identifiable person. It may be considered whether the protection ought to be extended to cover groups of persons; e.g. those of a certain race or sexual inclination. The idea is that information concerning the specifics of such a group can be processed, in particular communicated, in such a way that it actually violates the integrity of the individual member of such a group. In this case the arguments against inclusion are not as strong as it is still data related to individuals that are protected. However, it is not certain that data protection is the right kind of protection. Disclosure of data concerning groups will often best be assessed from a freedom of information perspective. Does the information in question lie within or outside the boundaries of this basic right? This will be the typical question and the answer will normally depend on rules within criminal law. It is not answers that data protection authorities are well suited to provide.[16] For this reason it seems best to maintain that data protection only concerns processing of data related to a specific individual. Accordingly, it is protection of the individual and the obligations of data controllers in the private sector that are in focus in the following.

6 The Individual as Controller

Although anybody can be a data controller with the obligations following from the rules, it is expedient to consider whether this starting point should be modified when the controller is an individual acting in that capacity. This is quite a difficult issue. The purpose of data protection is to protect individuals and not to restrict the actions of individuals. However, personal integrity may be violated also by another individual. Violations can occur even though the controller is not a collective entity or a public authority. Against this background it seems reasonable that individuals should conform to the principles of data protection but the problem is how this approach should be implemented in practical law.

In this respect it may initially be observed that the individual as data controller has traditionally been treated in a special way. Sometimes restrictive, sometimes lenient. In the original Danish act (293/1978) on private registers it followed from section 1 that it was unlawful for a private person to establish an electronic file containing personal data. As with respect to other first generation register acts the technological background was central mainframe technology and in this context this rule was not without reason. Technological developments, in particular the personal computer, made this prohibition absurd and it was neither respected nor enforced in practice. Today, the legal situation is

16 These authorities in general have difficulties handling freedom of information issues; see below in 6.

quite different. A private person may process personal data in accordance with the ordinary data protection rules. Although there can be certain practical problems with respect to supervision,[17] this processing is in principle treated in the same way as all other kinds.

However, processing "in the course of a purely personal or household activity" (Directive article 3(2)) is exempted from the ordinary rules. There is no doubt that processing that only occurs within the private sphere is covered by this rule and such an exemption is reasonable. It has been uncertain whether this exemption has a wider scope and also could cover private processing that includes disclosure of personal data. In practice, whether forms of data processing on the Internet could be exempted, e.g. a personal website or participation in chat groups. Such a wider application has been assumed in many countries. In the preliminary remarks to the Danish data protection act (429/2000)[18] it is stated that the fact that data are communicated to a broad and unknown number of recipients does not exclude the application of the exemption. As an example is mentioned a chat group concerned with the abilities of identified athletes. From these remarks follow that also personal websites could be exempted from the act. As mentioned the same line of thought has been followed in other countries.

In general this reading of the law is due to reluctance towards regulating private usage of personal data and furthermore is based on considerations to freedom of information. This last mentioned aspect has gained importance as the ECJ has interpreted the Directive in another way. According to the court,[19] processing is not private when data are disclosed broadly and for this reason personal websites must conform with the ordinary rules. From the outset this is the case regardless of the purpose of the specific home page. The opinion of the court is reasonable as general disclosure of personal data may violate privacy and ought not to be seen as private processing. It is exactly such disclosures that data protection law aims at restricting and if they should be treated in a special way this must be due to other considerations than privacy.

However, this interpretation of the rules does not imply that there are no practical or fundamental problems. The number of personal websites is enormous and it is unlikely that supervisory authorities have the capacity to control such sites. Providing such capacity will not be reasonable. Some websites will, dependent on national regulation, have to be notified or even require a license but it is not likely that such rules will be generally respected. These practical issues do however not differ from those that that are topical within other fields of data protection. In no area is it possible to ensure complete compliance and this should not be seen as decisive. Data protection always has to depend on the willing corporation of controllers and enforcement difficulties are not a decisive argument against a certain regulation although these have to be taken into account.

---

17 To the extent audits can take place in the private sector it is assumed that the Data Protection Agency may inspect private homes. In practice this has not been done in Denmark.

