SCRIPT-ed

Volume 2, Issue 1, March 2005

The Shape of Things to Come: Swedish Developments on the Protection of Privacy

Rebecca Wong[*]

Abstract

The article highlights the tensions that exist in the protection of privacy online in Sweden following the enactment of the Personal Data Act in 1998. It raises the question whether the Data Protection Directive 95/46/EC is outdated (complementing the Directive on Privacy and Electronic Communications 2002/58/EC) and whether it necessitates a review in the light of current online developments. The problem with dealing with the protection of privacy online as a national solution, such as Sweden does, is that the pervasive application of personal data in the cyberspace environment is a global problem requiring solutions that are not confined within the national borders. This article will consider the Swedish developments and raise the debate about the need for a global dialogue not confined within the European Union, but one that engages other countries such as the United States.

DOI: 10.2966/scrip.020105.98

---

[*] Currently a doctoral researcher at the University of Sheffield, examining the field of data protection and privacy. She also teaches Contract Law, ICT Law and English legal system at the University of Sheffield. This was derived from the original draft into the Swedish position on data protection for which I gratefully acknowledge the assistance of Sőren Őman and Mathias Klang. In addition, I am grateful for comments made by the anonymised reviewer. Views expressed in the article are entirely the author's and do not reflect the views of the institution.

1. Introduction

Sweden was the first country to enact data protection legislation in 1973 (Data Act 1973:289)[1] It has now been replaced by the Swedish Personal Data Act (*Personuppgiftslag*),[2] which was passed in 1998 in order to implement the Data Protection Directive.[3]

The main discussion of this article considers the current proposals to adopt a misuse-orientated approach and amend the PDA 1998. Before discussion of these proposals, the article will begin with a historical background into the main issues arising from the PDA and the reasons for the amendments. In particular, the issue of the freedom of expression and the internet and the transfer of personal data to countries outside the EEA on the internet will be addressed.

It should be stated from the outset that in 2002, Sweden (in conjunction with Austria and the UK) proposed to amend the Data Protection Directive.[4] These proposals included a simplified regulation of the protection for personal data with the insertion of a new article in the DPD[5] to protect against the misuse of personal data. To date, the proposals have not been adopted. However, as alluded, Sweden is now considering whether to adopt a misuse-orientated approach taking into account the DPD and this will be discussed later in the article.

2. Background

Prior to the enactment of the PDA 1998, there were several legislative committees established to reform the data protection regime in Sweden. One particular Committee was established in 1996[6] and chaired by Justice Staffan Vängby.[7] Their tasks were two-fold:

> Create legislation that would replace the Data Act 1973 and implement the DPD.
>
> Review the provisions under Chapter 2 of the Freedom of the Press Act regarding citizens' rights to gain access to public documents.

During this process, the Committee considered two models for data protection. These were the "processing model", which applies to any processing of personal data (which the Directive adopted) and the "misuse model", which applies to certain categories of data that could be misused. This would permit legitimate activities such as word processing and email activities without the possibility of criminal prosecution brought against private individuals.

---

[1] P. Blume. (ed). *Nordic data protection* (2001), at 116.

[2] Abbreviated "PDA" thereafter. See also the Data Inspection Board: Legislation @ http://www.datainspektionen.se/in_english/legislation.shtml.

[3] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) L281/31. "DPD", "Directive", or "Data Protection Directive" will be used throughout the article.

[4] See Department of Constitutional Affairs. "Proposals for Amendment made by Austria, Finland, Sweden and the United Kingdom Explanatory Note" @ http://www.dca.gov.uk/ccpd/dpdamend.htm.

[5] See the Swedish Government, "Misuse model" @ http://www.sweden.gov.se/sb/d/2771/a/15554;_ui9iGpj4, Accessed March 2005.

[6] P. Seipel. "Sweden", in P. Blume (et al), *Nordic Data Protection Law* (2001) 123.

