Whistleblowing, hotlines and transferring data across borders

Paul Lanois

In today's global and connected economy, a change in the legal landscape of one country can have significant repercussions on another country. An example of this new world we live in is the **Sarbanes-Oxley Act of 2002**[1], which was enacted by the Congress of the United States to restore investor confidence and curb various corporate excesses following the Enron scandal that unfolded in 2001. However, the impact of the Sarbanes-Oxley Act extends well beyond the sole territory of the United States.

Since the Sarbanes-Oxley Act does not contain an express exemption for foreign private issuers, multinational groups listed on U.S. stock exchanges are required to set up specific procedures in their subsidiaries in accordance with the Sarbanes-Oxley Act[2]. In particular, **section 301(4) of the Sarbanes-Oxley Act** imposes the implementation of a confidential, anonymous reporting mechanism:

> "*Each audit committee shall establish 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*."

However, the time when a multinational could simply "impose" the same policy around the world with little pushback has definitively passed. Instead it now has to bear in mind local specificities when drafting a global code of conduct.

According to the **EU Directive 95/46/EC** dated 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[3], member states must protect their citizens' "fundamental rights and freedoms, notably the right to privacy" regarding the processing of their own personal data[4]. Among other things, the EU Directive sets forth a number of requirements:

- An individual has a right to know when his personal data is being collected and which data is collected, he has the right to access personal details concerning him;
- Personal data has to be processed fairly and lawfully;
- Personal data has to be obtained only for one or more specified and lawful purposes;
- Personal data must be kept for no longer than is necessary and must be accurate and up to date;
- Personal data must be kept secure and appropriate technical and organisational measures must be taken to ensure its safety; and

[1] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745, 30 July 2002, 15 U.S.C. § 7201 et seq.
[2] See for example Paul Lanois, *Between a Rock and a Hard Place: The Sarbanes-Oxley Act and its Global Impact*, Journal of International Law and Policy, Vol. V, available at: https://www.law.upenn.edu/journals/jil/jilp/articles/5-1_Lanois_Paul.pdf
[3] EU 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, available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046
[4] See also Paul Lanois, *Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?*, Northwestern Journal of Technology and Intellectual Property, Vol. 9, Issue 2 (2010), p. 29 et seq.; Paul Lanois, *Privacy in the age of the cloud*, Journal of Internet Law, Vol. 15, Issue 6, p. 3 et seq.

- Personal data should not be transferred outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal data.

Companies listed on a stock exchange in the United States were faced with an interesting dilemma regarding how to effectively maintain a global compliance program, especially bearing in mind the restrictions imposed by European data protection legislation.

On the one hand, U.S. law obliges them to implement certain procedures to enable employees to report misconduct; and on the other hand; European law imposes mandatory restrictions on whistleblowing and hotlines. These opposing viewpoints put multinationals between the proverbial "rock and a hard place", since they are put in the less than enviable position of having to choose between violating U.S. law (the Sarbanes-Oxley Act) or violating European regulation.

The often cited illustration of such conflict is the decision known as the "**Wal-Mart Judgment**"[5] issued by the Labor Court of Wuppertal on 15 June 2005. Wal-Mart decided to implement a Code of ethics in all of its subsidiaries, including in Germany. One of the provisions of this Code of ethics was that any violations could be reported anonymously via a hotline established especially for this purpose. The problem is that under German Labor law, the employer and the works council each have a right of codetermination, which means each has an equal say in determining work conditions. The Labor Court found that the establishment of a hotline fell within the scope of the codetermination rights of the works council and because the works council was not involved in the decision process, Wal-Mart's hotline was invalid. This case is a striking example demonstrating how legal requirements in one country may be struck down in other countries for violations of local law.

Likewise, in two cases involving **McDonald's Corporation**[6] and **Exide Technologies**[7], France's data protection agency (the "CNIL") held that the hotlines that the companies sought to implement to enable employees to report, anonymously, inappropriate acts from the management were illegal under French and European privacy legislation. According to the CNIL, an anonymous hotline system increases the risk of "slanderous denunciation". Cultural reasons explain the reluctance of EU countries to accept hotline systems: whereas hotlines are considered a valuable tool to obtain information from employees; in Europe, they bring up dark reminders of World War II where people incriminated their neighbours during the Nazi occupation.

In order to resolve the predicament that multinationals were facing, the French data protection agency first published guidelines in November 2005 setting forth the conditions under which whistleblowing provisions would be permitted in accordance with the French Act on data protection. On 8 December 2005, it further issued a decision known as the **Single Authorization AU-004**[8], providing a blanket authorization for whistleblowing systems that adhere to the conditions imposed by the CNIL. The company simply has to self-certify their compliance with the conditions set forth by the CNIL, and once the CNIL issues an acknowledgement of filing, usually within a week, the company may immediately implement the whistleblowing scheme, without any further review from the CNIL.

