The Use of the Internet, Social Media and Search Engines in the Context of Administrative Investigations – A Need for an Adequate Legal Framework to Efficiently Protect Privacy and Democratic Values

Patricia Jonason

1 Introduction …… 272

2 The Need of a Robust Legally Binding Framework: **High Level Requirements from the European Legal Framework** ……. 274
2.1 Article 8 of the European Convention on Human Rights and the Protection of Privacy ……...……..….... 274
2.2 The European Legislation on the Protection of Personal Data 277

3 A Partially Flexible Legal Framework ……..….. 280
3.1 Multiple Issues Related to Administrative Investigation Practices on the Internet ……...…..... 280
3.2 The Contributions of a Flexible Legal Text ……...…….... 282

4 Conclusion ……..… 284

1 Introduction

> In 2013, Ms. S. lodged a complaint to the Swedish Parliamentary Ombudsman against a social worker in charge of the handling of her request to renew her social aid. The complaint concerned a privacy infringement. It was during an interview at the office of the public official that Ms. S. discovered, among the pieces constituting her administrative file, reproductions of photographs posted on her own Facebook account and on a blog belonging to a friend of hers. Ms. S. reported to the Ombudsman that she got the unpleasant feeling of having been "watched" and that the public official in charge of her case had "put his/her nose" in her private life.[1]

This case (hereinafter the Facebook case) of administrative investigation through the search and collection of personal information on social media and the Internet at large, using search engines, is not isolated. On the contrary, it seems to be common practice.[2] While the phenomenon is not completely new, it has begun to be noticed in Sweden, in a more pronounced manner, by the Swedish Parliamentary Ombudsman (JO) in the last few years. Indeed, while there were some disparate decisions from the JO tackling this issue in the past[3], it was first in the annual report of 2015/16 that one of the Ombudsmen highlighted the phenomenon by employing the expression of "new tools" in the activities of the administration.[4]

Unfortunately, the importance of the issue has not reached the Swedish legislator yet. The topic was for example not explicitly mentioned in a Government term of reference from 2014 [5] which gave a parliamentary committee the mandate to carry out a mapping and analysis over the risks of privacy infringements that may occur because of the use of information technology in the private and the public sectors. The terms of reference indicate that the individuals often have little possibilities to influence which personal data the public authorities have access to. The terms of reference also mention that individuals make a large use of social media and "that it may be difficult for them to get an understanding of the use of these data after their publication and dissemination […] which poses questions in terms of who has the right to the information after they have been published and how individuals should proceed

1 JO decision from the 15th of January 2015, Dnr 2611-2013. The Parliamentary Ombudsman had not concluded to a violation of legal obligations but encouraged discussions within public authorities on the issue of the use of information retrieved from the Internet. The Ombudsman also pushed for the enactment guidelines. For an analysis of the decision *see* Jonason, P., Administration et collecte de données personnelles sur Internet et les réseaux sociaux : à la recherche d'un cadre juridique adéquat, Revue internationale des gouvernements ouverts, 2017, n°5, p.13-32.

2 This is the perception I got from discussions with public officials from a number of Swedish public authorities. I did not however make a survey "dans les règles de l'art". A the same time, why should the public officials have another behavior than the rest of the population, i.e. an enclination to use search engines for retrieving information?

3 *See* for instance the decision from the 16th of October 2008, Dnr 3964-2007.

4 Annual report 2015/16, p.23.

5 Kommittédirektiv 2014:65 Den personliga integriteten.

in order to get the data deleted". However, the authors of the terms of reference do not make the link between the use of social media by individuals and the use of personal information published on social media or elsewhere on the Internet by public authorities.

The question is nevertheless worth discussing. The administrative practice of collecting personal information on the Internet, including on social media, is undoubtedly a means to improve administration efficiency. For instance, in a case such as the one described above, it makes it easier for the public official to verify the veracity of the applicant's sources of income. Administrative investigations on the Internet may nonetheless be potentially detrimental to privacy and to the foundations of democracy.

Indeed, the technical and the societal contexts make such a practice intrusive for the privacy of the individuals directly concerned by the investigations. By technical context we mean inter alia the online access of a large amount of information provided by the Web and the possibilities to search, gather and complile data offered by search engines. By societal context we mean especially the large tendency in the population to use social media,[6] how it is used, and the impact this use has on the forms of communication.

