Online Proactive Disclosure of Personal Data by Public Authorities. A balance between transparency and protection of privacy

PATRICIA JONASON

Sweden is well known for having a generous and well-functioning right of access to information. However, the legal framework, the 250th anniversary of which we have recently celebrated, only provides for reactive disclosure. This is because the Freedom of the Press Act, which regulates the right of access to official documents, only endorses the citizens with the right to access documents after a request been made, and not with the right to access documents that are proactively ”pushed out” by public authorities. This means in turn that the Swedish law only obliges the public authorities to disclose information after the submission of a request, and does not oblige these authorities to disclose information proactively. In practice Swedish public authorities, and not least local authorities, extensively publish information and documents on their websites. The procedure of publishing documents online certainly may constitute a useful tool for increasing transparency of the administration and improving public participation in public life[1], but the method may also have negative consequences. Indeed, when the information the public authorities make accessible on their websites contains elements of personal character, online disclosure may cause infringements of privacy. These risks of infringements that disclosure of personal information on the websites of public authorities can lead to, are exacerbated by the characteristics of the Internet and the possibilities of processing data offered by Cyberspace technology. The disclosure of data on the Internet doesn't know, in principle, any geographical limits. It does not know either any temporal limits: the information

[1] See Helen Darbishire, Proactive Transparency: The future of the right to information, *World Bank Institute; Governance Working Paper Serie.*

will never be deleted from the Internet[2] and will continue to define one's personal identity and personal history a long time after the information has lost its accuracy. Moreover, easy to gather together which other personal data by the help of search engines, the proactively disclosed information may be a supplementary piece in the mapping of an individual's personal circumstances, when it is not the first "link in the chain", from which other data are gathered. Additionally, if the degree of sensitivity of the disclosed data may increase the risks of privacy infringement, the dangers even exist if the personal data are quite insignificant by themselves, all the more since what constitutes an infringement is individual, it varies from person to person.[3]

The risks of privacy breaches are not only theoretical: the Swedish Data Protection Authority, has, as we will see further, handled several complaints stemming from citizens raising objections against the publication of personal data on the website of public authorities[4] as well as has on some occasions *ex officio* investigated cases where personal data were published on public websites.

So, if the method for giving access to information consisting of online proactive disclosure may be a useful complement to the right of access in its reactive form, it might in the meanwhile lead to privacy infringements. This

[2] See thus the Google case C-131/12 in which the Court of Justice of the European Union aknowledges a right to be delisted. See Jonason, P. (2017), *Le droit à l'oubli numérique en Suède*, Blog droit européen, https://blog§droiteuropeen.com/2017/05/19/le-droit-a-loubli-numerique-en-suede-par-patricia-jonason/

[3] An example of privacy violations due to online publication of information that could at first glance appear as non sensitive concerns the posting on the website of the municipality of Borlänge of the names of all the inhabitants of the municipality. This publication, which, according to the municipality itself had the artistic purpose to "represent what an amount (mängd) is, the soul of the city and its human capital", has nevertheless been experienced by some of the inhabitants as constituting an infringement of their private life. Among the plaintiffs, some were women who, afraid of harassment, didn't wanted to disclose where they lived, other were refugees who wanted to be anonymous in Sweden. Other persons were outraged by the simple fact that information about them was accessible from all over the world. See in decision of the Data Protection Authority, Case n° 1062-99 Tillsyn enligt personuppgiftslagen (1998:204) – (Invånare i Borlänge kommun på webbplats).

[4] In the meanwhile, its is difficult to estimate the number of complaints logded to the Swedish Data Protection Authority against online publication of personal data. Indeed, it has not been possible to get precise information from the authority itself on the number of complaints. Moreover, due to the fact that the Data Protection Autorithy has no obligation to investigate a case after it has received a complaint, the number of complaints investigated does not necessary correspond to the number of complaints lodged in practice.

in turn poses the question of the existence of a protecting legal framework. What do the legal rules in place look like? How are they applied? These are the two questions we aim to answer in this paper with a special emphasis on the balancing between the need for transparency and the need for protection of privacy.

In the following we will examine the applicable legal provisions and their application in concrete cases (1) before summarising our findings (2).

1. The legal framework applicable to online proactive disclosure and its application

As mentioned earlier the Swedish legal framework on the right of access to information does not provide for rules on proactive disclosure.[5] Public authorities, however, make use of this proceeding, not least in publishing diverse kind of documents and information on their websites, sometimes with an underlying aim of achieving more openness.[6] Is it lawful when public authorities publish information of a personal character in this way?

[5] On the contrary to many legislations on access to information around the world. See Manuela Garcia-Tabuyo, Alejandro Saez-Martin, Carmen Caba-Perez, (2017), "Proactive disclosure of public information: legislative choice worldwide", *Online Information Review*, Vol. 41 Issue:3, pp. 354-377. Some special Swedish legal instruments nevertheless regulate procative disclosure, as for instance the Regulation on legal information, Rättsinformationsfördningen (1999:175).

[6] Civil servants sometimes erroneously conceive that proactive disclosure is encompassed by the principle of access to information guaranted by the Freedom of the Press Act. The statement, reproduced below, stemming from a County Council, criticised for having published meeting documents containing personal data on its website, witnesses this attitude. In order to justify the online publication the County Council argued that "*all meeting are open, in a democratic way and all the material including minutes are accessible for the public which has the right to insight and controle in the decision-making*". See Decision of the Parliamentary Ombudsman of 4th March 2011, case n° 3684-2009, p. 2. Moreover, the fact that the Swedish Data Protection Authority underlines, in the introductory part of a checklist specifically drafted for municipalities and County Councils posting minutes and registers on their websites, that the principle of access to official documents doesn't pose any obligation to publish these kinds of documents on the Internet, could be seen as a confirmation that there is a certain faith among public authorities that the legal framework on the right of access to information encompasses the duty to disclose information on their own accord. *Checklista för kommuner och landsting – Webbpublicering av protokoll och diarier*. See also when it concerns the state 's public authorities the Guidelines published by the Data Protection Authorithy *E-förvaltning och personuppgiftslagen – Statliga myndigheters behandling av personuppgifter*.

In order to answer the question and to determine how to carry out the balancing between transparency and protection for privacy that is raised in this kind of situations, one needs to legally qualify such a publication and determine the legal framework applicable.

