WESTFÄLISCHE WILHELMS-UNIVERSITÄT
Institut für Informations- , Telekommunikations- und Medienrecht (ITM)
- Zivilrechtliche Abteilung -
Prof. Dr. Thomas Hoeren

Leonardo-Campus 9

D-48149 Münster
Tel.: +49/2 51/83-38600
Fax: +49/2 51/83-38601
Email: hoeren@uni-muenster.de

24. Oktober 2013

Comments to the Disclosure of Information and Protection of Whistle-blower Bill 2013.

1. The Althingi´s Judicial Affairs and Education Committee invited me to comment upon the Disclosure of Information and Protection of Whistleblower Bill 2013. Since 1997 I am working as a media law professor at the University of Münster (Germany) and as a former judge at the Court of Appeal of Düsseldorf (Media Law Senate). In the past, I have been a visiting professor at the Universities of Akureyri and Iceland and as the central coordinator of German-Icelandic relationships at the University of Münster.

2. My comments are based upon the Icelandic version of the draft.[1] I organized a private translation of the text into English; but I cannot guarantee that I have understood all the details of the draft correctly. I have already made comments on the previous draft[2]. As this draft obviously has not been changed, I will repeat most of my comments in the following considerations. The report added to the bill mentions that the comments received in the past were successful. Agreeing with the general tendency of the bill, I have to admit that I have never accepted the details of the bill which needs clarifications and corrections.

---

[1] http://www.althingi.is/altext/143/s/0012.html
[2] http://www.althingi.is/altext/141/s/0572.html

3. Whistleblowing has become a significant feature of international complaince systems. This particularly applies to international corporations bound by the US Sarbanes-Oxley Act (hereafter: "SOX").[3] SOX requires publicly held US companies and their EU-based affiliates, as well as non-US companies, listed in one of the US stock markets, to establish within their audit committee *"procedures for the receipt, retention and treatment of complaints received by the issuer regarding accounting, internal accounting controls or auditing matters; and the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters".*[4] In addition, Section 806 of SOX lays down provisions aimed at ensuring the protection for employees of publicly traded companies who provide evidence of retaliatory measures taken against them for making use of the reporting scheme.[5] The Securities and Exchange Commission (SEC) is the US authority in charge of monitoring the application of SOX.[6] In consequence, mayor Icelandic companies already have to install whistleblowing systems in compliance with the SOX requirements.

4. If the Icelandic Parliament has to draft a whistleblowing act, it has to take its existing international obligations into consideration. In its Resolution 1729 (2010) on the protection of "whistle-blowers" the Parliamentary Assembly of the Council of Europe[7] stressed the importance of "whistle-blowing" as an opportunity to strengthen accountability, and bolster the fight against corruption and mismanagement, both in the public and private sectors. It invited all member States to review their legislation concerning the protection of "whistle-blowers", keeping in mind the following guiding principles:

   - the definition of protected disclosures shall include all bona fide warnings against various types of unlawful acts, including all serious human rights violations which affect or threaten the life, health, liberty and any other legitimate interests of individuals as subjects of public administration or taxpayers, or as shareholders, employees or customers of private companies;

---

[3] Cf. *Saelens/Galand*, (2006) 3 European Company Law, Issue 4, 170.
[4] Sarbanes-Oxley Act, Section 301(4).
[5] For the effect of SOX on whistleblowing see *Mowrey* et al., 1 William & Mary Business Law Review, 431-449 (2010)
[6] Sarbanes-Oxley Act, Section 406.
[7] Accessible at: http://assembly.coe.int/main.asp?link=/documents/adoptedtext/ta10/eres1729.htm.

- the legislation should therefore cover both public and private sector whistle-blowers [...], and it should codify relevant issues in the following areas of law: employment law – in particular protection against unfair dismissals and other forms of employment-related retaliation; [...]
- This legislation should protect anyone who, in good faith, makes use of existing internal whistle-blowing channels from any form of retaliation (unfair dismissal, harassment or any other punitive or discriminatory treatment).
- Where internal channels either do not exist, have not functioned properly or could reasonably be expected not to function properly given the nature of the problem raised by the whistle-blower, external whistle-blowing, including through the media, should likewise be protected.
- Any whistle-blower shall be considered as having acted in good faith provided he or she had reasonable grounds to believe that the information disclosed was true, even if it later turns out that this was not the case, and provided he or she did not pursue any unlawful or unethical objectives.