Furthermore, considering that privacy constitutes a *sine qua non* condition for democracy, as privacy empowers citizens with the personal autonomy necessary for "[participating] in the political competition of ideas",[7] such a practice of administrative investigations may also jeopardize democracy. The collection of personal information by public authorities from digital platforms such as social media and by means of tools like search engines is indeed liable to affect the public's confidence in state bodies. This may, in the long run, generate citizens' distrust towards an administration they suspect is spying on them and could lead to self-restraint in the exercise of one's freedoms. This may in turn threaten the pluralism of opinion as well as the diversity of ways of life.

There is therefore a need to regulate these kinds of practices with a legal framework capable of protecting privacy as an individual value (the privacy of the person concerned) as well as a social value (privacy as a *sine qua non* condition for democracy). Such a framework should consist of hard law, not least to comply with the pertinent European Law (1).

It should also include soft law, a kind of law that is better suited to serve as an awareness tool as well as a compass for public officials (2). The current article aims to suggest potential avenues for reflection and future action.[8]

6 Sweden for instance counts 9 million Internet users (about 93% of the population) and 5 million social media users (about 52% of the population).

7 Boehme-Neßler, V., Privacy: a matter of democracy. Why democracy needs privacy and data protection, International Data Privacy Law, Volume 6, Issue 3, August 2016, p. 227.

8 Such a reflection should be multidiciplinary and include, among others, lawyers, political scientists and sociologists, but also information and media scientists.

2 The Need for a Robust Legal Binding Framework to Comply with the High Level Requirements of the European Legal Framework

Both the European Convention on Human Rights (1.1) and the data legislation of the European Union (1.2) impose requirements on administrative investigations on the Internet that the Member States have to comply with.

2.1 Article 8 of the European Convention on Human Rights and the Protection of Privacy

It seems possible to argue that Article 8 of the ECHR, which provides a right to respect for one's "private and family life, [...] home and […] correspondence", may potentially apply to administrative investigations performed through searching and collecting personal data on the Internet and the use of these data, including the surveillance these practices generate.

As of today I know of no decision from the Court of Strasbourg on this issue in particular. However, a certain number of cases submitted to the European Court of Human Rights have highlighted the problem of the surveillance and the mapping of citizens carried out by public authorities, especially in the field of investigations carried out by the Police or the Army in the name of national security. [9] A decision from the 18th of October 2016, Vukota-Bojić c. Switzerland,[10] in which the ECtHR condemned the Swiss State for invasive surveillance of an insured person by a public insurance company is a precedent by which the validity of our hypothesis may be discussed, less because of the methods used to carry out the monitoring than for the purposes of surveillance.

The case is as follows: the applicant, who had been a victim of a road accident in 1995, had obtained a disability pension from her insurance company. During the following years Ms. Vukota-Bojić passed several medical examinations. Some concluded that her faculties of work were fully recovered, others concluded on the contrary that she was incapacitated to work. After several years of litigation, the insurer asked the applicant to undergo a new medical examination. Faced with the latter's refusal, the insurer hired private detectives to track the applicant's movements and gather evidences concerning her health. The acts of surveillance consisted in that the detectives, over a period of thirty-three days, on four different dates and over long distances, followed and filmed Ms. Vukota-Bojić in public places and prepared reports on their observations. The evidence gathered was then used against the applicant during a trial in order to obtain from the court a substantial decrease of the applicant's disability pension. Before the Strasbourg Court, Ms. Vukota-Bojić won the case on the

9 *See* for instance the Murray v. United Kingdom judgment of 28th of October 1994 (application no. 14310/88) and, more recently, the Szabó and Vissy judgment against Hungary of 12th of January 2016 (application no. 37138/14).

10 Application no. 61838/10.

allegations of violation of privacy guaranteed by Article 8 of the European Convention on Human Rights.