Concerning the *qualification*, proactive disclosure of data of personal character constitutes data processing of personal data in the sense of data protection legislation. Indeed, it corresponds to the definition contained in Section 3 of the Personal Data Act (1998:204), which describes processing of personal data as "*Any operation or set of operations which is taken as regards personal data, whether or not it occurs by automatic means, for example* […] *disclosure by transmission, dissemination or otherwise making information available* […]".[7]

As to the *applicable legal regime*, as proactive disclosure – as opposed to reactive disclosure – is not encompassed by the constitutional obligations to give access to information, the *lex superior* principle[8], playing in favor of access to the detriment of protection for privacy when the right of access is guaranteed by the Freedom of the Press Act (1949:105), is not applicable here.[9] Instead, the data protection legislation, including the Personal Data Act, is applicable.[10]

[7] Which corresponds to Article 2 (b) of the Data Protection Directive 1995/46/EC, on which the Swedish Act relies. Article 2 (b) states:*"processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as* […], *disclosure by transmission, dissemination or otherwise making available,* […]*".*

[8] It means the principle aiming at solving law conflicts and according to which the law which constitutes the highest norm takes precedence before the law which has a lower status.

[9] See also Section 8 of the Personal Data Act which states that *"The provisions of this Act are not applied to the extent that they would limit an authority's obligation under Chapter 2 of the Freedom of the Press Act to provide personal data."* See also *Checklista för kommuner och landsting – Webbpublicering av protokoll och diarier.*

[10] Also to be noticed is that online publishing of information and documents doesn't fall into the scope of protection of the Fundamental Law on Freedom of Expression (1991:1469). Public authorities which have invoked been in possession of a so called *certificate of publication* and therefore benefiting, thanks to the database rule, of the constitutional protection of the Fundamental Law on Freedom of Expression, have been denied this protection by the Swedish Data Protection Authority. For example, in a decision regarding the publication by the municipality of Trelleborg of personal data related to students expulsed from a upper secondary school, the supervisory authority explicitly mentioned that a certificate of publication for a website "*does not constitute an obstacle for the application of the Personal Data Act (in the present case)*". In a com-

The legal framework applicable to online proactive disclosure, i.e. the pertinent data protection rules, has evolved over time. All online proactive disclosure that took place between 1998, the year of the entering into force of the Personal Data Act, and 2001 fell into the scope of the entire and rather burdensome Personal Data Act shaped according to the regulatory model.[11] However, two consecutives, but not directly correlated, changes in the data protection legislation have successively added lightened regimes.[12] First, the introduction, by the Government, in 2001 of a new provision in the Personal Data Ordinance has impacted proactive disclosure of certain kinds of documents carried out by local authorities. Indeed, publication of personal data in minutes and registers stemming from municipalities and County Councils have been exempted from the prohibition laid down in the Personal Data Act to transfer personal data to third countries. Second, in 2007, an amendment of the Personal Data Act, introducing the concept of *processing of personal data in unstructured material,* has potentially had an impact on all kinds of data processing, including online proactive disclosure, exempting data processings that are to be regarded as such processings, from the majority of the provisions of the Personal Data Act, and submitted these processings to a lightened set of rules with focus on preventive abuse of personal data, the so called abuse centred model.

The three applicable regimes will be presented further and be illustrated by cases handled by the Swedish instance in charge of monitoring the compliance with data protection legislation, the Datainspektion.[13] The deci-

prehensive reasoning the Datainpektion explains its position in arguing that "*the municipality* [which published on its website minutes containing decisions in a case where exercise of power is involved] *should, under these circumstances be considered to represent the State* (det allmänna). *The Data Protection Authority assesses therefore that the provisions of the Fundamental Law, aming at protecting the freedom of expression of the individuals, can not be invoked by the municipality in the present case in order to escape legal obligations, in particular when the obligations – as in the present case – exist in favor of individuals".* Decision 2010-01-29, Case n° 987-2009 Tillsyn enligt personuppgiftslagen (1998:204) – angående publicering av personuppgifter på Internet.). For further information on the system of certificate of publication see Inger Österdahl *Between 250 years of free information and 20 years of EU and Internet*, *Etikk i praksis*, 2016, Vol.10(1), pp.27–44.

[11] *Hanteringsmodell* in Swedish.

[12] In the second section of this paper, dedicated to the findings, we describe the successive "shapes" of the legal framework as some kind of "layers".

[13] It happens that the Parliamentary Ombudsman is involved in this type of cases. It seems than it then relies for its appreciation of the lawfulness or not of the online publication subject to a complaint, to the reasonning made by the Data Protection Authority. It has

sions of the Datainspektion that have been selected for analysis illustrate a large spectrum of decisions: besides illustrating the different stages/shapes of the applicable legislation, the decisions also mirror the diversity of the public actors involved in proactive disclosure, i.e. national agencies/ institutions, municipalities and County Councils. The focus of the analysis is for each of the selected decisions how the Swedish monitoring authority, the Datainspektion, deals with the balance to be drawn between the need to protect privacy and the need for openness.

1.1. The regulatory model and its application

Being a processing according to the definition contained in the data protection legislation, the online publication of personal data in documents published on public authorities' websites is subject to the rules of the data protection legislation, i.e. a set of rules aimed at protecting the privacy of the data subject. Indeed, the Personal Data Act (1998:204), issued 29 April 1998, aims to "*protect people against the violation of their personal integrity by processing of personal data*" (Section 1).

As the Data Protection Directive 95/46/EC on which it is based, the Swedish Act contains for that purpose a number of requirements the controller of the processing of personal data must fulfil as well as prohibitions that he/she has to comply with.

They are for instance the *fundamental requirements for processing of personal data* laid down in Section 9 regarding the quality of the data: the data have *inter alia* to be processed lawfully; be collected for specific, explicitly stated and justified purposes, and not have been processed in a way incompatible with those purposes.[14] The prohibitions relate to the proces-

been the case in the decision 2011-03-04, case n°3684-2009, where a County Council had been critised for having published on its website, before a meeting, reasoned opinions containing personal data. In the current case the Ombudsman, after having examined the incriminated publication of personal data - related to a person been in a psychiatric clinic - in the light of the secrecy legislation, assessed that the publication also had to be appreciated in relation to the Personal Data Act. The Ombudsman, referring to and reproducing a decision taken by the Data Protection Authority concerning a similar case, embraced the conclusion of the Datainspektion, i.e. that the County Council in the current case had, through the publication, processed personal data in breach of the Personal Data Act.

[14] Additionnally, the data must be processed in accordance with the principle of accuracy, as they have to be adequate and relevant and not excessive in relation to the purpose of the processing. The data must furthermore be correct and, if necessary, up to date and not be

sing of sensitive personal data (Section 13), the processing of information concerning legal offences (Section 21) and to the transfer of personal data to a third country[15] (Section 33).