18 Folketingstidende 1999-2000 Tillæg A p. 4058.

19 Lindqvist decision finding 47.

Much more disturbing are the consequences with respect to freedom of information. As it is well known, there is a classic conflict between freedom of information and privacy and a general necessity to balance these two fundamental rights. This conflict has been intensified by the Internet due to the fact that an increasing amount of personal data are being disclosed. This is a significant development that shifts the focus of data protection from registration to disclosure. Many citizens will perceive their personal website as an expression of their right to free communication. The homepage is in a sense their newspaper. The question is to which extent data protection should intervene in this freedom. The court does not provide any guidance in this respect as it merely states that it is not the purpose of the Directive to restrict freedom of information.[20] This is neither informative nor helpful and the national supervisory authority has been given no guidance and is in some sense not well suited to strike the balance. There does not exist any precise guideline that determines how specific websites should be assessed and this fact is likely to lead to a diverging practice within the EEA countries.

In Danish law, section 2(2) of the Act states that the data protection rules must not be used in contradiction to article 10 of the ECHR and in probably all democratic countries it is assumed that freedom of information as a political right is more important than privacy as an individual right. This could imply that if the website contains information of societal or democratic interest then personal data may be disclosed.[21] In specific cases it must determined whether the personal data has this nature. Although such an assessment will only be necessary in doubtful situations, such cases will pose a major challenge for the supervisory authorities in the future.

The Internet has generally meant that the ability to communicate data has been made more democratic. There is no longer a mass media monopoly. From the outset, this development should be viewed positively as it increases freedom. Challenges to privacy are created but they should not be exaggerated. The individual citizen is today an important data controller and this increases both the importance and the consequences of data protection.

7 Data as a Commodity

One of the main reasons for personal data processing in the private sector is commercial. Information has always represented value and in the information society this aspect has become much more evident. The possession of and the ability to use personal data is not just an economic asset but also a necessity for probably most corporations. Data symbolize both money and wealth. Personal data are furthermore a commodity that can be traded and such a trade is taking place especially on the Internet. In this environment goods and services are given away "freely" in exchange for personal data or acceptance of kinds of surveillance as for example the installment of spyware.

---

20 ECJ Lindqvist decision finding no.90.

21 *See* on this issue *Databeskyttelsesret* p.137-43.

In this respect it has been considered whether personal data should be viewed as property and whether data can be owned. In US legal discourse this is a question that has led to much controversy.[22] This is not an issue that data protection laws take into account and there are no rules on ownership. In order to achieve the mainly procedural purpose of current data protection laws it is not necessary to address this question. The Directive and statute law is neutral. However, the widespread application of consent may be understood as a certain accept of such an approach. When the data subject gives his consent then his data may be processed. Viewing personal data as property may seem tempting but the practical consequences of such an approach are uncertain. Furthermore this idea favors the strong citizens who are able to treat their property in a reasonable way. There is a risk of lack of control due to the fact that personal data have no fixed form. A full discussion is not necessary in this context. It is sufficient to observe that the notion of personal data as property underscores the economic implications of data protection law.

8 Marketing

A principal commercial interest concerns the possibility of utilizing personal data for marketing purposes. Today it is just as important for a corporation to have efficient marketing as it is to have a good product or service. In many situations marketing is more important than the product. The purpose of marketing is to convince the consumer that he should purchase a product. The basic problem for a corporation is how to achieve this goal. Personal data and knowledge of the individual consumer's interests are very important in this respect. Processing for marketing purposes has resulted in a complex regulation based upon the assumption that some consumers are opposed to their data being used for this purpose. There is much disagreement as to how restrictive this regulation ought to be, in other words whether certain forms of processing should be prohibited while others should presuppose consent (opt in) or just no objection from the data subject (opt out).

Before considering these options and briefly describing the current regulation it is expedient to consider to which extent this kind of processing constitutes a data protection issue or whether these issues ought to be confined to consumer law. If there is a privacy issue another question is whether it is serious. It seems possible to argue that marketing only to a minor extent influences privacy. Marketing does not imply a decision towards the individual and he or she can freely decide in which way a marketing approach should be received. There is no obligation to buy and although certain kinds of marketing can be a nuisance they can be neglected. From this line of thought follows that the privacy issue in general is not serious. However, such an issue exists. Personal data are being processed and it is evident that many individuals feel that this should only be the case if they agree or at least have a possibility to opt out. It may also be observed that processing in practice often is carried out in ways that make consumers feel