[5] Wal-Mart, Labor Court of Wuppertal, 15 June 2005
[6] McDonald's Corporation, CNIL Decision n° 2005-110, 26 May 2005, available (in French) at: http://www.cnil.fr/documentation/deliberations/deliberation/delib/73/
[7] Exide Technologies, CNIL Decision n° 2005-111, 26 May 2005, available (in French) at: http://www.cnil.fr/documentation/deliberations/deliberation/delib/74
[8] CNIL Decision n° 2005-305, Single Authorization AU-004, 8 December 2005, available (in French) at: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000264462

Whistleblowing systems which do not meet these conditions would require a specific authorization from the CNIL: in other words, if a company wishes to implement a whistleblowing system which does not mean the requirements of the CNIL, the company would have to undergo a complex and lengthy approval process.

The scope of the Single Authorization AU-004 was originally limited to financial, accounting, banking, and anti-bribery areas, as well as compliance with Section 301(4) of the Sarbanes-Oxley Act. On **14 October 2010**[9], the CNIL extended the scope of the Single Authorization to include the prevention of anti-competitive practices as well as compliance with the Japanese *Financial Instrument and Exchange Act* dated 6 June 2006, also known as the "Japanese SOX" or "J-SOX". On **30 January 2014**[10], the CNIL further amended the Single Authorization by removing the reference to the Sarbanes-Oxley Act and the Japanese SOX, while extending the scope of the authorization to cover workplace discrimination, harassment, health, hygiene and safety as well as environmental protection.

It is not possible to rely on the Single Authorization AU-004 if the scope of the whistleblowing system extends beyond the authorized areas. On 8 December 2009, the French Supreme Court[11] ruled that the whistleblowing procedures that **Dassault Systèmes** sought to implement in its Code of Business Conduct were invalid, on the grounds that Dassault's whistleblowing system not only covered the areas set forth in the Single Authorization AU-004, but also allowed whistleblowing reports as long as the vital interests of the company or the physical or moral integrity of an employee was at stake.

The French Supreme Court further held that the employees of Dassault were not informed in sufficient detail of the legal protections related to whistleblowing, in particular the right of the individual who is the subject of a complaint to access his data and request correction or deletion of the data.

Even if the CNIL approves a whistleblowing system, a French court may still find it contrary to French law. On 23 September 2011, the Court of Appeals of Caen[12] upheld a decision to suspend a whistleblowing program implemented by the French company **Benoist Girard**, an affiliate of the Stryker Corporation, even though the CNIL had actually inspected and approved the program prior to implementation. The Court of Appeals held that Benoist Girard's whistleblowing program was outside of the scope of the Single Authorization AU-004 because the whistleblowing platform allowed users to "*report anonymously to the company any suspected bad behaviour or other problems*" or "*compliance issues relating to the company's code of conduct and ethics policies*". The Court also noted that the system still allowed the submission of a report in relation to any type of misconduct. The Court further held that the employees of the company were not informed in sufficient detail of the legal protections related to whistleblowing, and that the workers' committee had not been properly consulted. For all of these reasons, the whistleblowing program was declared unlawful.

---

[9] CNIL Decision n° 2010-369, 14 October 2010, available (in French) at: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023175565

[10] CNIL Decision n° 2014-042, 30 January 2014 , available (in French) at: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028583464

[11] *La Fédération des travailleurs de la métallurgie CGT / Dassault systèmes*, Case n° 2524, Labour Law Chamber of the French Supreme Court, 8 December 2009, available (in French) at: https://www.courdecassation.fr/jurisprudence_2/chambre_sociale_576/2524_8_14408.html

[12] Benoist Girard / CHSCT, Labour Law Chamber of the Court of Appeals of Caen, 23 September 2011, available (in French) at: http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3236

In relation to anonymous reporting, the CNIL's indicated in its decision on 30 January 2014 that by default, a whistleblowing program should require the person making a report to identify himself, but a report from a person who wishes to remain anonymous may be accepted if the following conditions are met: if the seriousness of the alleged facts is demonstrated, if those facts are sufficiently detailed, and if the report is processed with additional precautions, for example, the initial receiver of the report should assess whether it is appropriate to disclose the facts within the whistleblowing framework prior to doing so.

In light of these decisions, it is apparent that companies wishing to implement a whistleblowing program in France need to ensure that it does not exceed the scope set forth in the CNIL's Single Authorization AU-004.