More interesting for the current study are the requirements regarding the legitimation of the processing of personal data, since the Datainspektion has focused its reasoning on these requirements when it has handled cases of online proactive disclosure. These requirements are to be found under the heading "When processing of personal data is permitted" (Section 10). As a general rule, the processing is permitted when the data subject has *consented* to the processing. However, the Personal Data Act, just as the Directive does, also allows data processing for other grounds exhaustively listed in Section 10, one of them being "*when a purpose that concerns a legitimate interest of the controller or of a third party to whom personal data is provided should be able to be satisfied, if this interest is of greater weight than the interest of the registered person in protection against violation of privacy"* (Section 10 f).[16]

This ground, that is at the front when it concerns the determination on whether online publication of documents containing personal data is lawful or not, entails a balancing of interests: online publication of documents containing personal data may be considered as lawful if the legitimate interest of the public authority (the data controller) or third party (generally the public) to disclose or to have access to information, outweighs the interest of the persons whose personal data are contained in the published documents to have her/his privacy protected.

This provision, as the rest of the Swedish Personal Data Act, originates from the Data Protection Directive. A look to the Swedish preparatory works leading to the implementation of the Directive shows that they are not particularly enlightening on the question of the balancing of interests. The preparatory works mention however that the Datainspektion may have

kept for longer than necessary, having regard to the purpose of the processing.

[15] With *third country* means country which is not a member of the EU or the EEA.

[16] See the translate Personal data Act http://www.wipo.int/edocs/lexdocs/laws/en/se/se097en.pdf. The other legal grounds are the following: to enable a performance of a contract; when the controller should be able to comply with a legal obligation ; when the vital interests of the registrered person should be protected ; when a work task of public interest should be performed or when the controller or a third party to whom the personal data is provided should be able to perform a work task in conjunction with the exercise of official authority.

a responsibility for providing data controllers with recommendations and guidelines about the balance of interests.[17] This has been done by the Data Protection Authority which has for example published a handbook tackling the issue of balancing of interests in a general manner.[18]

How the Datainspektion carries out the balancing in practice within the application of the regulatory model can be illustrated by a decision from **September 8, 2004.**[19] The decision concerns the planned publication on the website of a municipal committee in charge of environmental matters[20] of "project reports" that was meant to contain pictures and the names of pizzerias criticized for having an unsatisfactory level of hygiene.

The Datainspektion begins its analysis of the case noticing that the names of the pizzerias constitute indirect personal data when these pizzerias are individual firms/registered as sole proprietors, and assesses that the Personal Data Act is therefore applicable. The Data Protection Authority then reminds that the general rule for the legitimation of processing of personal data is, according to the data protection legislation, the consent, but points out that the processing might be lawful in other situations, *inter alia* when the interests of the data controller to publish personal data overweigh the interest of the persons concerned to be protected against privacy infringements that the publication may lead to.[21]

This was the case according to the Datainspektion which, in appreciating the interests involved and their balance, takes into account that the personal data processed are only indirect personal data (such as the name of the pizzerias) and that the interests that the data become publicly known is high. The monitoring authority concludes that the processing has to be seen as permitted. The interest of openness is, after a balancing of interests, in this case appreciated as outweighing the need of protection for privacy.

1.2 The specific rule regarding the transfer of personal data to third countries and its application

As mentioned above, the Swedish Government introduced in 2001 in the Personal Data Ordinance (1998:1191)[22], a provision tailor-made to create a

[17] See SOU 1997:39 *Integritet, Offentlighet, Informationsteknik*, p. 363.
[18] "*Interesseavvägning enligt personupgiftslagen. Datainspektionen informerar*".
[19] Case n°54-2004.
[20] Miljökontoret in Jönköping.
[21] Decision 2004-09-08 , case n°54-2004., p.2.
[22] The Ordinance contains supplementary rules to the Personal Data Act.

lighter regime for local public authorities publishing personal information on the Internet. Indeed Section 12 of the Ordinance, under the heading "Transfer of personal data to third country"[23] states that municipalities and County Councils are allowed to transfer personal data when these data are included in "*registers* (*diarier*), *a notice to a meeting with the members of the council or with a* [municipal] *committee, a notification about meetings with members of the council or agreed minutes of the meeting with members of the council or a committee*".

According to Section 12.2, personal data which in a direct manner point out the person registered shall not be subject to a transfer. There are exceptions when personal data concern elected representatives carrying out their mandates. The prohibition to transfer personal data to third countries also does not apply if the cumulative conditions set out in Section 12.2 are met, i.e. (1) "*other personal data related to the persons registered are not the ones encompassed by Section 13* (sensitive data) *nor by Section 21* (data about criminal offences) *of the Personal Data Act"* and (2) "*there is no ground for considering that there are risks that privacy of the persons registered been infringed through the transfer*". In any case, the unfailing identifiers constituted by the personal number (*personnummer*) and by the co-ordination number (*samordningsnummer*[24]) may never be subject to a transfer (Section 12.3).

Section 12 which, according to the Datainspektion[25], "*makes it easier*" for the local authorities to publish personal data on the Internet, could correspond to an endeavour to take into account the attitude of openness of the local politicians and civil servants and their wish to, by means of giving access to information regarding the issues of importance for the local community, promote the participation of the public.

One may say that by means of Section 12 of the Personal Data Ordinance and in determining the conditions for the legal publication of personal data,

[23] From the very beginning the provision was introduced in Section 11 (SFS 2000:1055; entered into force January 1st. , 2001). The number of the Section changed to 12 from October 1st 2001 (SFS 2001:582).

[24] Which is an identification number for people who are not or have not been registered in Sweden. The purpose of the co-ordination number is to alow *inter alia* public authorities to identify people even when they are not registered.

[25] The provision "*underlättar för kommuner att publicera personuppgifter på Internet*" states the Datainspektion in a report dedicated to processing of personal data by municipal committees of social affairs and Environmental affairs, *Behandling av personuppgifter hos social- och miljöförvaltningen. Datainspektionens rapport 2004:1*, p .22.

the Government itself has carried out the balancing between the interest of the public to access information and the need to protect privacy. The position statement of the Government – author of the reform – is reflected in the kinds of documents selected to benefit from the lightened regime. Indeed, the categories of documents selected for falling into the scope of the specific regime are the very ones which may inform the citizens on what is going on in the local communities (municipalities and County Councils). They are the kinds of documents to which access may provide the citizens with the possibility to monitor the compliance of the actions of the local decisions makers with the law, and may improve public participation.

The position statement is furthermore illustrated by the distinction made by the government between processing of personal data regarding politicians (data concerning elected representatives carrying out their mandates) on one hand, and processing of personal data regarding the other persons, on the other hand. For the former, the interest in privacy actually disappears for the benefit of openness. The result of the balance of interests is already stated in the law. For the latter, the legislator lays down the criteria that makes it possible to decide if the transfer is allowed or not. One of them requires nonetheless the appreciation *in concreto* of the situation, the appreciation whether or not "*there are risks that the privacy of the person registered would been infringed through the transfer*".[26] No mention is explicitly made of a balance of interests however.