[7] *Ibid.*

In its report published in 1997,[8] the Committee took the view that it would be untimely to adopt a misuse model because of the unease that people may have towards large collections of electronic data relating to themselves. If the misuse model was adopted, it would be questionable whether Sweden could fulfil its international commitments under the DPD. Furthermore, this model would not necessarily comply with Art. 5 of the Directive, which requires member states of the European Union to determine precisely the conditions under which the processing of personal data is lawful.[9] Therefore, the misuse model alternative was rejected and the Committee recommended the processing model akin to the Directive.

Under the second task, review of access to public documents, the Committee proposed that the right of access principle should be based upon the concept of the right to public data in preference to the right of access to public documents. The rationale for this is that if one can obtain access to a document, one should, according to the proposal, have access to the data contained in that document.[10]

The revision of the right to access official documents was, however, passed onto the Committee on Publicity and Secrecy Committee in 1998[11] to examine *inter alia* issues concerning publicity, secrecy, and information technology. Several proposals were made, including the amendment to the Freedom of the Press Act.[12] Suffice to state that the changes to the Freedom of the Press Act were adopted. The Act regulates public access to official documents and under the amendment, it no longer prohibits the public from gaining access to an electronic copy of a document provided that access is prescribed by the Government or Parliament under its own ordinances or Acts of Parliament.

---

[8] Integrity-Publicity-Information Technology, Bilega 7: Summary in English, SOU 1997:39. Grateful acknowledgments to Sőren Oman for providing the English summary to this report.

[9] *Ibid* – a question raised with Elisabeth Wallin from the Data Inspection Board.

[10] Integrity-Publicity-Information Technology, Op. Cit. See also P. Seipel, "Border Technology: its difficulties in a Swedish Perspective" @ http://www.juridicum.su.se/iri/seip/Citraeng.htm, Accessed August 2004.

[11] SOU 2001: 28: Committee on Publicity and Secrecy Committee. See also P.Seipel, *Sweden* In: Blume, P. (ed.) et.al. *Nordic Data Protection*, 2001, p. 123 . The reference of the committee is Dir.1998: 32.

[12] Prop. 2001-02:70. The amendments to the Act were published in SFF 2002:907. Grateful acknowledgments to Mr Őman for providing these details.

Figure 1: Chronology of Legislation

1766 First Swedish Freedom of Press Act – enabled access to the tradition of right of access to official documents.

1960 Swedish Legislative Committee addressed the following issues:[13]

- What principles should guide the keeping and structuring of data?
- How shall it be made possible for the citizens to orient themselves in the available information?
- How much, if anything, should information cost?
- How should information requests be treated when they do not coincide with the interests and wishes of the public authorities?

1972 Swedish Committee on Openness and Secrecy published a report entitled *Data and Privacy Report*, which suggested that computer recordings (data storage?) should be regulated separately.

1973 Data Act enacted

1974 Freedom of the Press Act passed

1980 Swedish Secrecy Act

1997 Data Legislation Committee 1997:39 revises the FPA and "introduces a new concept structure". The basic right of access to "data" was preferred over the definition of access to "documents" so that it is not confined by the physical qualities (or types of media), but rather defined by the "presentation" which has fixed context.

1998 The Committee on Publicity and Secrecy considered the issues of publicity, secrecy and information technology.

1998 Personal Data Act enacted

Several committees were established, after the Data Act 1973 because of the widespread use of data files held on computers. The Committees examined issues such as public access to official documents held in electronic form by public authorities.

[13] P.Siepel. "Borderline technology: its difficulties in a Swedish perspective" @ http://www.juridicum.su.se/iri/seip/Citraeng.htm. Accessed August 2004.

3. The Personal Data Act 1998

When the Personal Data Act was passed in 1998, it was criticized for failing to take into account developments on the internet. Opposition to the PDA was received from several organizations.[14] A subsequent campaign was launched with the slogan "don't touch my internet!", which registered over 40,000 people. In a report published by the Swedish Parliament,[15] a three-tier action plan was proposed[16] with the long-term goal of amending the DPD, so that internet developments were taken into consideration. Seipel summarized the criticisms as follows:[17]

The PDA was a serious threat to the freedom of speech and civil liberties.