22 *See* Samuelson, Pamela, *Privacy as intellectual property*, 52 Standford Law Review (2000) p. 1125-1173.

insecure and sometimes the data processing is concealed. For such reasons data protection must play a role.
From the outset there is a privacy issue but not a serious one. This kind of processing does not fall within the core of information privacy. As will become evident in the following this assumption is not proportionate with the extensive legal regulation which has been put in place. A reason for this may be that the problems relating to marketing from the outset are fairly easy to understand and that in contrast to many other issues a comprehensive data protection regulation can be developed. Legislators can argue that data protection law makes a difference. It may be difficult to enforce this regulation but it demonstrates a will to protect data subjects in their capacity as consumers.

The modest starting point is article 14b of the Directive. According to this rule a data subject has a right of objection with respect to this kind of processing and it is presupposed that it is possible to use this right. Before the enactment of the Directive there was a major policy debate concerning whether an opt in or opt out regulation should be preferred and opt out was chosen. However, national law in some countries is more restrictive and there has been a general tendency to prefer opt in. Directive 02/58 supplements the general rule and article 13 with a minor exemption in subsection 2 employs opt in with respect to e-mail marketing (Spam).

In the following the complex Danish regulation will be outlined.[23] This regulation is split between the data protection act and the marketing act (699/2000). A common starting point is that the controller must lawfully be in possession of the data that sustains marketing. Whether this is the case depends on the ordinary data protection rules. The marketing act, section 6a, concerns itself with the relationship between corporation and consumer. There must be prior consent with respect to marketing using e-mail, fax and telephone while ordinary off line marketing is governed by the opt out model. In this respect it provides a possibility of a general opt out[24] which in many ways is necessary in order to make such a model efficient. The rules in the data protection act, sections 6(2-4) and 36 concern disclosure of data with the purpose of marketing.[25] They apply both opt in and opt out. A distinction is made between marketing based on specific and on general knowledge of previous consumer behavior. If the data are specific, i.e. exactly concern what has previously been bought, e.g. red wine of a specific kind, such data can only be disclosed with consent. This is also the case when the data are sensitive, e.g. huge amounts of red wine. Data of a more general nature, e.g. just red wine, may be disclosed provided that the data subject does not object. A right of objection presupposes that this is a real option and this is the purpose of section 36 that provides a possibility of filing a general objection and also states detailed rules concerning individual objections. In this case the controller has to inform the data subject of

23 *See Behandling af persondata* p. 95-105.

24 A consumer can register an objection in the Central Persons File on a so-called Robinson-list and corporations have to consult this list every third month. As mentioned below this possibility also exists with respect to the opt out rules in the data protection act. In this case the list must be consulted each time data are being processed.

25 The same rules apply to marketing on behalf of another company.

the intended disclosure making it possible to object within 14 days of this information. It must be made easy for the data subject to object. It is worth noticing that this information cannot be given by electronic mail implying that disclosure with respect to e-commerce always presupposes consent.[26] The described regulation only applies when corporations are processing the data. In other cases, e.g. associations, public authorities, the ordinary data protection rules apply.[27]

In general corporations perceive the Danish regulation as very restrictive. This regulation views processing of personal data with respect to marketing as an intrusive procedure and provides data subjects with strong rights. Compared with more fundamental privacy issues such as data matching the regulation is comprehensive and restrictive but there is no doubt that the rules have both political and popular support. Seen under the corporation perspective an opt out regulation is preferable but as mentioned above opt in is gaining ground in many legal systems and it is not likely that the Danish regulation will be become less demanding in the future.

Data processing for marketing purposes has general interest as it illustrates the individualistic nature of data protection.[28] Some data subjects view such processing as infringing while others have no fears. There is no common demarcation of what privacy is. There might be general agreement as to the private nature of those data that have been categorized as sensitive but even in this respect all data types included in article 8 of the Directive are not viewed in the same way by data subjects.[29] This observation can sustain the general position that processing is made dependent on the decision of the individual as in the case of marketing but in many other areas this is a fragile road to travel as it leaves many data subjects in a vulnerable situation. Data protection may become unbalanced. The individualistic character of data protection will be further illustrated below in particular with respect to PINs and surveillance.

