BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 11, Number 12 December 2011

French Appeals Court's Suspension Of U.S. Company's Whistleblowing Scheme Despite CNIL Approval: Reasons And Implications

By Olivier Proust, of Hunton & Williams LLP, Brussels.

On September 23, 2011, the Labor Chamber of the Caen Court of Appeals upheld a decision suspending a whistleblowing scheme implemented by Benoist Girard, a subsidiary of the U.S. group Stryker, even though the French data protection authority, the Commission nationale de l'informatique et des libertés (CNIL), had inspected and approved the scheme before its implementation (*see WDPR, October 2011, page 19*).

The Court's reasons for suspending the whistleblowing scheme are mainly based on the company's failure to properly inform the employees collectively (through the Works Council) and individually, and the subsequent violation of several labor law provisions.

This decision illustrates how whistleblowing schemes may trigger the application of multiple laws (*e.g.*, privacy, data protection, labor, criminal).

This decision illustrates how whistleblowing schemes may trigger the application of multiple laws (*e.g.*, privacy, data protection, labor, criminal). In the context of whistleblowing, complying with different laws may be challenging for companies, particularly when such laws conflict with one another.

In this decision, it is interesting to note that, although the CNIL considered the whistleblowing scheme to be compliant with data protection law, the Court ruled that it did not comply with labor law.

A Whistleblowing Scheme Must Be Transparent Vis-à-Vis the Employees and Their Representative Bodies

In this decision, the Court considered that the employees of the French subsidiary had not received proper information regarding the whistleblowing scheme and, in particular, were not properly informed about their privacy rights (*i.e.*, right to access and rectify their personal data) both in the company's internal rules and in prior notices communicated to them.

However, the main reason for suspending the whistleblowing scheme was the fact that the company had not properly consulted the employee representative bodies (*i.e.*, the Works Council and the Employees' Hygiene & Safety Committee) before implementing the finalized version of its whistleblowing scheme.

Under French labor law, there are a number of circumstances in which companies are legally required to consult with the Works Council regarding the processing of personal data in the workplace. Specifically, compa-

nies must inform the Works Council about their processing activities involving employee data.[1] The Works Council must also receive prior notice of, and be consulted on, any introduction of new technologies to the workplace that may have an impact on the working conditions,[2] and any measure or technique that an employer intends to implement for the purpose of monitoring the employees' activities.[3]

In France, whistleblowing schemes are generally considered to be potentially invasive upon the employees' privacy, and thus companies are required to inform the Works Council and obtain its opinion before implementing such a scheme.[4] Failure to comply with these requirements constitutes an obstruction to the Works Council's prerogatives, which may be criminally sanctioned. In certain situations, the Employees' Hygiene & Safety Committee ("CHSCT") must also be consulted, for example, when a decision is taken that may impact the employees' health, safety or working conditions.[5]

In the given case, Benoist Girard had consulted the Works Council several times before adopting its whistleblowing scheme. It also chose to consult the CHSCT on a voluntary basis, even though companies are not required to do so for whistleblowing schemes.

However, the Court considered that the company had failed to properly consult the employee representative bodies, and had not obtained their opinion as required, on the grounds that those bodies were not consulted regarding the final changes made to the company's online reporting form.[6] As a result, companies must be transparent with the Works Council at all times, since even minor changes to the scheme may have serious consequences if the Works Council was not properly consulted.

The Scope of a Whistleblowing Scheme Must Be Limited to Pre-Defined Areas

Under French law, whistleblowing schemes must necessarily be construed to limited and pre-defined areas, namely: finance, accounting, banking, fight against corruption, anti-bribery, compliance with U.S. Sarbanes-Oxley Act regulation and, ever since the revision of the CNIL's single authorization AU-004,[7] the prevention of anti-competitive practices and compliance with the Japanese Financial Instrument and Exchange Act. On the contrary, whistleblowing schemes that do not fall within these pre-defined areas must receive the CNIL's *ad hoc* approval.

French courts usually interpret this provision strictly and rarely grant exceptions. In a recent court decision involving Dassault Systèmes, the Court of Cassation ruled that, once a company has self-certified to the CNIL's single authorization AU-004, it cannot use its whistleblowing scheme for purposes other than those defined in the CNIL's authorization (*e.g.*, to facilitate the reporting of incidents that pose a serious threat to the vital interests of the company, or to the moral or physical integrity of its employees).[8] This decision caused the CNIL to amend the scope of its single authorization AU-004 so as to be in line with the Court's ruling[9] (*see WDPR, January 2011, page 25*).

In the Benoist Girard case, it appeared that the information posted on the homepage of the website used by the company to report incidents was inconsistent with the information notice that had previously been provided to the employees. The notice informed employees that the whistleblowing scheme was limited to matters relating to accounting, finance, banking and the fight against corruption, whereas the website did not clearly limit the scope of reports to those areas and allowed employees to report various types of "suspected bad behavior and other problems" or "compliance issues relating to the company's code of conduct and ethics policies." Benoist Girard was ultimately sanctioned for lack of clarity and consistency in the information provided to employees, which illustrates that companies must not only inform their employees, but also must do so in a clear, comprehensive and consistent manner.

Furthermore, the Court considered that this lack of clarity regarding Benoist Girard's whistleblowing hotline had unavoidably led to various types of denunciations within the company. To avoid any unlawful use of its whistleblowing hotline, the company chose to filter the reports received and delete those that did not fall within the authorized scope. In doing so, employees were also encouraged to bring such reports to the attention of their local human resources manager. For this reason, the Court argued that the company had crossed the boundaries of its legal duties in a whistleblowing context and should have limited its action to reminding employees about the exact scope of the reporting line without encouraging them to pursue their reports with another person or department.