The gestation period of the directive and the implementation of the Directive meant that by the time there was legislation transposing the Directive, it was already obsolete. What was required was a national solution (such as the misuse approach) to the problem of internet publication of personal data.

The PDA failed to include exemptions such as harmless data published on web pages and internet search engines.

Palme[18] took the view that if the PDA was applied literally, it would criminalise legitimate activities such as:[19]

- An e-mail message addressed to a recipient outside Europe without the prior permission of the recipient.
- Internet-based discussion forums (except those run by newspapers, since newspapers are exempt from the law) in which any information about a person is mentioned without the permission of that person.
- Publication on the Internet of any scientific paper, which contains lists of references, unless each person in the list of reference has given permission in advance.
- Any criticism of a named person, where that person does not give permission for the criticism. For example, criticism of politicians would not be allowed, a trade union would not be allowed to criticize named employers, etc.

In addition, the Swedish Ministry of Justice, Thomas Bodström took the view that the PDA and the Data Protection Directive was too restrictive. In particular, the definition of data processing was too broad under the PDA to cover activities such as word processing, web publishing and email. The current proposals (to amend the PDA) clarifies this position by stating that applications (such as word processing) not

---

[14] *Ibid*., at 126.

[15] KU 1998/99:15.

[16] See S. Őman "Implementing data protection law" in P. Wahlgren. IT Law, *Scandinavian Studies in Law*, 2004, 47 at 391.

[17] P. Seipel. See note 20 at 126-127.

[18] J. Palme. "The Swedish Personal Register Law"@ http://dsv.su.se/jpalme/society/personal-register-law.html Accessed February 2005.

[19] *Ibid.*

structured to facilitate the retrieval of personal data would only apply, if it causes harm to the individual. However, data structures created for easy retrieval of data would be subject to the PDA 1998.[20] The proposals are discussed later in the article. In the context of the PDA, there are three main issues for analysis:

The scope of the PDA that implements the DPD

Publication of personal details for journalistic purposes

Proposals to adopt a misuse-orientated approach

3.1 Scope

The first issue concerns the scope of the PDA. It is relevant because the main area of contention is whether the publication of personal details on the internet should fall within the scope of the PDA. Although, s 4 – 8 PDA define the scope of the Act, the relevant provision is s 6 of the PDA, which states that:

> *This Act does not apply to such processing of personal data that a natural person performs in the course of activities or a purely private nature.*

The above provision corresponds to Art. 3(2) of the DPD, which does not apply to the processing of personal data carried out by a natural person in the course of a purely personal or household activity. Further guidance can be found in recital 12 of the DPD, which includes personal correspondence and the holding of records of addresses.

One question that has arisen is whether a webpage created by an individual containing a list of names of other individuals could be considered to fall within the exemption for the private processing of personal data? Firstly, a list of people on a webpage would be regarded as personal data under the DPD and PDA, because it is personal data relating to an identified or identifiable natural person. Leaving aside the publication as a "processing" activity under the PDA (which it is), the question is whether publication on the web can be exempted under the PDA? If the literal approach was adopted, then the exemption for private purposes would not apply unless the activities were exclusively personal or domestic.[21]

The Swedish position has applied the Directive literally, so that the consent of each individual should be obtained before placing his or her name on the internet.[22]

It was held in the case of *Lindqvist*,[23]

1. The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies,

---

[20] Privacy and Human Rights 2004: The Kingdom of Sweden@ http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-83530 Accessed February 2005.

[21] Recital 12 of the DPD.

[22] See *Ramsbro* case (293-00) @ http://dsv.su.se/jpalme/society/Ramsbro-HD-domen.html, Accessed November 2004. See also *Lindqvist* decision C-101/01, which reached the European Court of Justice.