Indeed, the European Court of Human Rights considers that the surveillance exercised towards the applicant, which is characterized by a permanent nature of the footage, and the use thereof in an insurance dispute "*may be regarded as processing or collecting of personal data about the applicant disclosing an interference in her ' private life' "within the meaning of Article 8§1*".[11]

In reaching this conclusion on the application of Article 8 (1), the Court states *inter alia* that

> "'private life' within the meaning of Article 8 is a broad term not susceptible of exhaustive definition"[12] and that Article 8 "protects, inter alia, a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world".[13] The Court goes on to say that "There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'". [14]

The European judges also take into consideration circumstances such as

> "whether there has been a compilation of data on a particular individual, whether there has been processing or use of personal data or whether there has been publication of the material concerned in a manner or degree beyond that normally foreseeable."[15]

The definition of private life employed by the Court, which goes beyond a purely private circle and insists on the social function of the right to privacy, seems to be well suited to the situation in which administrative investigations are performed on the Internet and social media : the former is considered as a public space, the latter more as a hybrid space,[16] both deal *de facto*, with interactions between Internet users.

---

11 Para 59.

12 Para 52.

13 Para 52.

14 Para 52.

15 Para 56.

16 The very nature of the Internet and social media has been tackled be sholars. *See* for example Camp, J.., Chien, Y.T., *The Internet as Public Space: Concepts, Issues, and Implications* in Public Policy, Concerning social media *see* Bös, B., Kleinke, S., *Publicness and privateness* in Christin Hoffman W., and Bublitz, W., (eds), Pragmatics of social media, 2017. According to the authors "Social media […] have shaped new hybrid spaces "neither conventionally public nor entirely private", p. 89. They quote in turn Papacharissi, Z. and Gibson, P.L, *Fifteen Minutes of Privacy: Privacy, Sociality, and Publicity on Social Network Sites* in Trepte**, S.,** Reinecke**,** L., *Privacy Online Perspectives on Privacy and Self-Disclosure in the Social Web*, 2011. *See* also Burkell, J., Fortier, A., Yeung, L., Wong, C., Simpson,, J.L., *Facebook: public space, or private space?* Information, Communication & Society Volume 17, 2014 - Issue 8 Pages 974-985. According to these authors the "private" or "public" character of social media is largely determined by the privacy settings of the account.

Another element of the appreciation, made by the Court in the Vukota-Bojić case, for assessing privacy infringement may be subject to more discussion regarding its application to cases of administrative investigations on the Internet: it is the question of the taking into account of "A person's reasonable expectation as to privacy".[17] Indeed, one may discuss which level of respect for his or her private life an Internet or Facebook user is expecting while he or she exposes in a more or less controlled manner his or her private life on the Web and therefore if he or she can invoke an interference with his or her privacy if undergoing Internet based administrative investigations. Is it possible to argue, as the Ombudman did,[18] that social media users have to blame themselves if the administration collects data concerning them on their profiles? The answer seems to be more nuanced, for several reasons. First, not all social media users understand how to use privacy settings or understand when their account is accessible to everyone or to a limited circle of "friends".[19] Second, the information posted is not addressed to the administration. Third, the data subjects are not aware of the public authorities' potential use of the data they post on their social media accounts. Fourth, the information might be collected by the public officials on social media profiles belonging to other individuals, i.e. platforms outside the control of the person concerned.

Anyway, the "blame yourself" argument is refutable from a legal perspective because if "reasonable expectation" "is […] significant" for the ECtHR in assessing the interference with privacy, it is however, according to the same Court, "not necessarily conclusive [...] factor".[20]

It may be argued that surveillance by camera, as in the Swiss case, is of a higher grade than surveillance conducted over the Internet and social media. While there is undeniably a difference in the severity and intensity of the methods employed, the insidious nature of Facebook-type investigations is nevertheless also problematic. Moreover, in both cases, the administration, which acted undercover, accumulated elements enabling the verification of a citizen's statements in the context of the handling of his or her case. Furthermore, the effect of the investigations on the individual is the same: in both cases, the women felt watched and infringed in their privacy.[21]

---

17 Para 54.

18 The Ombudsman, author of the "Facebook decision", refers to a decision of October 16th 2008 (Dnr 3964-2007) taken by another Ombudsman in a case in which a social security agency had collected information on the blog of a social insured person. The Ombudsman did not in this decision criticize the social security agency in question on the grounds that a person who publishes information in this way must take into account that the information is also accessible to public authorities, and that the latter have the obligation to take into consideration all the information that comes to their knowledge.

19 This was the case in the Facebook case.

20 Para 54.

21 There is a noticeable difference, however, between the two cases: while the documented information was used to support the decision to reduce the invalidity pension in the Swiss case, the information collected on the Internet did not impact the decision taken by the social services in the Swedish case.