Therefore, companies must be cautious when processing whistleblowing reports. Based on the Court's ruling, the scope of a whistleblowing scheme must be strictly limited to the areas defined in the CNIL's single authorization AU-004. Any data relating to an alert that falls outside the scope of the whistleblowing scheme must be immediately deleted or archived.[10] As a result, whistleblowing schemes may not be used to forward unrelated reports to other competent departments. In this respect, the Court's ruling appears to contradict the CNIL's guidelines,[11] which state that employees may be redirected to a competent department within the company if necessary. Thus, to avoid any unlawful use of a whistleblowing hotline, companies are advised to implement an internal standard operating procedure explaining the scope, purpose and limits of the whistleblowing scheme to the employees operating it.

French Court Overrules CNIL Decision

Companies that self-certify to the CNIL's single authorization make a formal undertaking that their whistleblowing scheme complies with the CNIL's pre-defined conditions. In most situations, the CNIL grants applicants an approval without formally reviewing their whistleblowing schemes. However, in the Benoist Girard case, the CNIL did review and inspect the company's

   ISSN 1473-3579

whistleblowing scheme before authorizing it. To this end, the CNIL conducted a series of tests and ultimately decided that the measures implemented by the company regarding the security, retention and deletion of data complied with the requirements of the Data Protection Act.

Despite the CNIL's decision, the Court considered that this whistleblowing scheme had been unlawfully implemented.

This is not the first time that a French court has overruled a CNIL decision approving a whistleblowing program. On December 8, 2009, the French Court of Cassation struck down several provisions of a whistleblowing scheme implemented by Dassault Systèmes, despite the company having self-certified to the CNIL's single authorization AU-004 setting out the pre-established conditions for whistleblowing schemes.[12]

In this context, compliance with data protection law is not sufficient to guarantee that a whistleblowing scheme is lawful, since it may also trigger the application of other laws (including labor laws). The French Data Protection Act limits the supervisory powers of the CNIL to verifying compliance with data protection law and such powers do not extend to other areas of law.[13] Consequently, a decision by the CNIL approving a whistleblowing scheme does not exempt companies from also verifying compliance with other applicable laws, particularly when their data processing activities involve the processing of employee data. As often is the case, privacy and data protection are at cross purposes with other areas of law, and, thus, companies risk being sanctioned if they analyze this issue solely from a data protection point of view.

Conclusion

In a globalized world, companies must be cautious when implementing their whistleblowing schemes across jurisdictions. Currently, there is no harmonized legal framework for whistleblowing schemes in the European Union, which means that companies must tailor their whistleblowing schemes to the local laws of each country in which their scheme is operating, or may face sanctions for failing to do so. At a minimum, this exercise can be particularly burdensome and costly. In the worst-case scenario, compliance with the laws of each country becomes a challenge and companies often choose a common denominator that applies across jurisdictions.

In conclusion, it has become increasingly complex to operate a whistleblowing scheme in today's world, with multiple laws applying and often conflicting with one another. In the past, this topic has caused some tension between the United States and the European Union due to diverging philosophical views about corporate investigations.[14] Soon, however, the European Commission will release its proposal for a new Regulation on the protection of personal data in the European Union,[15] the purpose of which is to harmonize the application of the data protection principles within the Member States (*see analysis of the draft Regulation in this issue*). Data protection authorities may use this opportunity to streamline the approval of whistleblowing schemes and facilitate their use in the European Union.

NOTES

[1] Article L.2323-32 of the French Labor Code.

[2] Article L.2323-13 of the French Labor Code.

[3] Article L.2323-32 of the French Labor Code.

[4] The CNIL's single authorization AU-004 states that data controllers have an obligation to consult the Works Council on whistleblowing issues.

[5] Article L.4612-8 of the French Labor Code.

[6] After consulting the Works Council, Benoist Girard amended several fields in the scroll-down menu of its online reporting form (*i.e.*, those named "questions relating to the company's vital interests" and "topics for concern"). The Court viewed those changes as potentially impacting the working conditions of employees and therefore considered that the company should have consulted the Works Council.

[7] See Olivier Proust, "French revised framework for whistleblowing: analysis", Data Protection Law & Policy, February 2011.

[8] See Cour de cassation, chambre sociale, 8 décembre 2009, n° pourvoi 08-17191, available at: http://www.legifrance.gouv.fr

[9] See Délibération n°2010-369 du 14 octobre 2010 modifiant l'autorisation unique n°2005-305 du 8 décembre 2005 n°AU-004 relative aux traitements automatisés de données à caractère personnel mis en oeuvre dans le cadre de dispositifs d'alerte professionnelle.

[10] Article 6, Délibération n°2005-305 du 8 décembre 2005 portant autorisation unique de traitements automatisés de données à caractère personnel mis en ceuvre dans le cadre de dispositifs d'alerte professionnelle.

[11] CNIL, FAQ sur les dispositifs d'alerte professionnelle. Please note that, following the CNIL's revision of its single authorization AU-004, these guidelines are no longer available on the CNIL's website.

[12] See above, note 8.

[13] See Article 11, French Data Protection Act.

[14] See WP 117, Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, adopted by the Article 29 Working Party on February 1, 2006.

[15] See Hunton & Williams' Privacy and Information Security Law Blog at: http://www.huntonprivacyblog.com/2011/12/articles/european-commission-drafts-to-reform-the-eu-data-protection-framework-enter-interservice-consultation/

Olivier Proust is an Associate with Hunton & Williams LLP, Brussels, and a member of the Paris Bar. He may be contacted at oproust@hunton.com.