[23] C-101/01 OJ C 118 of 21.4.2001. See also M.Klang "Technology, speech, law and ignorance: the state of free speech in Sweden" *Hertfordshire Law Journal* (2003) 1(2) 48 at 56.

> **constitutes the processing of personal data** wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
>
> 2. Such processing of personal data is not covered by any of the exceptions in Article 3(2) of Directive 95/46.[24]

In this case, L had created a webpage, which named various people within a church and listed each of their activities. Although, L had subsequently removed the webpage following concerns that this would infringe the PDA, the case was brought before the Swedish courts and a preliminary ruling was made to the European Court of Justice regarding the application of the PDA (implementing the DPD) to the internet.

What was interesting were the arguments submitted by Sweden and the Netherlands. In the same case, the Swedish Government contended that the dissemination of personal data via the internet cannot be described as 'a purely personal or household activity' in as much as it entails the transmission of that data to an indefinite number of people. Similarly, the Netherlands argued that the DPD was not purely personal or domestic in as much as it implies the dissemination of personal data to an unknown and unlimited number of people. Finally, the European Commission argued in the same case that the publication of personal details on a webpage was not 'a purely personal or household activity because in the first place, a homepage is accessible not only to anyone who knows its address but to anyone using a search engine and in the second place, such activities are by definition concerned only with the private life of the person processing the data.'

It should be borne in mind that if consent has been obtained from the data subject, then the publication of personal data on the internet would not contravene the PDA.

Another question is the nature of a webpage, which may be regarded as private by users online. Why should it matter who can access this? In addressing this issue, Seipel argues that it illustrates the

> *…complications associated with information technology as a 'borderline technology', i.e. a technology that tends to blur dividing lines that have traditionally been relied upon in legal regulation…the fuzzy borderline concerns the private sphere versus the public sphere. Is it really so clear that putting a home page on the Internet must be regarded as a public and not a private activity?*[25]

The question is whether such a distinction is necessary? The idea of the webpage as public or private publication can be further complicated, when access is restricted to a few people (through an intranet). Furthermore, personal webpages may not

---

[24] Art. 3(2) defines the scope of the Data Protection Directive and excludes any processing of personal data for "purely personal or household activity" or those that fall outside the scope of the activities of the Community Law, such as national security etc.

[25] P.Seipel. *Sweden* In P. Blume (ed) *Nordic data protection* (2001) at 131.

necessarily be found through standard search engines such as google (i.e., "deeply embedded" webpages).[26]

Nevertheless, the *Lindqvist* case clarifies the issue of a home page in the context of Art. 3(2). Art. 3(2) only applies to activities that are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people. It, however, leaves the question that individuals may find themselves in breach of the PDA unless there are exemptions provided for the publishing of personal information on the internet. Indeed this has been argued to be a form of censorship[27] by restricting an individual's right to express his or her opinion even if this would include the naming of individuals (with the exception of well-known figures and politicians). It appears that the literal approach adopted by Sweden (to transpose the DPD) has led to some form of restraint by curtailing the freedom of expression on the internet. This leads to the question over the publication of personal information for journalistic purposes.

3.2 Publication of personal details for journalistic purpose

There are a number of factors to consider in this context. The relevant provisions are s 7 and s 33 of the PDA. s 33 of the PDA 1998 corresponds to Art. 9 of the DPD, whereby exemptions are provided for the processing of personal data when it is carried out for journalistic, artistic and literary purposes. According to Seipel,[28] Sweden has adopted a broad interpretation so that it is the form or medium of expression rather than the content or quality of the communication that is considered.