In spite of dissimilarities concerning the *modus operandi* of the investigation and thereby of the surveillance measures employed, it seems to me that it is possible to rely on the Vukota-Bojić judgment to consider that the search, collection and use of data in the context of digital administrative investigations satisfy the criteria laid down in Article 8.1 on the existence of an interference with privacy.

What about the question of the justification of the interference? In other words, is such interference "prescribed by law" under Article 8.2, as understood by the ECtHR? In the case of Vukota-Bojić v. Switzerland, the Court, having reviewed the national texts applicable, admits that the relevant legal provisions, read together, allow the Swiss insurance authorities, in case of the insured person's reluctance to provide the information requested, to take the appropriate investigative measures and to collect the necessary information. The Court also agrees that the provisions in question were "accessible" to the applicant.[22] On the other hand, the European judges criticise the Swiss legal framework on the grounds that it does not offer sufficient guarantees against abuse[23] and that it is silent on the procedures of storage, access, examination, use, communication and destruction of data collected through secret measures of surveillance.[24] Consequently, the Court finds a violation of Article 8 without having to decide whether the contested measures were "necessary in a democratic society".

The high requirements laid down by this judgment concerning the legal framework to be put in place should be applicable to administrative investigations such as the one performed in the Facebook case.

2.2 The European Legislation on the Protection of Personal Data

The collection of personal information from the Internet, including social media, and the further use of this information for the purpose of administrative investigations should be deemed to constitute data processing in the sense of the General Data Protection Regulation (GDPR) (EU) 2016/679,[25] which, since the 25th of May 2018, replaces the Data Protection Directive 95/46/EC and the national legislations transposing the Directive.[26] According to the GDPR, and more precisely Article 4 (2), processing of personal data is defined as:

> "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection,

22 Para 70.

23 Para 73 and 74.

24 Para 75.

25 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

26 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.

> recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or

As it falls within the GDPR's definition of processing, the practice of the administration which consists of collecting personal data on the Internet and using them, must be subject to the protecting rules of the European data protection legislation, not least the Principles relating to the Processing of Personal Data (Article 5) and the Principles of the Lawfulness of processing (Article 6).

First, the processing of personal data has to follow the *Principles relating to the Processing of Personal Data* laid down in GDPR Article 5,[27] that is the principle of lawfulness, fairness and transparency (5 a), purpose limitation (5 b), data minimisation (5 c), accuracy (5 d), storage limitation (5 e), integrity and confidentiality (5 f). The controller shall "*be responsible for, and be able to demonstrate compliance with*" all of these principles (accountability) (5.2). The principle of accuracy of personal data is especially interesting in the context of administrative investigations taking place on the Internet, a platform where the veracity of a large proportion of published information may be questioned, whether it is the person concerned itself or others who have posted the information. The principle of fairness and transparency which means inter alia that the data subjects are informed of the processing is also of particular interest in the context of Internet-based investigations.

Second, the processing performed (both the collection and the subsequent use of the data) must satisfy the conditions for the *lawfulness of the processing* (Article 6[28]), meaning that it has to be supported by a legal basis listed in article 6. The adequate legal basis for the processing in the context of administrative investigations should be the one stated by Article 6.1 e in the second part of the sentence, i.e. that the processing is lawful if such processing "is necessary for the performance of a task carried out […] in the exercise of official authority vested in the controller".

Art. 6.2 states that "Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation […] by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing […]". This provision allows the national legislator, if necessary, to take into account the specificities of the collection of personal data on the Internet and social media.

When such a legal basis as Article 6.1 e applies, the GDPR also requires, in Article 6.3, that the basis for the processing *shall be laid down* by Union law or the Member state law.

It does not require "a specific law for each individual processing" and therefore "A law as a basis for several processing operations […] may be sufficient" (Recital 45).

Furhermore, according to Article 6.3, mirrored in recital 45:

---

27 Principles relating to data quality, according to Article 6 of the Directive.

28 Criteria for making data processing legitimate according to Article 7 of the Directive.

> "That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedure […]".[29]

Article 6.3 in fine indicates "The Union or the Member State law shall meet an objective of public interest and be proportioned to the legitimate aim pursued". This wording seems to implicitly refer to the law of the European Convention of Human rights.

Recital 41 makes, on its part, an explicit reference to the law of the Convention, assessing that the legal basis:

> "should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights".