A decision from July 2008 may give an idea as to the application of Section 12 of the Personal Data Ordinance and shed light on the balancing of interests the Datainspektion actually carries out when applying this provision. The decision, from **3 July 2008**[27], concerns the online publication of personal information by the County Council of Sörmland. The personal data, the publication of which was challenged, consist of the name, the title, the private e-mail address and the private cell phone number of a person who had lodged a complaint to the Parliamentary Ombudsman against the County Council. The complaint was in fact attached to minutes stemming from the committee for Health and Medical Care and published on the website of the County Council. The data subject was particularly worried about the online publication of his personal data as he was working at a psy-

[26] We will come back to this "appreciation" further on, under Section 2.
[27] Case n° 788-2008.

chiatric hospital in a department taking care of patients suffering from serious psychic disorders.

Like the County Council against which the complaint was lodged, the Datainspektion, although implicitly, considers that the documents at stake in the case fall into the scope of the special regime set out in Section 12 of the Personal Data Ordinance. The Datainspektion further assesses that the publication does not touch upon sensible data, nor upon data about legal offences, i.e. the kind of data that the Ordinance excludes from the field of application of the lightened legal regime. The Data Protection Authority nevertheless considered that the County Council had published data that point out an individual in a direct manner, because of the complaint the individual had lodged to the Ombudsman. The Supervisory authority and the County Council do not agree on the question of the existence of risks for privacy infringements potentially stemming from the transfer of data/the publication. The assumption of the County Council that it has been no risk for privacy infringement is primarily based on the fact that the personal data in the case were contained in a complaint to the Ombudsman, a document which was accessible to the public (*offentlig*). The Datainspektion emphasises, on the contrary, that the current publication on the Internet leads to risks of privacy infringements and concludes that the publication is therefore not allowed. The arguments related to the interests of having the current personal data published on the Internet are particularly interesting and show that both the County Council and the Datainspektion entered into the field of balancing, although the legislator has not expressly invited the concerned actors to it. Indeed, the County Council for its defense put forward the fact that the publication was aimed to inform the members of the County Council about the activities of the Health and Medical Care Committee, while the Datainspektion counterattacks stating that the interest in having the name and the private numbers of the person published on the Internet (the website of the County Council) is very low. The Datainspektion bases nevertheless its conclusion on the criteria posed by the Ordinance, the question of the risks of infringements of privacy due to the transfer/the publication, and concludes that the processsing could not be allowed.

1.3 The introduction of a lightened regime, the abuse centred model and its application

Six years after the introduction in the Personal Data Ordinance of specific rules for the publication by local authorities of personal data in minutes and registers, the Personal Data Act has also been subject to a reform, due to the enactment of a new provision, Section 5a.[28] This general reform, aimed at simplifying compliance to the data protection legislation for all kinds of data controllers, actually entails "en passant" a lighter regime for public authorities publishing personal data on the Internet.

The reform consisted in supplementing the traditional regulatory model (*hanteringsmodell*[29]), which lays down every step in the processing of personal data, by an abuse centred model (*missbruksmodell*) which focuses on the use of personal data being considered as an abuse.[30] So, when processing of personal data may be considered being a processing in *unstructured material*, the majority of the provisions of the Personal Data Act, including *inter alia* Section 10 on the conditions of legitimation of the processing[31], Section 13 on sensitive data, Section 21 on legal offences and Section 33 on transfer to third countries, do not need to be applied. Nevertheless, the processing of personal data in unstructured material shall not occur "*if it entails an infringement of the privacy of the person concerned*" (Section 5a *in fine*).

What is a processing of personal data in unstructured material? According to the definition contained in Section 5a of the Personal Data Act, it consists of "*processing of personal data which is not included nor intended to be included in a collection of personal data which has been structured in order of facilitating the search or the compilation of personal data*". This encompasses *inter alia* running text published on the Internet, which for instance, the minutes of local authorities generally are.[32]

[28] SFS 2006:398, entered into force on January 1st, 2007.

[29] See SOU 1997:39, *Integritet, Offentlighet, Informationsteknik* p.p. 179 and Prop. 1997/98: 44 *Personuppgiftslag,* p.p. 36.

[30] Prop. 2005/06:173 *Översyn av personuppgiftslagen,* p. 12.

[31] "When processing of personal data is permitted".

[32] See the examples given in the next section. Nevertheless, "*If material, for instance the running text, be included in a database with a structure based on personal data, as for instance a case management system, the rules from the regulatory model then apply*". Prop. 2005/06, *Översyn av personuppgiftslagen*, p.59.

The fact that personal data can be searched by means of search engine (such as Google) and linked with other personal data does not entail the character of processing of personal data in *unstructured material* on postings made on the Internet.[33]

The preparatory works give some elements for appreciating whether or not the processing in unstructured material entails a privacy infringement. According to these preparatory works the appreciation "*shall not be made on a flat rate basis* (*schablonartat*) *but has to also have its point of departure in for instance the context in which the personal data appear, the purpose they are processed for, the dissemination that has occurred or the risk for dissemination and what the processing may lead to*".[34] The preparatory works mention furthermore that should also be taken into consideration the fact that what can be experienced as a violation for a certain person or in a certain context does not need to be experienced the same by another person or in another context.[35]

The legislator touches moreover upon the question of the balancing of interests, pointing out that "*by its very nature the application of a provision such as the one proposed may (får) build on the balance of interests in which the interest of the person concerned to have a private sphere is balanced against contrary interests in the concrete case*".[36]

Three decisions taken by the Datainspektion after the introduction of the abuse centred model in the Personal Data Act will be analysed here. The two first decisions illustrate cases where online publication of personal data by *local authorities* was in focus, while the third and last decision concerns

[33] See the judgment of the Swedish Supreme Court (NJA 2013 s. 1046). The case concerned the publication of a judgment containing the name of the defendant on the website of a debt collection agency (incasso). While the first court (tingsrätten) considered that as the personal data of the defendant that were contained in the published judgment were searchable on the Internet with the search engine Google which links to the website of the agency where the judgment was published, the personal data were to be considered as related to an identified person. The personal data were therefore to *be considered as included in a structure based on personal data*. This interpretation of Section 5a of the Personal Data Act was not accepted by the Court of Appeal (Hovrätten) nor by the Supreme Court (Högsta domstolen) who both perceived the processing in question as a processing falling into the scope of the abuse centred model.

[34] Prop. 2005/06:173, p. 59.

[35] Idid.

[36] Prop. 2005/06:173, p. 27. We will come back to this point further on under the second section of this paper.

online disclosure of information by a *national institution*, in the current case the Parliamentary Ombudsman.