Before examining s 7 of the PDA, it should be stated that although the PDA provides exemptions for the processing of personal data on the grounds of journalistic purpose under s 7 and s 33 (which conforms to Art. 9 of the DPD), it should be remembered that the DPD (on which it is based) does not merely protect privacy. Art. 1 of the DPD provides that 'member states shall protect the **fundamental rights and freedoms** including privacy of natural persons, and in particular their right to privacy with respect to the processing of personal data.' The reference to fundamental rights and freedoms is further expounded in recitals 1 and 10 to allude to the European Convention of Human Rights. The European Convention of Human Rights also provides for the freedom of expression under Art. 10, which states that:

> *1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*

---

[26] With the right search tools and keywords, it is possible that Google can find deeply embedded webpages, but it does not always follow that all deeply embedded webpages can be found on Google.

[27] See M.Klang. See note 24.

[28] *Ibid.*

> *2 The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*

This is relevant because Sweden incorporated the European Convention of Human Rights in 1995.[29] Without going into detail over the issues arising over the legal status of the Convention in Sweden, suffice to state that, although the ECHR has the status of ordinary law to ensure that the Convention is not given constitutional status that may conflict with the Swedish Constitution, a further provision was inserted in 1995, which provides that 'a law or other regulation [sic] may not be issued in conflict with [the Convention].' It has been interpreted to mean that any laws or regulations conflicting with the ECHR would also conflict with the Swedish Constitution.[30]

Returning to Art. 1 of the DPD, the protection of privacy is not absolute and exemptions can be found in the DPD to permit the freedom of expression. The question concerns the extent in which the freedom of expression can be curtailed by the implementation of the DPD and the PDA. Art. 9 of the DPD states that:

> *Member states shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.*

Further guidance is provided under recital 37 of the DPD, which states that

> *Where the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive* ***in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the protection of Human Rights and Fundamental Freedoms.***

In clarifying the individuals' freedom to receive and impart information, the European Court of Justice held in *Lindqvist*,[31] that:

---

[29] See Cameron, I. & M.K. Eriksson. *An introduction to the European Convention of Human Rights*, 2nd ed. (1995) at 124-135.

[30] *Ibid.*, at pp. 130-131.

[31] See note 24.

> *The provisions of Directive 95/46 do not, in themselves, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined inter alia in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome on 4 November 1950. It is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question, including the fundamental rights protected by the Community legal order.*

It raises a broader question over the extent of the exemptions of the PDA and whether the incorporation of the ECHR will ensure that there is a balance between the rights and interests, including Art. 10 of the European Convention of Human Rights.

The first paragraph of s 7 of the PDA state that the provisions of the laws do not apply where they would 'contravene the provisions concerning freedom of the press and freedom of expression contained in the Freedom of the Press Act or the Fundamental Law on Freedom of Expression.'

This is interpreted by Seipel to mean that the provisions of the Act do not apply to the extent that it conflicts with the provisions in the FPA on the freedom of the press or in the FSA on the freedom of speech.[32]

The second paragraph of s 7 of the PDA implements Art. 9 of the DPD to provide for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression. The main area of contention is the interpretation of journalistic and artistic purpose. Can reference to specific individuals and their activities (whether it is for wrongdoing or not) on the internet be justifiable on the grounds of journalistic requirement? The relevant case is *Ramsbro*, whereby R had created a website publishing derogatory statements about Swedish banks and naming individuals who worked for these banks. The aim was to inform and protect people from unscrupulous banks and unethical network-capitalists. The question was whether R had committed a criminal offence under the PDA for transmitting personal data abroad through the web? Could R rely on the exemption (under s 33 PDA) that the website was published for journalistic purposes? The case is particularly important, because the Supreme Court made it clear that the DPD should be interpreted with particular regard to the ECHR.

The Supreme Court held the view that the interpretation of "solely for journalistic purpose" was not restricted to professional journalists or those within the media.

Furthermore, the Court reiterated the view that the basic purpose of journalistic activity was 'to inform, exercise criticism and provoke debate about societal questions that are of larger significance for the general public' irrespective of the fact that it contained derogatory information about named individuals[33] and that R's activity fell within this exemption.[34]

---

[32] P.Seipel. See note 20 at 132.

[33] Though, this does not exempt the individual from liability for potential defamation claims under Swedish law.