5. In addition, Iceland is a signatory of the European Convention of Human Rights[8] and thus in its effort to legislation concerning whistleblowing bound by the provisions of this Convention.[9] The pertinent right to freedom of expression as provided in Article 10 of the Convention, reads as follows:

> "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent states from requiring the licensing of broadcasting, television or cinema enterprises.
>
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of

[8] Accssible at: http://eycb.coe.int/Compass/en/pdf/6_8.pdf.
[9] *Cameron*, (2008) 14 European Public Law, Issue 4, pp. 465 ff.

information received in confidence, or for maintaining the authority and impartiality of the judiciary."

The European Court for Human Rights (ECHR) ruled by judgment dated 21 July 2011 (no. 28274/08)[10] that employees who publicly disclose deficiencies within the enterprise of their employer cannot be terminated without notice.[11] However, the Court determined a number of factors when assessing the proportionality of the interference in relation to the legitimate aim pursued (66).

In the first place, particular attention shall be paid to the public interest involved in the disclosed information. The Court reiterates in this regard that there is little scope under Article 10 § 2 of the Convention for restrictions on debate on questions of public interest (66).

Moreover, freedom of expression carries with it duties and responsibilities and any person who chooses to disclose information must carefully verify, to the extent permitted by the circumstances, that it is accurate and reliable (67).

On the other hand, the Court must weigh the damage, if any, suffered by the employer as a result of the disclosure in question and assess whether such damage outweighed the interest of the public in having the information revealed (68).

The motive behind the actions of the reporting employee is another determinant factor in deciding whether a particular disclosure should be protected or not. For instance, an act motivated by a personal grievance or personal antagonism or the expectation of personal advantage, including pecuniary gain, would not justify a particularly strong level of protection (69).

Lastly, in connection with the review of the proportionality of the interference in relation to the legitimate aim pursued, a careful analysis of the penalty imposed on the applicant and its consequences is required (70).

6. In the light of these considerations, the Disclosure of Information and Protection of Whistleblower Bill Act has to be applauded in general. It highlights the social and economic importance of internal and external whistleblowing systems in a very courageous and highly sophisticated manner. It is an important element of the IMMI

[10] Accessible at: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-105777.
[11] For the US approach see the US Supreme Court decision Garcetti v. Ceballos 547 U.S. 410 (2006).

plans which are, in my view, a unique and fascinating attempt to create very modern media law regulations in Iceland.[12]

7. However, the draft does not sufficiently take into consideration the implications of whistleblowing systems on fundamental rights. While emphasizing the purpose of "encouraging the sharing of information", it does not contain any reference to personality rights or rights to privacy. Whistleblowing concepts might be protected under the freedom of expression rights. But they often and severely intermingle with said rights and right to privacy (see below).[13]

   Unfortunately, the draft does not consider the interference of whistleblowing with data protection regulations, especially the Icelandic Data Protection Act. Obviously, the Icelandic Data Protection Commissioner has not considered the draft. This is astonishing as the Commissioner has been involved in drafting the EU Article 29 group paper on whistleblowing in 2009 (Working Paper 117)[14].
   In this paper, the Article 29 group only deals with internal whistleblowing systems. The paper mentions a lot of strategies for balancing internal whistleblowing procedures with data protection requirements.

   > "The application of data protection rules to whistleblowing schemes implies deal with the question of the legitimacy of whistleblowing systems (1); application of the principles of data quality and proportionality (2); the provision of clear and complete information about the scheme (3); the rights of the person incriminated (4); the security of processing operations (5); the management of internal whistleblowing schemes (6); issues related to international data transfers (7); notification and prior checking requirements (8)" (p.7)

8. The draft does not consider the legal status of external whistleblowing systems in depth. It simply states that these platforms should be governed by the same rules as those on whistleblowers (Art. 6). This approach is not convincing:

---

[12] See my comments on the first IMMI plans in CRi 2010, 141; published at http://www.uni-muenster.de/Jura.itm/hoeren/veroeffentlichungen/hoeren_veroeffentlichungen/IMMI_The_EU_Perspective.pdf
[13] Cf. *Runte/Schreiber/Held/Bond/Dana/Flower*, CRi 2005, 135, 136.
[14] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf.