With respect to marketing it may be concluded that the legal regulation is well developed and provides protection to those citizens who feel that their privacy is violated. However, it should also be observed that these rules are not always adhered to in practice and in particular that the international nature of e-marketing makes it very difficult for data protection agencies and other authorities to make enforcement efficient.

9 Groups of Companies

Personal data are used for many other purposes than marketing and are in general essential for corporations. It is not the purpose of data protection to

---

26 This is due to the fact that the corporation only possesses the e-mail address.

27 *See* for an example *Datatilsynets Årsberetning 2000* p. 41-42. The association for the elderly (Ældresagen) could use its data on members promoting an offer for cheap travels as this is in accordance with the purpose of being a member.

28 According to Bennett and Raab p. 17 this is the reason why data protection regulation is procedural.

29 This is in particular the case with respect to data on trade union membership.

impose obstacles on business as its rules exclusively aim at ensuring that personal data are not used in ways that violate personal integrity. This starting point is important when considering corporate use of data concerning employees and customers. There are several issues that could be discussed in this context but here focus is upon the issues that are related to groups or families of companies. As it is well known, many corporations are linked to other corporations as this is necessary in order to have sufficient size and strength in the market. Many of these corporate families are international.

The legal issue is how data processing should be viewed in this context.[30] This issue has both practical and theoretical interest. The general problem is whether the corporate structure, dependent on a choice between legal business models, should have consequences with respect to the possibilities of processing personal data. Should a family of corporations be treated in another way than an unified corporation. At the outset there does not seem to be any reason for making a difference. The level of protection and its implementation ought to be the same and the choice of corporate model should not influence this protection. This legal policy statement is however not in accordance with current regulation and has actually never been. The practical issue concerns flows of data and the ability of utilizing data within the single family of corporations.

The ability of data processing depends on how a corporate family is viewed in data protection law. In Danish law as well in many other legal systems each corporation in a family is seen as an independent corporation. Each company is data controller with respect to the personal data it processes. The data cannot be shared freely within the family implying that delivery of data from one company to another is categorized as disclosure. In contrast, within a single company processing is seen as internal usage.

This difference has legal consequences although one might think that this was not the case. According to the Directive and the transposing national acts all kinds of processing are treated in the same way and have to be accordance with the general principles (article 6) and fulfill the conditions of processing (articles 7 and 8). However, regardless of the uniform text different kinds of processing are treated differently as it is recognized that their ability to infringe integrity differs.[31] Disclosure that includes communication of data is normally seen as especially risky and must accordingly in practice fulfill stronger conditions than e.g. internal use. This is a reasonable line of thought and in most cases it sustains an adequate level of protection. However, in this situation it implies that the choice of corporate structure has serious consequences with respect to the ability to process personal data.

According to Danish law these consequences depend upon the precise nature of the data and the purpose of processing. It is recognized that one of the reasons for establishment of a corporate family is to achieve a synergy effect with respect to the total amount of data. This is part of the economic rationale. Data protection should only modify this aspiration when this is evidently necessary. When the purpose of processing is solely administrative then data can be

30 *See Databeskyttelsesret* p. 195-199.

31 *See* Blume, Peter, *Behandlingsbegrebet i databeskyttelsesretten,* Ugeskrift for Retsvæsen 2000 p. 425-30.

matched. This is also the case with respect to sensitive data as such data especially concerning employees often will be stored in a central database. However, this does not imply that everybody within the corporate family may access these data. The economic benefits can be achieved without allowing a general access. It is technical and not organizational matching that is acceptable from the current data protection perspective. This means that it is still only the single corporation that can access the data as a kind of internal processing. In other cases disclosure must have authority. This is even more evident with respect to customer data. Joining corporations together in a family does not establish improved possibilities of using data for marketing purposes.[32] For this reason it is often corporate families that are most skeptical towards the marketing rules. In some situations, i.e. mainly financial institutions, sectoral legislation makes a somewhat broader access to the data possible but this is due to the special obligations of such institutions and in particular to the fact that strict rules on confidentiality apply. All in all families of companies do not have a special position on the national level.