[34] *Ibid.*

The Swedish Supreme Court held that the "journalistic exemption" under s 7 of the PDA should be interpreted broadly.

> *The limitation to "solely" journalistic purposes alludes firstly to make clear that a processing of personal data, which takes place in the mass media and by journalists for other than journalistic purposes are outside the limitation. The processing by mass media of personal data, for instance for factoring, advertising or mapping of reader's profiles, thus falls outside the limitation…Any support for an idea that the expression "solely" should be interpreted as meaning that it, independent of the fact that publishing has had journalistic purposes, should be possible, on the basis of the Act on Personal data, to penalise an attack on someone else's good name and reputation cannot be considered to exist.*[35]

Although, the Supreme Court did not make a preliminary ruling on the interpretation of "journalistic purposes" to the European Court of Justice, this clarifies the extent of the exemption to cover the publication of personal data (on the web) on journalistic grounds. Although, this judgment applies to Sweden, it would be of interest to countries implementing the DPD on how far this provision can interpreted in accordance with the DPD. Though, the *Lindqvist* decision is also relevant. It should be added that the role of the internet as a vehicle for information, opinions and debates is also significant in this context.

3.3 Transfer of Personal Data to Third Countries

The second issue concerns the transfer of personal information to countries outside the EEA by the publication of personal data on the web. Can access to a webpage constitute a transfer between the author of the webpage and the recipient in a third country? The relevant provisions are s. 33-34 of the PDA, which corresponds to Arts. 25 and 26 of the Data Protection Directive. These provisions prohibit the transfer of personal data to a third country unless there is an adequate level of protection for personal data. A third country refers to countries outside the EEA that do not have data protection laws that conform to the Data Protection Directive. To date, the European Commission has held that Argentina, Guernsey, Hungary, Isle of Man, Switzerland and Canada (through the PIPEDA) have satisfied these provisions.[36]

One of the major arguments concerning the world wide web is that the internet is a ubiquitous environment, accessible to anybody who has an internet connection. Although, Art. 25 of the DPD was not drafted with the internet in mind. There has been a divergence of opinions concerning this.

Blume raised the following question: Should there be special rules governing the internet?[37] It was acknowledged that the main challenge with the internet is that it can

---

[35] Judgment B239-00 of the Swedish Supreme Court: Unauthorised translation by Bertil Wennergren, former Justice of the Swedish Supreme Administrative Court at 11. Grateful acknowledgements to Mr Őman for providing this.

[36] Europa. "Commission decisions on the adequacy of the protection of personal data in third countries" @ http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm.

[37] Blume, P (ed) (et al.) *Nordic data protection*, 2001, p. 33.

be difficult (on a practical level) to control and supervise the processing of personal data on the net and that personal data can be transferred (even unknowingly by users) through a third country.

Referring again to the case of *Lindqvist*,[38] the European Court of Justice held that:

> *There is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.*

The Swedish position has in the past (prior to *Lindqvist*) been to prosecute individuals who place personal information on the web; holding the view that this constituted the "transfer" of personal data contrary to s 33 of the Personal Data Act 1998. For example, in *Linkőpings Tingsrätt*,[39] the defendant published a list of the names of left-wing activists on the internet.

This constituted a breach of the PDA and a transfer of personal data to third countries under Art. 25 of the DPD, or its corresponding provision under s 33 PDA 1998. The court held that this publication on the internet hindered persons in their political engagement and hindered the freedom of speech of the media.

The current Committee takes the view that there is insufficient guidance from the ECJ regarding the interpretation of "transfer of personal data to third countries," notwithstanding the decision of *Lindqvist*.

The question of transfer of personal data under s 33 of the PDA has been settled by the recent ECJ decision in *Lindqvist*. It held that it would not constitute the transfer of personal data, where an individual in a member state loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another member state, thereby making those data accessible to anyone who connects to the internet, including people in the third country.