Read together, the pertinent provisions of the GDPR require a clear and precise legal and foreseeable legal basis[30] and encourage the States to more narrowly determine the conditions for the data processing through regulation.

As in the Vukota-Bojić case, the requirements in terms of the clarity, the precision and the foreseeability of the legal framework regulating the surveillance measures may be considered of a high level when it concerns Internet-based administrative investigations. This in turn requires from the legislator to determine, in the legal basis for the exercise of official authority or in another regulation, the narrower conditions for the processing consisting in

---

29 Another requirement from the GDPR is that the purpose of processing of personal data shall be *necessary* in relationship to the legal basis, in the current case in relationship to *the performance of a task carried out in the exercise of official authority vested in the controller*". (Art. 6.3) The term *necessary* is to be interpreted in an extensive manner according to the Swedish legislator, the term having a larger content in EU-law context than according to the Swedish definition. *See* SOU 2017:39, p. 105 and prop. 2017/18:105, p. 46.

30 The Swedish legislator interprets this as meaning that the level of precision concerning the legal basis varies, with consideration for the character of the processing and the character of the activities. The legal basis can be general when the processing does not constitute an infringement (such as the processing of the names of the students by a school) but has to be more precise when it comes to sensitive data such as within the health sector. If the infringemennt is *significant, occurs without consent and consists in surveillance or the mapping of the personal circumstances of the individual*" then the processing is submitted to the requirement of having a specific legal basis according to the the Instrument of government Chapter 2, Section 6 (RF 2:6) and Chaapter 2, Section 20 (RF 2:20). *See* prop. 2017/18:105, p. 51. It is nevertheless unclear how to interpret RF 2:6, introduced in the catalogue of human rights of the Instrument of government during the constitutional reform that took place in 2011.

the collection of data on the Internet and of the use of these data by public authorities for the purpose of administrative investigations.[31]

It follows from the foregoing review of the European legal instruments that bringing Internet based administrative investigations into line with European law presupposes the adoption of legal instruments laying down the conditions for the processing of personal data as well as mechanisms to prevent abuse and arbitrariness.

In any case, if a clear, precise and accessible binding legal text containing mechanisms for protecting privacy is indispensable, it seems that, given the importance and plurality of the issues involved in administrative investigations on the Internet, such practices must additionally be framed by instruments under the soft law.

3 A Partially Flexible Legal Framework

The question of regulating administrative practices of search and collection of personal data from social media, and more generally from the Internet, is crucial and complex. The challenge is indeed to reconcile administrative efficiency with two crucial imperatives: the protection of privacy and, further, the protection of the foundations of democracy (2.1). However a binding legal instrument is not enough to adequately capture the different dimensions involved. A legal binding instrument can only have a general and rather vague character, whereas the carrying of administrative investigations by means of the Internet requires an assessment on a case-by-case basis of the limitations that may legitimately be placed on citizens' freedoms. Public servants should therefore need guidelines helping them in making decisions, including information of the interests at stake when using these methods (2.2).

3.1 The Potential Detrimental Impacts of Internet-based AdministrativeInvestigations

The use of platforms (social media and other) and tools (such as search engines) provided by the Internet is not insignificant from the point of view of the fundamental rights and freedoms of individuals, and beyond, of the foundations of a democratic society.

31 When it comes to Swedish law, there are already examples where the legal basis for the exercise of official authority contain rules especially dedicated to the processing of personal data, such as the Social Insurance Code. There are also examples of specific acts dedicated to the processing of personal data in a specific sector, such as the Data Protection Act for Patients (patientdatalagen). It is interesting to notice the proposal made 2015 to enact a so-called *Administration Data Protection Act* (myndighetsdatalag) which should have contained a general legal basis for the processing of personal data by public authorities. The proposed draft stated "a public authority may process personal data when it is necessary for carrying out its activity". It was also proposed that the law had encompassed annexes relating to specific public activities. *See* SOU 2015:39. The law has not been enacted.

First, this method has many implications in the area of the right to *privacy*. The four components we include in this notion[32] – the "right to be left alone", the right to informational self-determination, the "power of a person to behave like he or she wants to 'in this part of his or her life' " [33] and the individual's ability to participate in society – are all affected by administrative methods of investigation making use of the Internet.