In the first decision of the Datainspektion from **January 29, 2010**[37], the issue at stake is the publication on the website of the municipality of Trelleborg of minutes containing a decision of the committee for high school and adult education to expulse two students from an upper secondary school. The Datainspektion, which considers that the publication is deemed to be a processing falling into the scope of Section 5a of the Personal Data Act, concludes, after having carried out a balancing of the interests at stake, that a violation of Section 5a of the Personal Data Act has taken place. The supervisory authority, which refers to the fact that the appreciation of privacy infringement shall not be made on a flat rate basis[38], takes especially into account that information about expulsion may be particularly sensible for the students concerned and for their relatives. The Data Protection Authority mentions that the information may have negative consequences when the students will search for employment or education, and it also emphasises the fact that the risk for dissemination of the data has been high since the data have been searchable by means of search engines. The Datainspektion also assesses that personal data "*in this context may be considered to have a limited interest for the municipality and the public*", and further considers that the interests for the municipality and for the public "*may be satisfied without naming the students with name and dates of birth*".[39]

In the second decision, from **April 7, 2010**[40], the criticised proactive disclosure consisted of two cases of publication of personal information in minutes posted on the website of the County Council of Sörmland.[41]

The first case concerns the online publication of a reasoned opinion of the County Council in a court case regarding co-payments for heavy medi-

[37] Case n° 987-2009 Tillsyn enligt personuppgiftslagen (1998:204) – angående publicering av personuppgifter på Internet. It is the decision mentioned ealier (footnote 10) in which the Datainspektion rejected the argument of the public authority from having the publication on its website protected by a certificate of publication.

[38] Case n° 987-2009, p. 6.

[39] Id., p. 7.

[40] Case n° 119-2010 Tillsyn enligt personuppgiftslagen (1998:204).

[41] There is a connection between this case and the case we analysed previously (2008-07-03, case n°788-2008) on the basis of Section 12 of the Personal Data Ordinance. In fact the County Council of Sörmland did published again the personal data it was supposed to take away from its website. See footnote 27.

cal treatments. The reasoned opinion contains the name of the spouse of a patient suffering from a serious disease. Her surname is quite unusual and the information constitutes, according to the Data Protection Authority, sensitive personal data related to health in the sense of Section 13 of the Personal Data Act,

The second case concerns the online publication of a reasoned opinion from the County Council addressed to the Parliamentary Ombudsman after a complaint against the County Council made by an individual. It appears from the incriminated minutes that the individual named in the reasoned opinion had requested access to its journal from a center for addicted persons of a psychiatric clinic. Again, the information that a person has been the patient of a health institution constitutes, according to the Data Protection Authority, sensitive data related to health.

After having established that these publications constitute a processing of personal data in unstructured material regulated by the abuse centred model and that the prohibition to process sensitive data as laid down in Section 13 of the Personal data Act is therefore not applicable in the current cases, the Datainspektion nevertheless assesses that the publication of such sensitive personal information on the Internet may lead to an infringement of privacy as prohibited by Section 5a of the Personal Data Act. The Datainspektion refers to the fact that the appreciation has not to be made on a flat rate basis.[42] The Data Protection Authority also emphasises that the attitude of the person concerned vis a vis the processing may be of importance for the determination of the privacy infringement, and uses the wordings of the preparatory works to explain that what constitutes a privacy infringement may differ between persons as well as between contexts. When carrying out the balancing between the interest of the County Council to render its activities transparent, and the interest of the protection of privacy, the Data Protection Authority considers that the interest of the person concerned "*significantly outweighs*" the interest of the County Council in both cases.[43]

The third and last decision analysed here illustrates online publication of personal data performed by a *state authority*. The decision from **October 5, 2010**[44] concerns a plaintiff who had brought a complaint to the Parlia-

[42] Case n° 119-2010, p. 4.
[43] Id., p. 5.
[44] Case n° 663-2010.

mentary Ombudsman and whose name has subsequently been published in the case law database located on the website of the Parliamentary Ombudsman. After concluding, with some reluctance[45], that the abuse centred regime was applicable in the current case, the Datainspektion carries out a balancing of the concrete interests at stake, referring to the non-flat-rate rule set out in the preparatory works. In fact, the Datainspektion does not only examine the balance of interests in the current case but also investigates more generally the balance of interests concerned by the publication of the name of the plaintiffs in the online database as well as the lawfulness of the publication in the online database of the name of the civil servants involved in cases handled by the Parliamentary Ombudsman. Interestingly, the Datainpektion refers to the fact that the applicable provisions (from the Personal Data Act) have their origin in the European Data Protection Directive, and emphasises that the balance of interests to be made cannot be based on an interpretation that contradicts the fundamental rights protected by the European Union such as the right to private life guaranteed by Article 8 of the European Convention of Human Rights (ECHR).[46] Additionally, as if to give more weight to its arguments, the Data Protection Authority mentions the need to respect the principle of proportionality contained both in the Data Protection Directive and in the ECHR, and concludes that the balance of interests laid down by the Swedish legislator contains a similar proportionality assessment.[47] Within the balancing, the Datainspektion takes into account the increasing risks for privacy infringements stemming, in particular, from the publication of personal data on the Internet.[48] Moreover, the Data Protection Authority assesses that the very fact that a person has made a complaint to the Ombudsman may lead to complications for the plaintiff (when searching employment for instance) and that the publication of such information may in turn lead to the unwillingness to make complaints. Against the arguments raised by the Parliamentary Ombudsman, i.e. that the online publication of the names of the civil servants involved in the cases was a transparency measure, the Data-

[45] According to the Datainspektion "*it may be questioned if the legislator had in mind to make the abuse centred regime applicable to the kind of processing at stake when the Parliamentary Ombudsman make its case law database accessible on Internet*", case n° 663-2010, p. 3.
[46] Case n°663-2010, p. 4.
[47] Id., p. 5.
[48]Id.., p. 6.

inspektion[49] uses the arguments that the transparency goals the Ombudsman aims to achieve may be satisfied also if the name of the civil servant is taken away from the decision.

The Datainspektion concludes that in a general manner, as well as in the current case (regarding the issue of the plaintiff), the publication of names in the case law database accessible on the website of the Ombudsman should not be seen as permitted on the basis of the abuse centred model. The Datainspektion is, moreover, of the opinion that a legal instrument is needed for permitting this kind of online proactive disclosure.[50]

2. Summary and findings

From the analysis above we may now make some reflections on three questions: the relationship between the different legal regimes regulating online publication by public authorities (2.1), the basis for the balancing of interests (2.2) and the balancing of interests itself (2.3).

