SROUJI AVOCATS
AVOCATS À LA COUR

www.sroujiavocats.com

The changing compliance landscape for international companies in Europe: whistleblowing and data protection under French Law

September 2019

Célia Tellaa, Avocate à la Cour
Joseph Srouji, Avocat à la Cour

Introduction

In a country where companies were able to deduct from turnover *pots-de-vin* paid for "new business" (also politely called "facilitating payments") until 2000 when France adopted the OECD's Anti-Bribery Convention (officially the "Convention on Combating Bribery of Foreign Public Officials in International Business Transactions")[1], it comes with some scepticism how effective the wave of new French laws and regulations will be in the fight against corruption. But times are indeed changing, and European governments realise that weeding out corrupt practices is increasingly required if companies are to effectively compete on the global stage.

The most significant legislative salvo against corruption, and one that has received significant press, is known as "*Loi Sapin II*" (Act No 2016-1691 of 9 December 2016 relating to transparency, fight against corruption and modernisation of economic life). Shortly thereafter the "*Loi Vigilance*" was adopted to reinforce companies' internal compliance governance (Act No 2017-399 of 27 March 2017 relating to the duty of surveillance of parent companies and contracting companies).

In parallel to the anti-corruption initiatives, the European Union (EU) moved to overhaul its data protection regime, adopting the General Data Protection Regulation (GDPR) on 27 April 2016 (coming into force on 25 May 2018). It is important to take note of this complementary legislation since it's based on the same logic for companies to implement internal compliance measures of accountability.

But the data protection regime in some ways competes against requirements under *Loi Sapin II*, most notably in regards to whistleblowing programs as we will see later in this article. And despite its good intentions, these new laws tend generally to overlap and, in some cases, contradict each other.

It remains to be seen if these new laws, and the oversight that comes with them, will have their intended effect, or will just be another box to tick and cost to provision for doing business in Europe. While the scope of these various laws is too vast for this article, we will focus on one particular aspect of *Loi Sapin II* – whistleblowing – and how it interacts with the new EU data protection regime in France. In a second part we will look at the creation of a new French authority established to ensure compliance with French anti-corruption requirements. Just how effective will it be?

Part I

I. Whistleblower requirements and data protection: a complicated cohabitation

A. Background on whistleblowing in France

Outsiders are sometimes perplexed by the reticence in Europe, and France in particular, to adopt legislation to implement whistleblower regimes. One explanation comes from the strong negative connotation of denouncing others, especially anonymously, since it can be associated with the darker side of deportations and assassinations, often due to "whistleblowers," that occurred during World War II under Nazi occupation. But times change and governments – in the face of corruption and terrorism – are more open now when it comes to encouraging others to *denoncer leur voisin* – for tax evasion, corruption, suspected terrorism…

Article 6 of the *Loi Sapin II* describes the whistleblower as a natural person – either internal to the company or a third party – who denounces crimes and illegal actions committed within a company. In order to benefit from the regime's protected status, the potential whistleblower must be "disinterested" and act in good faith. Some areas, however, are out of scope for whistleblowing: information related to attorney-client privilege, medical secrecy, or national defence classified information.

B. Whistleblower requirements under *Loi Sapin II*

A company employing at least 50 employees must implement a whistleblower policy. For companies with more than 500 employees, and whose turnover exceeds 100 million euros, a whistleblower policy must be implemented as part of their Code of Conduct. And the Codes of Conduct must be communicated broadly.

If a whistleblower alert is raised then in theory it must be handled by the whistleblower's manager or by a designated person within the company. If it is not, then it can be referred to the state authorities or judicial services. If no action is taken within three months, then the alert can be disclosed publicly but only if there is a serious and imminent threat or risk of "irreversible prejudice."

C. Special protected status of whistleblower

Someone who qualifies as a whistleblower is entitled to immunity when disclosing information qualified as "necessary and proportional" to safeguard interests at stake. The whistleblower cannot be dismissed or discriminated against (or denied a raise) when disclosing information on working conditions, for example.

Also, the Act of 2018 on trade secrets (Law n°2018-670 of 30 July 2018) provides that protections covering trade secrets cannot impede whistleblower disclosures provided the disclosure is intended to reveal, in good faith and in order to protect the public good, illegal activity, misconduct or reprehensible behaviour.

Attempts to obstruct a person from whistleblowing is a criminal offence and can result in up to a year imprisonment and a fine of 15,000 euros.