Instead of being *left alone* by public authorities, the persons subjected to this kind of investigation may on the contrary feel "watched" by public officials. The Swedish Facebook case bears witness to this. Such practices also contribute to the *citizens' loss of control* over the use of their data. In fact, public authorities use information and data that is not intended for them, without the knowledge of the persons concerned. In addition, the use of the possibilities offered by search engines is likely to lead to two types of particular risks for the data subjects' privacy. It is, first, the danger of *aggregation*[34] that comes from the possibility to map a particular person, thanks to the mass of information obtained on this person when using search engines. The second danger, that of *distortion*,[35] consists in that all collected information put together do not necessarily give a representative picture of the person concerned. It may be that important pieces of the puzzle of the current person's life are missing, or that some elements are given too little or too much weight, or that elements that do not conform to the reality of the person concerned are presented as truth.

Furthermore, as social media are *par excellence* tools for societal action and interaction it is not difficult to conceive that the components of the right to privacy such as "the power of a person to behave like he or she wants to 'in this part of his life'"as well as the "possibility of individuals to participate in social life" may also be affected if public authorities carry out administrative investigations on the Internet, including social media.

The risks caused by Internet-based administrative investigations are not confined to the interferences with the right to privacy of the person directly concerned by the investigations, but may have broader repercussions. Indeed, the right to privacy does not only have an individual value of protecting the persons concerned but also has a collective value of protecting the democratic values as a whole.

The recognition of the societal value of the right to privacy, which has been explicitly proclaimed by the German Federal Constitutional Court in the landmark Census decision from 1983,[36] is also to be found in the case law of the

32 *See* Blanc-Gonnet Jonason, P., Démocratie, transparences and État de droit – la transparence dans tous ses états, European Review of Public Law, vol. 27, nr 1, 2015, pp. 122-124.

33 In Kayser, P., *La protection de la vie privée par le droit*, Economica. 1995, p. 11-12.

34 *See* SOLOVE, D. J., *Nothing to hide - The False Tradeoff between Privacy and Security*, Yale University Press, 2011, p. 27.

35 Id., p. 28.

36 Judgement of the15th of December 1983, BVerfG, *EUGRZ*, 1983, 588.

European court of Justice. Thus, in its Digital Rights decision,[37] by which it invalidates the Data Retention Directive 2006/24/ EC for non-compliance with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, the Grand Chamber of the CJEU emphasizes the risk that the retention of communication data by operators generates for the freedom of expression of citizens. [38]

The awareness about the relationship between privacy and fundamental democratic freedoms is also echoed in Sweden. In a parliamentary report entitled "What's the state of privacy?",[39] the investigators (),[40] argue that the right to privacy is:

> "an important element also for [...] the fundamental rights and freedoms which form the basis of a democratic society, and in particular freedom of expression, the right to information and the right of communication". The report continues, "[...] fundamental values may be endangered if individuals give up doing business because of a loss of confidence or fear of being recorded, mapped or otherwise monitored in a manner that ultimately could harm them".

One may fear that the use of administrative investigative methods consisting of gleaning personal information from the Internet and social media may lead to a reaction of self-censorship and, more generally, of self-restraint among citizens. This might be manifested in a reluctance of Internet users to publish information on their own social media accounts. Self-restraint may also express itself in the reluctance of citizens to take part in social activities that would leave traces on the Internet, such as participating in sports event or joining an association. This can be an even more serious attack on individuals' freedoms. Concomitantly, the risk may exist that citizens' trust in the State diminishes as well as the trust in the professionalism of the states' agents, gleaning information on social media as investigation means.

3.2 The Contributions of a Flexible Legal Text

Faced with these primordial issues, a legally binding text framing Internet-based administrative investigations is not enough, especially if it is a general (i.e. non sector specific) and thus vague text. Civil servants on the contrary need a

37 Judgment of the 8th of April 2014, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd., Kärntner Landesregierung.

38 According to the Court "it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter". Para 28.

39 SOU 2016: 41 Hur står det till med den personliga integriteten?

40 Under a heading entitled "Privacy, a value of importance to society as a whole". In fact, Swedes have long emphasized the relationship between the protection of privacy and freedom of opinion.

relatively accurate compass that helps them, on a case-by-case basis,[41] to assess not only the legality but also the legitimacy of investigations carried out on the Internet. Moreover, a legal binding instrument aiming at regulating the collection and the use of personal information lets outside of its scope privacy infringements that the search itself causes and the feeling of surveillance this generates. There therefore seem to be a need for supplementing the hard law instrument by a legal instrument[42] of a soft law nature which would raise awareness and provide civil servants with tools helping them to strike a proper balance between the interests involved.