2.1 The relationship between the legal regimes regulating online publication

As we could notice above, the legal framework has changed over time, or, more correctly, it has got more layers over time. The regulatory model that has been applicable since the entering into force of the Personal Data Act in 1998, has been applicable to online publication of personal data also after the introduction of the abuse centred regime in 2007. Indeed, when the disclosure of data takes the shape of processing of personal data in *structured material*, the whole set of rules laid down in the Personal Data Act are applicable on the processing. As an example, the set-up on the website of a municipality of a search function enabling the citizens to get information about food establishments having been subject to public monitoring, is subject to the all obligations laid down by the Personal Data Act. Indeed, according to a statement of the Datainspektion dated 2015 this kind of processing has to be considered as a processing in structured material.[51] In this case, Section 10 f) of the Personal Data Act should be the legal basis

[49] Id., p. 6.
[50] Id., p. 10.
[51] The search function been deemed to obtain specific information from a cases management system (ärendesystem).

permitting the processing of the data – as it was the case in the Datainspektion's decision from 2004 illustrating the regulatory regime, where the names of pizzerias were involved.[52] For the processing to be lawful, it is also required that the other conditions posed by the Act are fulfilled, not least the conditions regarding the quality of the data processing. In the case mentioned here concerning the search function for accessing information on food establishments, the Datainspektion expresses nevertheless doubts on the compliance of the processing with the *fundamental requirements for processing of personal data* laid down in Section 9. Indeed, according to the Data Protection Authority "*taking into consideration the purpose of the processing, i.e. to satisfy the need of the public to have access to the results of the controls, it is high doubtful if the accessibility of the data related to controls that occurs for many years ago may be considered as motivated*". The Datainspektion also concludes that it can be highly doubtful too if the balancing of interests may give support for such a long reaching processing of personal data.

The regulatory regime is thus still applicable for online proactive disclosure on the basis of Section 10 f), but in practice it is not used that much as online publication of documents and data are often qualified as unstructured material and falls into the scope of Section 5a of the Personal Data Act and its abuse centred regime.

The relationship between Section 12 of the Data Personal Ordinance (as introduced 2001) and the other regimes, not least to the abuse centred regime, is less clear, however.

First the introduction of the new Section 12 in the Personal Data Ordinance is quite perplexing. Indeed, the provision that seems to have been introduced – as the heading of the new provision ("Transfer of personal data to third country") and its wordings reflect – as a means for circumventing the prohibition to transfer data to third countries, was actually introduced before the clarification made by the European Court of Justice in the case Bodil Lindqvist. In its judgement from November 6, 2003, the European Court gave an interpretation of Article 25 of the Data Protection Directive on the prohibition to transfer personal data to third countries, being of the opinion that there is no transfer of data to third countries when personal data are published on a website which is stored with a hosting provider established within the EU. Nevertheless the Datainspektion has

[52] Se above under 1.2., the case n° 788-2008.

claimed that "*although this provision is, according to its wording, about exemptions from the prohibition to transfer personal data as laid down in the Personal Data Act Section 33, the very purpose of the provision was to regulate under what conditions the municipalities and County Councils may (*får*) publish registers, minutes etc. on the Internet*".[53]

When we turn to the application of Section 12 of the Ordinance, we can conclude from the decisions of the Datainspektion we have analysed that this provision is rarely applied as a self-standing and self-sufficient legal basis. It was the case in the decision from September 3, 2008, that we used to illustrate the application of Section 12. In this decision Section 12 of the Personal data Ordinance was the only provision discussed by the Datainspektion as the legal basis permitting the publication on the Internet.[54] In the decisions we analysed and that were taken later, the Datainspektion uses Section 12 of the Ordinance only as a benchmark for appreciating the case and not as a self-standing legal basis. Indeed, the Datainspektion assesses that the provision "*may give guidelines for what has to be considered as an infringement according to the abuse centred rule*". [55]

Instead of being a self-sufficient basis for allowing publication, Section 12 of the Ordinance is thus primarily to be regarded as an interpretation tool for the application of another provision, namely Section 5a of the Personal Data Act.

We can also notice that the guidelines drafted by the Datainspektion with the purpose to help the local authorities to comply with the data protection legislation when they publish minutes and registers on their websites[56], have integrated the requirements posed by its 12th Section, however without explicitly referring to the Personal Data Ordinance itself.[57]

[53] Decision 2010-04-07 case n°119-2010 Tillsyn enligt personuppgiftslagen (1998:204) – angående publicering av personuppgifter på Internet, p. 4.

[54] We may also notice that the Datainspektion never uses the expression *transfer to third country* but employs the term *publication*.

[55] See case n°119-2010 , p. 4 and case n°987-2009 p. 7.

[56] The Datainspektion has indeed drafted Guidelines/a checklist after having 2011 monitored about 50 municipalities (*kommunstyrelsen* – Municipal executive boards), which represent about 1/6 of the total of the Swedish municipalities. Through the survey the Swedish Data Protection Authority could assess that all the municipalities published minutes on their website, that about 15 of them also published registers (*diarier*) and that all the municipalities published personal data. Moreover through verifications at random the Datainspektion discovered that personal data were processed in breach of the Personal Data Act. These observations have led the Datainspektion to draw up a checklist addressed

As we can see, the legal framework that may apply to online publication of personal data – especially when proactive disclosure is performed by local authorities – is not easy to comprehend.

2.2 The basis for the balance of interests

When personal data is subject to online proactive disclosure by public authorities, the question of the balancing of the interests of transparency and the interests for protecting privacy is always raised, whatever the legal regime applicable for determining the lawfulness of the processing. The ground or basis for the balancing varies however depending on the regime.

As for the regulatory model, the requirement to carry out a balancing is contained in the law itself. Indeed, Section 10 f) of the Personal Data Act states that a processing is lawful "*when a purpose that concerns a legitimate interest of the controller or of a third party to whom personal data is provided should be able to be satisfied, if this interest is of greater weight than the interest of the registered person in protection against violation of privacy*".

The balance of interests is thus constitutive of the legal ground that has to be in place in order for the processing to be permitted. This provision derives from the Data Protection Directive. The Swedish preparatory works, which focused on how the Data Protection Directive had to be transposed in the Swedish legal system, do not, as we mentioned before, contain information of proper interests for carrying out the balancing.[58]

As for the balancing that has to be made in the frame of the application of Section 5a of the Personal Data Act in the context of the abuse centred model, the requirement to carry out a balance of interests is not laid down in the law but in the preparatory works as we mentioned above. And these are generous in giving information for the carrying out of the balance, at least when giving guidelines and examples of how to determine if a privacy infringement occurs.[59] In any case, the legislator states that "*it is in the last instance a question for the application of the law to, in each case, take into*

to the municipalities and the County Councils - *Checklista för kommuner och landsting – Webbpublicering av protokoll och diarier.*

[57] See p. 2 and 3 of these guidelines *Checklista för kommuner och landsting – Webbpublicering av protokoll och diarier*

[58] Furthemore, it seems that the majority, if not all of the examples used in order to illustrate how to understand and implement the rules concern the private sector. See SOU 1997:39, p. 363.