Another question concerns the possibilities of transfer of data.[33] In many cases corporations are located in different countries and need to have smooth possibilities of transferring data. In particular, usage of intranets are seen as desirable. Transfer can only take place if it is in accordance with the ordinary rules (Directive article 25 and 26). Restrictions on transfers have often been criticized and it is still not certain how best to create a framework that allows a corporate policy to constitute the authority for such transfers.[34] Such a policy must have some binding force and accordingly be within a framework recognized by the European Commission. The policy must therefore be in accordance with the common data protection principles. Even when such a framework has been established it is still a basic condition that a transfer represents a lawful processing seen from the national perspective. The framework only concerns the additional conditions. When this is taken into account we are more or less back to square one. The problems with respect to transfers are primarily due to national law. As long as communication of data within a group of companies is perceived as disclosure there are very limited possibilities of (lawful) transfer.[35]

Against this background the legal policy question is whether an acceptable level of data protection can be achieved without the segmentation of the corporate family. The question is whether it is really necessary to view processing as disclosure. From the outset modifications seem reasonable but this, however, depends on whether transparent data processing can be achieved.

---

32 On this issue *see Datatilsynets Årsberetning 2001* p. 31-33 (financial corporations).

33 The general questions with respect to transborder data flows and the diverging attitudes in different countries are not discussed in this article. However, it ought to be mentioned that this is a major issue that is not sufficiently solved in current law. In this respect see *Databeskyttelsesret* kapitel 8.

34 *See* in this respect Article 29 Data Protection Working Group Opinion 8/2003 *on the draft standard contractual clauses submitted by a group of business associations ("the alternative model contract").*

35 With respect to data concerning employees the employment contract may provide authority.

The basic problem is that it is very difficult for the data subject to know how his data are being treated. A corporate family is often not transparent. The solution may therefore be acceptance of increased cross corporation usage on the condition that extensive informational obligations apply. Thorough information combined with a possibility for data subjects of opting out might make it feasible to accept such transfers of data. Processing of personal data has a price and if paid it should be possible. This is not the place to outline all the details and they will need careful consideration but a solution along these lines may bring data protection more in accordance with modern business without sacrificing personal integrity.

10 Personal Identity Numbers

Today, data processing and surveillance are closely connected. This is the case as well in the public as in the private sector. In the following different issues are discussed starting with the traditional question of personal identification numbers (PINs).[36] All Nordic countries have a personal identity number and the actual existence of such a number is not discussed often today. It is recognized that a PIN-system is one of the foundations of an orderly society. However, this does not mean that there are no problems and especially in the private sector it is still debated to what extent this number ought to be used. As the identity number furthermore illustrates certain general features of data protection it should still be kept on the legal policy agenda.

The Directive article 8(7) leaves it to national law how such numbers should be regulated. There is no common European position due to the fact that not all member countries have such a number that may be defined as an identifier that can be used within all areas of society and for all purposes. In Danish as in other national law there has been a tendency towards liberalizing the conditions of processing but before outlining these rules some general features of the identity number are highlighted.

The personal data contained in the (Danish) personal identity number are trivial in the sense that they only provide information on age and gender. This is ordinary data that most data subjects are willing to share with anybody. It is not the data that give cause to alarm. Those data subjects who are critical towards the identity number or even are scared of it are concerned with the functionality of the number. It provides an unambiguous identification of each citizen and thereby makes it possible to combine and match data. In this way profiles can be established and these may be used for surveillance purposes. The citizen is more transparent than he was before the number was introduced.

In many ways it is reasonable to be cautious with respect to the identity number but it is interesting to observe that this attitude is not shared by all data subjects. There are very big differences with respect to how the identity number is viewed. Some see it as trivial information and an expedient instrument to prevent identity theft[37] while others view it as a tool for major privacy invasions.

36 The issue seen from a Danish perspective is discussed in *Databeskyttelsesret* p.202-08.

37 In practice this can still take place. It is common that Danish newspapers during the low news

These divergencies are in themselves interesting as they once again illustrate the individualistic nature of data protection. There is not in all cases a common opinion as to what data are private and this actually makes it difficult to draft the legal rules. With respect to the identity number the legislator has no clear guidance and to a large degree has a free hand.