D. The anonymous whistleblower and the GDPR

The French data protection authority (*Commission nationale de l'informatique et des libertés*, or "CNIL") initially issued guidance on implementing whistleblower programs back in 2005. This guidance, known as AU-004, had many shortcomings, the most notable being its limited scope and insistence that whistleblower regimes should not be anonymous. In addition, such programs usually required prior authorisation since they could conceivably collect "sensitive data" relating to criminal offences.

In response to the *Loi Sapin II*, the CNIL modified its AU-004 guidance in 2017, now permitting anonymous reporting, broadening the scope and *in fine* aligning its recommendations more or less with the requirements under the new French law. The CNIL still encourages the whistleblower to provide his or her identity but holds that it must be kept secret (except for revealing it to judicial authorities). An anonymous alert can be transmitted to the judicial authorities only if it is considered founded[3].

More broadly, all GDPR requirements regarding processing, conservation and tracking of personal data are applicable to the whistleblowing policy. It is therefore a balancing act to ensure that whistleblowing programs are designed and work in compliance with the CNIL guidelines provided in AU-004. This is especially true for international companies that have competing requirements under US law in particular.

E. Challenges from abroad: the US CLOUD Act

The United States, for their part, adopted the Clarifying Lawful Overseas Use of Data ("CLOUD") Act on 23 March 2018. The CLOUD Act aims to clarify the rules on requisitions by US authorities for data stored outside their territory.

In brief, the CLOUD Act expressly provides that certain US law-enforcement orders may obtain data located in other countries. The Act also encourages foreign governments to enter into

new mutual legal assistance treaties regarding data communications. The Act imposes certain limits and restrictions on law enforcement requests to address privacy and civil liberty concerns. More precisely, the CLOUD Act, in §103(a), provides that a "provider of electronic communication service or remote computing service" must comply with a US law-enforcement order to disclose data within its "possession, custody, or control," even when that data is "located […] outside the United States."

On February 2019, the European Council published a recommendation authorising the EU to negotiate, in the name of the EU member states, a bilateral treaty with the US regarding the communication of data in the context of a judicial procedure.

The provisions of this Act would be triggered within the framework of a criminal investigation, corruption being considered as such. As we await ratification of a future bilateral treaty between the US and EU, this Act could potentially be a way to bypass the GDPR, *Loi Sapin II* and its anonymous whistleblowing system. US investigators could conceivable obtain information protected under EU law directly from the electronic communication service provider even if this data is located within the EU territory.

F. Whistleblowers in action

Before *Loi Sapin II* came into force, whistleblowers were able to come forward and raise alerts, albeit with legal uncertainty. For example, regarding the French part of the UBS tax evasion scheme case, on 5 March 2015 – when the *Loi Sapin II* was not yet drafted – a French labour court condemned UBS France for workplace harassment suffered by one of its former employees. The employee was responsible for organizing events for high net worth clients and was dismissed after she refused to destroy documents likely to reveal the existence of a criminal offence. Her workplace harassment claim gained traction since she was able back up her allegations with company documents, and she eventually became a key witness that unmasked criminal activity.

In the end, UBS was ordered to pay 30,000 euros in damages to its former employee who was dismissed in 2012. The Court, however, did not recognize the discrimination claim nor the offence of obstruction[4].

While it is too early to know how *Loi Sapin II* will be interpreted there are indications that the law is having some effect. In one recent case the criminal chamber of the *Cour de cassation* (French Supreme Court) remanded a case to the *Cour d'appel* so the lower court could factor in requirements under *Loi Sapin II*. In this case, an accused party of a criminal offence was able to benefit from the recent law that offered greater leniency [5].

G. Governance requirements under *Loi Sapin II*

Like the GDPR, the *Loi Sapin II* imposes internal compliance requirements such as training managers as well as employees who are at risk for exposure to corrupt practices. One particularity of the *Loi Sapin II* is that it applies to managing directors of *Sociétés Anonymes*

(SA) as well as *Sociétés par Actions Simplifiée* (SAS) and the President of a SAS but does not cover the *Président du conseil d'administration* of a SA[6].

Both *Loi Sapin II* and the *Loi Vigilance* also impose obligations for completing a risk mapping exercise. Article L 225-102-4 of the French Commercial Code created by the *Loi Vigilance* requires that companies having more 5,000 employees adopt a "vigilance plan" outlining measures to prevent infringements of human rights, health and security as well as the environment.