[59] See Prop. 2005/06:173, p.p.26-29.

account all circumstances, to balance the privacy infringement of the data subject against potential contrary interests".[60]

Regarding the special regime provided by Section 12 of the Personal Data Ordinance governing online proactive disclosure of minutes and registers performed by local authorities, the legislator (the government in this case) has itself made a statement on the balance of the interest to promote transparency of the local public authorities carrying out proactive disclosure on the one hand, and the interest to protect privacy of the data subject on the other hand.[61] When it comes to the *application* of this regime, i.e. the application of Section 12 of the Personal Data Ordinance, if we consider that there is a balancing of interests to be carried out in the concrete cases, this should appear when it comes to appreciate that "*there is no ground for considering that there are risks that the privacy of the data subject been infringed through the transfer*". In fact, we have no knowledge about how the legislator has reasoned when it concerns the application of Section 12 of the Personal Data Ordinance and if the appreciation has to be based on a balancing of interests. At the same time, Section 12.2 of the Personal Data Ordinance has large similarities with Section 5a of the Personal Data Act whose application, as we saw before, is built "*by nature*" on the carrying out of a balance of interests. In the decision taken for illustrating the application of Section 12 of the Personal Data Ordinance, we noticed that such a balance was carried out in practice.[62]

The Guidelines of the Datainspektion addressed to municipalities and County Councils are not so explicit concerning the balancing. They only state that "*For the publication of other personal data* [i.e. other than data that directly point out an individual] *a so called balance of interests has to be carried out in the concrete case*".[63]

In fact, the function of the balance of interests varies: in the context of the regulatory regime (Section 10 f) of the Personal Data Act) the outcome of the balance of interests is aimed to give an answer to the question of whether or not there is a ground for the processing.

[60] [D]et är i slutändan en fråga för rättstillämpningen att i varje enskilt fall, med beaktande av samtliga omständigheter, väga det intrång som kan ha skett i den personliga integriteten mot eventuella motstående intressen, Prop. 2005/06:173, s. 29.

[61] See above under 1.2.

[62] I.e. case n° 788-2008, see under 1.2 above.

[63] *Checklista för kommuner och landsting– Webbpublicering av protokoll och diarier*, p. 3.

In the context of the abuse centred model (Section 5a of the Personal Data Act) as well as when it comes to the special regime put in place for proactive disclosure of minutes and registers by local authorities (Section 12 of the Personal Data Ordinance), the balance of interests gives an answer to the question if there is a privacy infringement/a risk for privacy infringement or not which, in turn, gives an answer to whether or not the processing is permitted.

2.3 The balance of interests itself

The lawfulness of online publication of personal data is dependent on the outcome of the balance between the interest of privacy of the data subject and other interests. Two questions related to the issue of the balance of interests caught our particular attention: the question of whose interests are balanced against the interest of the data subject, and the question of taking into account the specific dangers for privacy that publication on the Internet generate.

Whose interests have been taken into account in the balance of interests?

The way the interests to be taken into account in the balance is formulated appears to differ between the regimes. However, it seems that the interests encompassed in practice when it is about online publication by public authorities are the same, at least in the context of the application of Section 10f) and Section 5a of the Personal Data Act.

Concerning Section 10 f) of the Personal Data Act, the wordings refer to the legitimate interest of *the controller or of a third party to whom personal data is provided*. In the context of online publication of documents, it means principally the interest of the public authorities publishing the data and the interest of the public to receive information.

In the preparatory works explaining the balancing to be made when Section 5a of the Personal Data Act is applicable, the legislator mentions the balancing of the interest of the data subject against "*contrary interests in the concrete case*".[64] The range of interests is wider in this case. In the meantime, when it is about online publication of personal data, the "contrary interests" at stake should reasonably be the interests of the public authority to

[64] Prop. 2005/06:173, p. 27.

perform the publication as well as the interests of the public to receive the information.

In summary, the interests that may be put in the balance are all related to the need for transparency: the need of the public authorities to be transparent and inform the citizens on what's is going on; the need for the public to have access to information, in order to control public actions and/or to participate in the decision making process.

There is no mentioning of a balancing of interests in Section 12 of the Personal Data Ordinance, and we do not know if the question has been tackled in the "preparatory works". However, when applied in the decision of 2008, the public interests to have access to the published information was brought to the fore.[65]

We may say some words on the need of *transparency for the sake of the persons having a political mandate* - i.e. the need for them who participate in the formal decision making process to have access to information by online publication - argument sometimes used by the public authorities having published personal data online[66], is an interest worth to be taken into consideration. It seems to us that publishing information with the purpose to inform the political representatives by means of the website is of more practical character than "ideological" if we may say so. The website is used in this case as an electronic notice board. It can be questioned if there is a need to publish the information world-wide then, and if it not sufficient to publish the information on the intranet of the public authority. It seems to us that this interest has therefore less dignity than the other two above-mentioned interests. We may further notice that this kind of interest has not been paid any particular attention by the Datainspektion.

For their part the two interests more directly connected to the ideal of transparency, the interest of the public authorities to inform (an active kind of transparency, we could say) and the interest for the public to be informed (a passive kind of transparency) are abundantly referred to by the Data-

[65] Case 788-2008, p. 2.

[66] See for example in a decision of the Datainspektion from March 9, 2010, Case n°1857-2009, where the County Council of Dalarna justified the online publishing of the meeting documents (möteshandlingar) containing the criticised personal data by the wish to ensure the general public's insight as well as for facilitating the dissemination of the documents to the members of the County Council.

inspektion. Sometimes separately, sometimes together, and sometimes with other elements more or less related to transparency.