The basic problems concern the private sector as it is not from the outset obvious that companies should be able to process identity numbers. Originally, there were limited possibilities but this has changed in current law. According to section 11 of the Danish data protection act, numbers can be processed with consent or in situations where a company performs tasks on behalf of public authorities, e.g. tax collection. It has been debated whether it is acceptable that consent can sustain processing but in practice this has not created new problems compared with the situation before the act. It can be observed that the personal identity number is widely used in the private sector but also that this does not seem to have led to increased surveillance. As it is well known there is widespread profiling with respect to marketing but these profiles are rarely based upon the identity number. Modern information technology can utilize other methods. However, it should not be disregarded that there is a potential for surveillance and the old fear of PINs can still come true. There exists a lot of personal information that easily can be traced due to the existence of the number.[38] In this respect it is interesting and somewhat disturbing to notice that the fight against terror has made new countries interested in applying PINs thereby increasing the traditional fear of surveillance.

11 Surveillance

Other forms of surveillance attract the main attention. The Internet as an open information framework has not only created new freedom but has also developed into a field of surveillance and control. Technological phenomena such as datamining, cookies and spyware are commonly used. In particular with respect to the workplace, surveillance of e- mail and net usage have been widely debated. Many different phenomena could accordingly be discussed. In the following focus is on CCTV surveillance in respect to openly accessible areas. CCTV surveillance in private homes or in workplaces is not included thereby bypassing several special questions. CCTV has been chosen as it represents one of the more developed kinds of surveillance in the private sector. This kind of surveillance concerns both classic forms of privacy and data protection. It is related both to the physical behavior of citizens and their data.

CCTV surveillance has gained increased momentum in recent years. This has been most widely employed in England and it has been estimated that there are 2.5 million cameras in this country and that a citizen in London will be watched on average 300 times a day. England still represents a special case but usage of

period of summer demonstrate that it is easy using another persons PIN and thereby acquiring even very sensitive data.

38 A feature of the rules on data security is that the PIN must not be applied as the sole point of access to stored data. Unfortunately, this is not always respected in practice.

video surveillance has become prominent in most European countries. A survey published in the beginning of 2004 indicated that there are more than 100,000 cameras in a small country like Denmark. The national regulatory framework differs but the factual consequences are more or less the same in all countries. There are fewer places where citizens can be private and the risk of abuse of personal data has increased. In the private sector it is not Big Brother who is watching but in increasing numbers a lot of small brothers and sisters. The threat to privacy is in many ways acute.

The following observations are based on Danish law.[39] Besides the data protection act there is a special statute on the prohibition of TV-surveillance (no.76/2000). This is an act that promises more than it delivers. It chiefly aims at regulating use of surveillance in the private sector and prohibits such surveillance in spaces that are freely accessible or in legal terms places where the traffic code applies. There are only very few exemptions from this principle. However, surveillance may be carried out elsewhere, in particular in shops, malls, banks, petrol stations, etc. This is taking place with increased intensity and still more efficiently as digital technology has been much improved and also has become cheaper and easier to use. The surveillance of today only slightly resembles the surveillance of yesterday. The surveillance act permits this practice when general information is provided. It is only mandatory to inform citizens that an area is under surveillance while it is not necessary to provide information on why this is being done or which parts of an area actually are being surveilled. Cameras do not have to be visible. There is very limited transparency and it is difficult to escape the impersonal eye that is watching. The surveillance act is not concerned with the data resulting from the surveillance. These data do not have to be personal but modern technology combined with face recognition systems entail that personal data increasingly are being processed.

This development has meant that it has become more important to consider how the relationship between the two acts is and more accurately than previously to determine Danish law.[40] As a starting point there is no doubt that surveillance of personal data constitutes processing covered by the data protection act. Surveillance may be perceived as collection. In this respect there are two main issues. First, whether surveillance without recording is regulated by the data protection act or whether such processing only has to fulfill the conditions under the surveillance act. The problem is whether this collection is too temporary to be subjected to the conditions of the data protection act. Although all activities in principle are included in the definition of processing, such surveillance is probably exempted from the act. The consideration to privacy has to be fulfilled by employing general forms of information. The second question concerns whether analogue surveillance is covered. While this for some time was doubtful it is today assumed that to the extent that the act

39 For more details *see Databeskyttelsesret* p. 301-11.

40 On this issue *see* Lind, Martin Gräs, *Persondataloven og lov om tv-overvågning – gennemtænkt samspil*, Rettid 2003 “www.rettid.dk”.

covers analogue processing,[41] this kind of surveillance is covered provided that recordings are being made.