Whistleblowing internet platforms are subject to press law and as such bound to the same duties and privileged by the same rights as traditional press.[15] This classification can be based upon the judgements for instance of the European Court of Justice. In the Satakunnan case[16], the Court ruled that the term "journalistic purposes" has to be interpreted broadly due to the significance of freedom of expression in a democratic society. It should include "the mere fact of making raw data available". For being classified, it is enough that the "information communicated relates to a public debate which is actually being conducted". This approach points to an inclusion of whistleblowing platforms into existing press law regulations.[17] Hence, if treated equally, the same principles as for the traditional press have to apply to whistleblowing platforms. This involves application of the standards for weighing data protection and privacy law on the one and freedom of press on the other hand, as determined by the European Court of Justice. The platforms have to consider and check the value of documents and not only in good faith pursuant to Art. 5, but according to the same ethical and legal standards as the traditional press.[18] As "press", whistleblowing platforms have in particular to consider the presumption of innocence. In return, they get the same privileges as "press" including the protection of sources or exemptions from the application of data protection laws. [19]

9. The regulation in Art. 4 on internal whistleblowing follow the rules established by the Council of Europe (Resolution 12729 (2010), see above). But several details need further clarification. Art. 4 (3) of the draft sanctions unlawful actions as well as violations of ethical standards. This term is very vague and unclear. Further, it is superfluous to refer to "fraudulent or corrupt" behaviour as such behaviour in general violates the law as well. The "abuse of power"-concept is very vague. Either abuse of power is sanctioned by law or it is lawful and thus not a reasonable object of whistleblowing. Or the concept relates to all cases of mobbing. The reference to "threats to health" is misleading: It is i.e. questionable whether a medical

[15] It is interesting to note that Icelandic whistleblowing platforms call themselves "press" (i.e. the "Associated Whistle Blowing Press").
[16] Case C-73/07 *Tietosujvaltuutettu v Satakunnan Markkinopörssi Oy and Others.*
[17] ECJ , Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Case C-73/07, I-09831 paragraph. 56.
[18] Cf. *Infobank*, (1995) 16 Business Law Review, Issue 2, 41, 48.
[19] There is a lot of literature focusing on external whistleblowing as press; see for instance *Corneil*, 41 Cal. W. Int'l L.J. 477 (2010-2011); *Bacon/Nash*, 21 *Australian Journalism Review,* 10 (1999) with further references.

operation/threat to health should be a reasonable object of whistleblowing systems since any medical treatment is such a "threat to health".

The draft seems to underestimate the impact of internal whistleblowing systems on data protection[20], especially the Icelandic Data Protection Act. According to Article 21, the data subject has the right to access the sources of information. This right does not apply of the data subjects interest is deemed secondary to "vital public or private interests" (Art. 21 (2)). It has to be clarified with the help of the Data Protection Commissioner under which circumstances internal whistleblowing is regarded as a case of a "vital public or private interest". In addition, Art. 25 give the data subject a right to rectification and deletion of incorrect and misleading data. According to Art. 26, the data processor has to erase personal data where there is no longer a reason to preserve the data. All these instruments have to be evaluated in the face of whistleblowing considering the Working Paper 117 of the Article 29 Group mentioned above.[21]

In this context, I suggest to integrate the institution of an Icelandic Whistleblowing Ombudsman into the act. The Ombudsman might be extremely important and valuable within internal whistleblowing systems.[22] He might be installed as an internal institution within a company. This is for instance the model used in the United States where internal whistleblowing is coordinated via an Inspector General according to Sec. 7 des Inspector General Act of 1978.[23] Furthermore, it might be possible to create the institution of an independent official Whistleblowing Ombudsman for all organizations. Especially in the comparably small economic structure of Iceland, it is possible to allow all residents to send internal information to the ombudsman. He will then check the validity of the complaint and contact the corporations or institutions concerned. The model could be structured in analogy to the US Office of Special Counsel (OSC).[24]