In the decision of April 7, 2010, concerning information related to an individual's health status and information related to the contacts taken by an individual with a centre for addicted persons, information that were contained in complaints lodged to the court and to the Parliamentary Ombudsman respectively, the Datainspektion only refers to the *interest of the County Council* – the public authority criticised for having published personal data online – to give the public insight into its activities This corresponds to what is set out in the Guidelines of the Datainspektion addressed to local authorities: the Data Protection Authority only mentions the "*interest of the municipality or of the County Council to publish personal data*".[67]

In one of the decisions analysed, only *the interest of the public* has been mentioned. The decision in question is the one dated July 3, 2008, in which the Datainspektion made an application of Section 12 of the Personal Data Ordinance. The Data Protection authority did not expressly mention a balance of interests but assessed that "*the interest that the name and the private cell phone number will be accessible to the public knowledge through the publication on the Internet has to be considered as relatively low*".[68]

In two of the decisions analysed, both *the interest of the public authority* and *the interest of the public* have been taken into account by the Datainspektion. In the decision of January 29, 2010 concerning personal data on expulsed students, the Data Protection Authority referred to the "*interests of the municipality and the public*" for being informed of the case.[69] In the decision of September 8, 2004 concerning data related to pizzerias, the Data Protection Authority stated that for the processing being permitted "*the interest of the data controller for the publication has to outweigh the interest of the data subject to be protected against the privacy infringement the publication may lead to*"[70] adding that "*moreover it should be taken into account that the interest that the current data are accessible to the public* (kommer till allmän kännedom*) may be considered as high*".[71]

[67] *Checklista för kommuner och landsting– Webbpublicering av protokoll och diarier*, p. 3.
[68] Case 788-2008, p. 2.
[69] Case 987-2009, p. 8.
[70] Id. p. 2.
[71] Id., p. 2.

In the decision of October 5, 2010 in which the Datainspektion criticised the Parliamentary Ombudsman for publishing the names of the plaintiffs and of civil servants in the case law database located on its website, the Data Protection Authority mentions, without validating the privacy infringments, the purposes presented by the Ombudsman. They consist in providing the public insight into the activities of the Ombudsman, but also in disseminating knowledge about the legal appreciations contained in the decisions of the Parliamentary Ombudsman with the aim to give public authorities and civil servants guidelines for how to act in a correct way".[72]

The specific threats due to the publication of personal data on the Internet

The disclosure of personal data by means of the publication on the websites of the public authorities is surrounded by specific threats due especially to the wide dissemination of the data posted on the Internet as well as to the efficient searching possibilities and the easiness to make compilations of data that search engines offer.[73] The threats for privacy having to be taken into account in order to carry out the balancing of interests, the Datainspektion does refer in its decisions to the specific threats stemming from the Internet, although elaborating more or less on them.

Indeed, except for the decision of September 8, 2004 regarding the pizzerias in which the Internet was not mentioned at all, and for the decision of July 3, 2008 concerning the publication of a complaint lodged to the Parliamentary Ombudsman by a person working at a psychiatric hospital were the specific risks with Internet were only referred to *implicitly*, the Datainspektion does in its decisions *explicitly* mentions the risks due to the publication of personal data on Internet.

In the decision of April 7, 2010 in which *inter alia* data related to the health status of a data subject were at stake, the Datainspektion stated that "*through the publication on the Internet there is a high risk for a large dissemination*".[74] In the decision of January, 29, 2010 concerning the students expulsed from an upper secondary school, the Supervisory authority emphasises that the risk for dissemination of the data – which may be very sensitive for the students and their relatives – has been high due to the fact

[72] Case n° 663-2010, p. 6.
[73] More on that issue in the introductory part of this paper.
[74] Case 119-2010, p. 5.

that the data have been searchable with means of search engines.[75] The Data Protection Authority was even more precise about the risks that emanated from the Internet in its decision of October 5, 2010, in which it criticised the Parliamentary Ombudsman for publishing the names of the plaintiffs and of civil servants in its online database. The Datainspektion mentions explicitly the increase of the risks for privacy due to online publication "*What makes the publication so sensible* […] *is the way of publishing*" the Datainspektion states. The Data Protection Authority refers *inter alia* to the relative easiness to make comprehensive compilations, emphasises that the data are easily accessible especially by means of search engines, and mentions the possibilities to make compilations and to reuse the material that is accessible on the Internet.[76]

Surprisingly and regrettably, the guidelines of the Datainspektion do not mention the necessity to take into the account the specificity on the Internet and the particular risks that online disclosure of personal data generate for privacy.

***

The question may be raised on what the legal framework will look like after the entering into force of the General Regulation on Data Protection (EU) 2016/679, and how this will affect proactive disclosure. It seems clear that the abuse centred model, which, in an indirect manner has lightened the conditions for online publication carried out by public authorities, will disappear.[77] Will we then go back to a system similar to the one that applied before the reform of 2007 of the Personal Data Act, i.e. a system where online proactive disclosure of personal data is permitted if the interest of the data controller or of third party outweighs the privacy rights of the data subject?[78] The formal answer seems to be uncertain due to different interpretations of the Regulation. According to one of the interpretations none processing carried out by public authorities will be encompassed by this legal ground, which could mean in turn that online proactive disclosure car-

[75] The Datainspektion states "Google, for instance". Case 987-2009, p. 7.
[76] Case n° 663-2010, p. 6.
[77]See the statement of the Datainspektion on http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/missbruksregeln-upphor/
[78] Legal ground laid down in the Regulation (Article 6 1.f) as it was in the Data Protection Directive (Article 7).

ried out by public authorities would be considered as "*processing necessary for a performance or a task carried out in the public interest*" and will consequently be submitted to the requirement of having a legal basis (Article 6.3[79]). If the other interpretation takes precedence however, the one according to which not all processing from public authorities will be excluded from this legal ground, the balance of interests might be theoretically still applicable to online proactive disclosure performed by public authorities.[80] Whatever the interpretation adopted, we think that the legislator should, in order to give some space for the public sector to publish information while ensuring the protection of the privacy of the persons concerned, adopt specific legal instrument(s), in the way it did partially in 2001[81] and set out the overarching frame for the balance between the interests of transparency and privacy.[82]

In legal terms, online proactive disclosure of personal data by public authorities should, with the new European Data Protection framework, enter a new phase. This shift could give the Swedish legislator the opportunity to re-think and rationalise the legal framework for online proactive disclosure of public documents and information containing personal data. The enactment of a new framework could be advantageously accompanied by guidelines and other recommendations drafted by the Datainspektion, addressed to all public authorities and with a special emphasis on the threats for privacy generated by publication on the Internet. The aim of this kind of guidelines should not only be to inform about the applicable data protection rules, but also to spread awareness among the public sector on the specific and serious threats online publication of personal data may have for privacy, and in turn for democracy.

[79] This legal basis "*should*", according to Recital 41 of the Regulation "*be clear and precise and its application should be foreseable to persons subject to it*".

[80] See *Remittering av betänkandet SOU 2017:39 Ny Dataskyddslag*, 2017-09-04, n° 1210-2017, p.8.

[81] By means of the Personal Data Ordinance, Section 12. The legal framewok concerned the publication of the minutes and registers of the local authorities.

[82] This corresponds also to recommendation of the Datainspektion to enact specific legal instruments, expressed in the 2010 decision in which the Data Protection Authority criticised the Parliamentary Ombudsman for publishing names in the decisions published in the case law database accessible on its website,