The primary issues concern digital surveillance with recordings and this is also increasingly the applied method. It may be assumed that such surveillance is lawful when acceptable under the surveillance act and that the data protection rules merely impose further obligations on the controllers. The main problem in connection with this line of thought concerns the question of information where the data protection act (sections 28 and 29) together with the Directive (articles 10 and 11) impose greater demands than the surveillance act. According to these rules a data subject must be informed of the identity of the controller and the purpose of processing together with other relevant information. In Danish practice it is assumed that these rules apply but whether they impose greater demands than the surveillance act depend on whether exemptions can be made and this again depends on which kind of collection is taking place. A distinction between direct and indirect collection is made. If collection is indirect there are further possibilities of exemptions, in particular in situations in which providing information is in practice very difficult for the controller. From the outset it would seem obvious that taking a picture of a data subject constitutes a direct collection. There is no one between the subject and the controller and the data come directly from the data subject. However, this is not the opinion of the Danish data protection agency.[42] Collection is seen as indirect and this assumption is sustained by the argument that the data subject does not actively participate in the collection. One might suspect that this position has been taken in order to make it possible to use the exemption. The practical consequence is that (identified) customers and other "ordinary" citizens do not have to be informed while the exemption does not apply to employees who are well known by the controller.

Although many data subjects do not have a right of information there are other rights, including the right of access. In normal circumstances the different exemptions from this right will not apply entailing that it is necessary to consider whether access is at all possible. A video recording will in most cases contain data on many identifiable persons and access only gives a right of knowledge of data concerning the individual data subject. The question is whether the controller can or should be obliged to edit the recording in order to provide access. This would be a demanding burden for the controller but it may be argued that editing is not necessary in order to provide access. The data subject must be informed of the data being processed but this does not necessarily imply that the actual processing is provided.[43] This result is not certain as it may be argued that access without viewing the recording will be misleading. The issue is difficult due to the fact that data protection rules have been drafted from the perspective of textual data processing. The right to access with respect to CCTV seems to be unsolved in current law.

---

41 Manual files and systematic manual processing (section 1(2)) are included.

42 *Datatilsynets Årsberetning 2002* p. 63-68.

43 Access to public administration files provides the data subject with a right to be informed of the data being processed and is not a right to have the file delivered.

Another interesting question concerns when recordings can be stored and to which ends they can be used. In order to answer this question it is expedient to focus upon the purpose of surveillance. There can be different purposes but the most common concerns the detection and prevention of different types of crime. Video surveillance provides security. This is the basic mantra. It follows from the principle of secondary use (Directive article 6(1b)) that the purpose creates a limit as to what data may be processed for. Data may not be processed with respect to purposes that are incompatible with the purpose of collection. This is the basic starting point. Additionally it has to be considered which kinds of data are being processed. It could seem tempting to assume that these data are sensitive as they concern criminal offences.[44] The restrictive conditions for processing such data without consent must accordingly be met. Against this background it could be assumed that only such data may be stored and only when this is legally possible. Such a state of law would in practice lead to a situation where only few recordings could be stored and, when possible, such recordings would have to be edited in order to delete irrelevant data (Directive article 6(1c)). However, as probably in most countries current Danish law is much more lenient. The purpose specification principle is upheld but recorded data are not considered as sensitive. From this perspective, it is the actual data and not the purpose of processing that determine the nature of processing. These data will rarely be sensitive. This is not obvious and may once again be perceived as a pragmatic approach. It sustains a practice which makes it permissible to store recordings for a limited time.

There are many other problems attached to video surveillance but those mentioned illustrate that it is difficult to apply the ordinary data protection rules in this area. As mentioned above, data protection law is to a large extent drafted in respect to textual data processing and it is often difficult to apply the rules to other forms. If a balanced approach is preferred it must be recognized that the basic principles have to be applied in a specific way in order to ensure adequate protection with respect to different kinds of technology.[45] Video surveillance is spreading all over Europe and the current legal framework is not satisfactory. It ought to be considered whether a specific directive could form the basis for a more consistent regulation before the factual situation constitutes such a fait acompli that only little can be done. This might already be the case and if not there is not much time left.