This text should, in the form of guidelines, elaborate on the elements that the public officials should take into account in order to achieve the balance mentioned above,[43] i.e. the balance between the administration's efficiency on the one hand and the protection of freedom and democracy on the other hand, for deciding to perform or not perform investigations on the Internet. Among the questions the official in charge of investigations should ask him or herself prior to taking such a decision are the following: What information does the official already have? What is the need to obtain additional information? What kind of complementary information is needed? What are the interests at stake for the administration to obtain the missing information? Has the subject been encouraged to provide information that is missing? Are there reasons to doubt the veracity of the information already available? Has the public been informed that the administration is likely to search the Internet?

Striking a fair balance of interests also requires that the civil servants have knowledge about and understand the technological, informational and societal context in which they act. The elements to remind public officials, even if it goes without saying, could include the wide use of social media and the primary goals of the use of these social media by private persons, namely the communication between peers. Additionally, public officials should be reminded that a large share of personal information found on the Internet is published outside the control of the persons concerned, or even without their knowledge, and that participation in many activities (e.g participation in a sporting or scientific events) leave traces on the Web. It would also be useful to emphasize the need

41 The Swedish Ombudsman in his Facebook decision addresses the question of the need for guidelines, arguing *inter alia* that it should not be left to the public servant alone to determine when it is appropriate to proceed with Internet searches in the context of administrative investigations.

42 Chevallier, J., *L'État post-moderne*, L.G.D.J, Droit et société, 2008. Chevallier argues that the fact that a text consists of a recommendation doesn't impact the legal nature of the instrument.

43 The Ombudsman cites, as an example to follow and develop, the guidelines adopted by some administrations, including the National Agency for Social Affairs (Socialstyrelsen). However, it seeems to us that these guidelines should be improved in order to act as compass for decision-making as well as a tool to raise awareness among civil servants. Beside sectoral guidelines, it could be adequate to also bring awareness on the issue in the general ethical guidelines enacted by the Swedish Agency for Public Management (Statskontoret) in the handbook *Ethical foundations of the state – Professional values for good governance* (Den statliga värdegrunden – professionella värderingar för en god förvaltningskultur).

for public servants to have a critical approach to the data available and collected, particularly in view of the risk of distortion.

Public servants should furthermore be made aware that the search and collection of data on social media carry risks for individuals' privacy but also, beyond that, for democracy. They should be made aware of the loss of confidence in the State these practices may lead to. They should also be enlighted of the risks of people's self-restraint in the exercise of their freedoms to behave and communicate.

Finally, it would be appropriate to remind public servants of their duty to act professionally. They should not It is not for them to give in to the ordinary curiosity of Internet users. The respect of deontology is in this matter essential for establishing a good relationship between the citizen and the public official in charge of his or her case and, more generally, for establishing citizens' confidence in State representatives.

4 Conclusion

It seems inevitable, and sometimes appropriate, for public authorities to take advantage of the opportunities provided by new technologies, including search engines and new social platforms, to investigate information on citizens. The *ordinary* shape of such administrative investigative methods (in that public authorities make use of tools and digital platforms made available to everyone, and that, like everyone, public officials have acquired the habit of using search engines) must not obscure the potentially detrimental nature of such practices for privacy, for citizens'confidence in the state and for democracy if they are not properly framed. It is high time for national legislators to seize upon this issue in order to avoid the insidious development of Orwellian surveillance tools. The ongoing drafting of complementary measures to the GDPR constitutes a perfect opportunity for European national legislators to enact adequate rules and for the public authorities in charge of Internet-based administrative investigations to develop supplementing guidelines.[44]

44 The instances involved in the drafting of measures for accompagnying the GDPR (and not least the appointed committee of inquiry) should only focus on the drafting of a general Act, thus setting aside the sectoral regulations. *See* Kommitteedirektiv 2016:15. The legislative work resulted in the enactment of the *Act with supplementing provisions to the EU Data Protection Regulation (in short the Data Protection Act, Lag med kompletterande bestämmelser till EU:s dataskyddsförordningen* (2018:218).