However, the judgment of *Lindqvist* further noted that there was the absence of criteria under Chapter IV of the Data Protection Directive that would apply to the internet and more specifically, whether a transfer would be deemed to occur in the place of establishment of the service or at its business address or in the place where the computer(s) constituting the service's infrastructure are located.

One does question whether the rules governing transborder data flows to third countries under Art. 25 should be updated to take account of technological developments such as devices that could be used on computers, such as spyware, that

---

[38] C-101/01 [2004] 1 C.M.L.R. 20.

[39] 2003-08-01, B260-01.

could be implanted into a computer and re-transmitted to countries that do not have adequate levels of protection for personal data.[40]

However, the use of hidden devices such as spyware (which is not defined), but are covered under the recent Directive on Privacy and Electronic Communications 2002/58/EC,[41] which complements the Data Protection Directive. Given the limitations of the article, I will not be considering this.

The other issue regards the enforcement of such provision and the practical difficulties with compelling companies to adhere to the data protection regulations, where they operate outside of the European Economic Area. Irrespective of the potential problems arising from enforcement, this is an issue that should not be neglected.

In the light of the above problems, the question arises on the current proposals to adopt a misuse-orientated approach to the protection of personal information.

4. Personal Data Act Inquiry 2004

The Personal Data Act Inquiry[42] headed by SörenŐman was tasked to review the current Personal Data Act. The review aimed to amend the existing PDA by adopting a misuse-orientated approach taking into account the Data Protection Directive. This would be achieved by utilising the exemptions provided under the DPD to deviate from those provisions (where this was possible) for the processing of personal data in unstructured material.[43]

It should also be stated that the long-term aim of the Swedish Parliament would be to amend the DPD, so that exemptions are provided under the DPD for the processing of personal data in non-structured material, such as word processing and the publication of text on the internet.[44] Therefore, the current proposals should be viewed as a short-term strategy to address the problems arising from the PDA in Sweden.

Under the current proposals, the PDA would not apply to everyday processing such as email correspondence and processing of personal data on the internet ("publication of running text on the internet").

One of the main rationales for the change is that computers today have become a tool for information handling used everyday, by everybody, everywhere, and for everything, and therefore it is not reasonable to apply the traditional, bureaucratic data-protection principles on the person handling the personal data, writing an email

---

[40] There is provision made under the Directive on Privacy and Electronic Communications to obtain consent before such devices are installed, but one questions the practicability of this, given the nature of "spyware" is that it is installed without the user's knowledge.

[41] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L201/37 31.7.2002 @ http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

[42] Swedish Ministry of Justice. "Summary of SOU 2004:6" @ http://www.sweden.gov.se/content/1/c6/01/55/42/24980a18.pdf, Accessed August 2004.

[43] S. Őman. "Implementing Data Protection in Law" *Scandinavian Studies in Law* (2004) 47, 390.

[44] *Ibid.* See also Report KU 1998/99:15.

and so forth. It is premised on the rule that the processing of personal data is not permitted if it involves improper intrusion of personal integrity. The proposals would principally apply to the automated processing of personal data (on a computer).

The main amendments (in brief) are as follows:

Right to subject access – people could obtain a "data extract", including personal data processed subject to the exception that it proves impossible to provide a data extract or would require a disproportionate effort to do so because of the difficulty of ascertaining information about a particular person in running text and in sound and image recordings.

New exemptions (as permitted under the Data Protection Directive) where this is necessary to safeguard the fulfillment of public and governmental functions or to safeguard the protection of rights and freedoms of individuals to be introduced.

Decriminalisation for individuals, who currently may be sentenced to a fine or to prison for infringement of the PDA. Only intentional acts or actions committed through gross negligence will be a criminal offence.

New provisions to clarify the procedures for appealing decisions of public authorities.

The PDA will be amended to provide a clearer reference on the relationship of the PDA to the principles of public access.

If the amendments are accepted, then at the earliest, it could take effect from July 2005.[45] If implemented, the proposed change will clarify the problems arising under the PDA through its implementation of the DPD.