12 Actual Data Protection

In the previous sections different aspects of data protection in the private sector have been outlined. There is a need for such a protection and the issues that

44 According to article 8(1) of the Directive these data are not sensitive but in national law they are categorized in this way. In order not to contradict the Directive they have in Danish law been placed in a special category (section 8 of the data protection act) but are in practice rightly treated as sensitive.

45 This seems also to be the case in countries like Norway where rules on video surveillance are included in the data protection act (chapter seven).

have to be dealt with are very diverse. Against this background it is necessary to consider how actual data protection is achieved. It is not sufficient to enact fine legal rules if they are not respected in practice and it is a well-known criticism of data protection that this is actually the case. Whether this is a correct description of the current situation is uncertain. To my knowledge there are no surveys that document to which extent data protection rules are complied with but regardless of this fact it does seem likely that they are not observed in many situations. This is probably in particular a problem in the private sector.[46]

It is accordingly important to consider how this situation can be improved. In this respect the national data protection agency can play an important role. It is not possible for such an agency to control all processing that takes place and it is also not helpful to impose extensive notification obligations as these rightly will be perceived as bureaucratic measures. It is not by traditional legal measures but as an educator that the agency has its primary role. The objective is to convince controllers that the legal rules are sound and that it is also in their interest to respect them. This is by no means an easy task. There are many different types of private controllers. Some are in principle easy to communicate with and others are more or less out of reach. Communication can have a general form and for example be guidance and explanation of the law. A direct dialogue with one or several controllers is expedient but resources will only make such communication possible in a limited number of cases. Education of controllers can also be an integrated part of actual decisions implying that a pragmatic approach is taken in the sense that a consideration to the interests of the controllers is demonstrated. The majority of data protection rules are drafted in such a way that they may be applied in a flexible manner (legal standards etc.) without sacrificing the fundamental principles of the law. Many methods can be applied[47] but it is often difficult to choose the right one. None of them guarantees success but they all contribute to a situation where controllers follow the law recognizing the societal interests that it sustains.

It is furthermore important to argue that also commercial interests favor respect for data protection. If all controllers follow a practice in accordance with data protection rules then there is no competition in this respect. Such a competition is not a commercial interest. Equal conditions for corporations in the market are a mutual interest.[48] However, there should be no illusions. Many private controllers do not and will not in the future respect data protection. It is a consequence of the information society that personal data have a value and it is accordingly tempting to exploit it as profitable as possible. The best to be hoped for is that a situation can be achieved in which at least vast parts of the private sector respect the regulation.

---

46 In contrast to the public sector there is no administrative law and tradition to fortify data protection law.

47 *See Behandling af persondata* kapitel 6.

48 Concerning the commercial importance of personal data *see* Blume, Peter, *Persondata-beskyttelse i den private sector* , FSRs Forlag, København 1995, p. 22-26.

13 The Future

Looking towards the future there seems to be both positive and negative dimensions. The legal regulation both nationally and on the EU level has increased in recent years. Furthermore, there is a growing international understanding of the necessity of regulating the private sector. There also seems to be certain although not unambiguous popular support for such a development. From the outset most of the legal rules appear to be sound and there are furthermore experienced and competent data protection agencies in many countries. The legal apparatus is in place.

However, there is much uncertainty as many of the rules only with difficulty can function in practice at the same time as it seems likely that they are often not respected. The global dimension, symbolized by the Internet, is the best example of these difficulties. However, it is not just the Internet. Also in the physical world many difficulties have not been solved. The workplace as well as the market place do not always provide an environment that ensures sufficient data protection. There is no doubt that the economic and commercial importance of personal data will increase in the coming years challenging the rationale of data protection.

Concurrent with these developments, a tendency to decrease the general importance of privacy may be observed. Modern technology has changed attitudes and more people are today willing to share their private data with others. The openness and transparency of the on line world create new ways of viewing personal data and this also affects the way in which such data are conceived in the physical world. On line influences off line and this is probably in particular the case in the private sector. Privacy is a societal and historic concept and we may possibly be moving into a period with less privacy and in particular less recognition of privacy. Data protection law should reflect general opinions and attitudes. It must adjust to the times. The general tendencies are not clear and the future is as always uncertain. Data protection may increase and it may decrease. Only one thing seems certain. The near future will present major challenges to data protection law.