---

18 See the analysis made by the French Data Protection Committee CNIL from 2005; published at http://www.cnil.fr/fileadmin/documents/en/CNIL-recommandations-whistleblowing-VA.pdf

16 The Working Paper has been subject of a controversy between the US SEC and the European Data Protection Authorities. See the letter of *Ethiopis Tafara* to Peter Schaar of 8 June 2006 published on https://www.sec.gov/about/offices/oia/oia_rulemaking/schaar_letter_060806.pdf

17 See *Steigert*, Data protection in internal whistleblowing systems, Dissertation Münster 2013 (to be published soon).

[23] Inspector General Act 1978 (5 U.S.C. Appendix).

[24] Http://www.osc.gov/Intro.htm. See *Fisher*, 43 Rutgers L. Rev. 355, 371 (1991).

10. Art. 5 of the draft, by using the word "or", relies heavily on alternative possibilities which may prove to be detrimental. The article relates to an offence against public interest without any further definition of this term. It is not clear whether a "public interest" is to be construed ex ante or ex post. For instance Pedro Noel, one of the organizers of the whistleblowing platform ljost.is, once gave an interview in Grapevine which took place in a coffee shop in Reykjavik. There, he explained that whistleblowing systems should be allowed to publish any documents relating to tax law violations made by the coffee shop owner on the web.[25] There remain doubts as to whether any violation of tax law immediately constitutes a violation of public interests. The coffee shop owner might have "forgotten" to pay 10 Kroner income tax. Is that a matter of public interest? Who is deciding upon the classification of a "public interest"? The whistleblowing platform? The court - ex post – after years of court proceedings? What is happening if there is no tax law violation at all and the allegations are wrong?

    Furthermore, the social effects[26] of external whistleblowing systems, especially internet platforms[27], are left out of consideration. If mentioned in such an internet platform, an individual's name will be stored and made available for decades. Due to the almost instant availability of data via search engines (i.e. Google), the name and the "whistleblowing story" connected with it can be accessed without further ado. Even if such data were deleted afterwards it may have been copied and mirrored on other servers. Hence, an individual loses every chance of his actions, which were believed in good faith (cf. Art. 5 of the draft) to have violated the law, ever being forgotten.[28]

    Art. 5 allows, by using "or", the press publication of documents without public interest, even when based upon violations of law, for instance where the whistleblower has reason to believe that internal systems are "ineffective". It is not defined what "ineffective" means. The detrimental uncertainty of this blanket clause can be

---

[25] http://grapevine.is/Home/ReadArticle/Shine-A-Light: "Suppose that the owners of this cafe aren´t paying taxes. Somebody who works here, who has access to this information, could scan those documents and send them to this (= our) platform."
[26] *Fleischer*, (2012) 9 European Company Law, Issue 4, 200.
[27] In my understanding, the Bill unfortunately does not distinguish between external systems and the publication via press/internet whistleblowing platforms.
[28] *Saelens/Galand*, (2006) 3 European Company Law, Issue 4, 170, 173.

demonstrated in the following example: A Bonus employee has stolen one chewing gum in the shop. This is definitely not an action violating public interest laws. The employer is notified via the internal whistleblowing system that the gum has been stolen - but he is not interested in the case and remains inactive. This is to a certain degree "ineffective". However, it is not reasonable for the whistleblower to be allowed to publish these facts on the web with the full name and for a long period of time, for all Icelanders to access.

These examples demonstrate that the authors of the Bill apparently have not considered the decision of the ECHR from July 2011 (see above). There the Court held that the damage caused by whistleblowing, the proportionality and the motives of the whistleblower have to be considered before publishing information to the public. Furthermore, the Court believed that the whistleblowing platform "must carefully verify" the accuracy and reliability of the data. All these criteria are not mentioned in the Bill.

Münster, the 17th of January 2013

(Prof. Dr. Thomas Hoeren)