An exemption would be provided under the PDA from the majority of handling regulations for the processing of personal data that does not form part of a set of personal data that has been structured in order to facilitate searches. Furthermore, the proposals (if adopted) would facilitate the publication of personal data on the internet.

However, I want to consider (in brief) the misuse-orientated approach to the handling of personal data.

4.1 Misuse-orientated approach

First, if a misuse-orientated approach is adopted, how is misuse to be defined? There are different perceptions to what constitutes misuse. Should it be interpreted objectively or subjectively? Thus, the criterion for determining "misuse" can be problematic. One person's perception of misuse may be different from another. In addition, what if the handling of the personal data does not result in misuse?

A further argument is that the misuse model does not entirely solve the protection of personal information online. This is particularly the case where large amounts of personal data are collected through "data mining" techniques from various sources.

"Data mining" is defined as 'a class of database applications that look for hidden patterns in a group of data that can be used to predict future behavior. For example,

---

[45] *Ibid.* at 392-398.

data mining software can help retail companies find customers with common interests.'[46]

In his article entitled *Transborder data flow*,[47] Blume refers to the Danish approach; namely, that personal data could be disclosed on the internet, if it legally can be disclosed in another manner. Blume argues that within the framework, the usage of the internet has no specific importance.[48] Although, it was acknowledged that this ignores the problem of obtaining consent from individuals, it takes a pragmatic response to the handling of personal information online.

In a recent report compiled by Korff on the implementation of the DPD, it examined the Data Protection Working Party's response to the protection of personal data. Whilst acknowledging that the internet is not exempt from the requirements of data protection and that the data protection laws apply to the collection, dissemination and use of personal data of on the internet including email addresses and traffic data, the Working Party was also prepared to assist in the development of special rules for the internet, which are based on the requirement of the DPD. Its aim 'was to persuade the main actors and regulators in European Union and elsewhere to agree to the substantive requirements on terms as close as possible to the Directive.'[49]

It is not the purpose to examine the report in detail, but suffice to state that although the DPD applies to the handling of personal data on the internet, it should raises the question over the approach adopted by the current Data Protection Directive and whether it is in need of revision taking into account of other countries' approach to the protection of personal information online.

5. Conclusion

To conclude, the article aimed at examining the effects and undesirable consequences arising from Swedish implementation of the Data Protection Directive. The discussion focused on the enforcement of the Personal Data Act 1998 and the results it would have on the freedom of expression on the internet. Although, the European Court of Justice has given its ruling under the *Lindqvist* case on the application of the Data Protection Directive to the internet, it has raised questions about the strict application of the PDA through the legal proceedings instigated against private individuals (not falling within the realm of private purposes) for publishing personal information of other individuals without their consent.

Furthermore, the decision in *Ramsbro* should be regarded as a triumph for the freedom of expression. It, however, raises the question on whether the case should have reached the courts in the first instance.

---

[46] Webopedia. "Data mining" @ http://www.webopedia.com/TERM/d/data_mining.html.

[47] P. Blume. "Transborder data flow: Is there a solution in sight?" *International Journal of Law and Information Technology* (2000) 8(1) 65 at 83.

[48] *Ibid.*

[49] D. Korff. "Study on Implementation of Data Protection Directive – Comparative Summary of National laws" @ http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf.

Although, the "misuse-orientated" approach is considered by Sweden, other member states of the European Union should also assess the stance adopted by the Data Protection Directive and whether this is in need of amendment in the light of these recent developments.

The Data Protection Directive, if rigidly applied (through implementation of national laws) may have the effect of prohibiting what is regarded as a form of "legitimate activity", as in *Ramsbro*. Further discussion is required at a European level to consider how the Directive can be best approached in the context of internet developments to ensure that the data protection laws are applied consistently throughout the European Union. Countries outside the European Union should also take heed of the potential implications that the *Lindqvist* decision raises and consider whether data privacy laws (whether online or not) adequately address the issues raised in the article.