Loi Sapin II also places additional burdens on companies having more than 5,000 employees with a turnover of 100 Million euros: they must regularly complete a risk mapping exercise so the company can identify, analyse and hierarchise the risks faced by the company, weighing them against exposure to potential corrupt practices.

Part II

II- The question of oversight

A. The French Anticorruption Agency (AFA)

The *Loi Sapin II* created the AFA, which has national competence and is attached to the Justice and Budget Ministries. Its mission is to assist the competent authorities and others to prevent and detect acts of corruption. The agency is managed by an independent judge nominated by the French President but does not respond to any hierarchy.

The AFA provides recommendations to help legal entities comply with the *Loi Sapin II*. The AFA has oversight on government entities and, more importantly, all companies in scope of the *Loi Sapin II* and their compliance with the Act. The AFA works closely with the CNIL, the French competition authority as well as the special body under the Ministry of Finance to combat money laundering (*Tracfin*).

AFA's notoriety is increasingly being felt. In 2018, the AFA led 43 audits on 28 entities, 11 of them were subsidiaries of international groups, and 15 were public organizations[7]. Only 6 % of the French companies complied with the new requirements of *Loi Sapin II* on December 2018[8].

B. On the horizon: the company as a responsible social and environmental actor

Multinational companies appear to be generally at ease with *Loi Sapin II* (US companies, for example, had implemented such compliance measures in response to other laws long before the French law came into effect). The AFA's pedagogical approach is also well-received by companies who act in good faith and look to the authority for guidance on how to make their compliance programs as effective as possible.

In some ways the *Loi Sapin II* is being eclipsed by another recently adopted French law: *Loi PACTE* (action plan for business growth and transformation). While this law does not address compliance per se it does introduce a fundamental shift regarding the notion of the company in modern society. Article 61 states that, "The company is managed in its social interest, taking into consideration the social and environmental issues of its activity."

The "*raison d'être*" of a company is thus not just one of making money for shareholders but one of being a responsible social and environmental actor for all stakeholders. The new law is not without detractors who point out that the *Charte de l'environnement* adopted in 2011 by the *Conseil Constitutionnel* already requires companies take into account social and environmental issues.

These new compliance standards, as well as attempts to redefine the role of a company in modern society, equate to more effort, resources and diligence on the part of companies as they operate globally. French law may not only have caught up with anti-corruption regimes already in place in the US and UK but in some ways goes beyond. And even if the French legislator is still searching for the right balance between encouraging economic growth while ensuring compliance with anti-corruption and data protection, indications are that companies are readily adapting to this more stringent reality of doing business in Europe.

[1] La lutte contre la corruption en France, Daphné Latour et Pierre-Edouard Gondran de Robert, 2013 :
https://laurentcohentanugiavocats.com/wp-content/uploads/2018/07/LA-LUTTE-CONTRE-CORRUPTION-EN-FRANCE-DaphneLatour-002.pdf

[2] Ignominie ordinaire du délateur parisien, André Loez, Le Monde, 01 juin 2017 :
https://www.lemonde.fr/livres/article/2017/06/01/ignominie-ordinaire-du-delateur-parisien_5137006_3260.html

[3] Alertes professionnelles: modification de l'autorisation unique n°AU-004, 28 juillet 2017 :
https://www.cnil.fr/fr/alertes-professionnelles-modification-de-lautorisation-unique-ndegau-004

[4] La justice reconnaît le harcèlement moral pour une ex-salariée d'UBS France, lanceuse d'alerte, Le Monde, 5 mars 2015 :
https://www.lemonde.fr/europe/article/2015/03/05/la-justice-reconnait-le-harcelement-moral-pour-une-ex-salariee-d-ubs-france-lanceuse-d-alerte_4588138_3214.html

[5] Cour de cassation, chambre criminelle, 17 octobre 2018, N° de pourvoi: 17-80485 :
https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000037536230&fastReqId=1308050364&fastPos=2

[6] A quels dirigeants la lutte contre la corruption incombe-t-elle dans les SA et SAS ?, Editions Francis Lefebvre, La quotidienne, 7 février 2018 :
https://www.efl.fr/actualites/affaires/societes/details.html?ref=ui-1272f64e-5a22-4f5d-8d9f-f0fd734212ca

[7] Anticorruption : quel bilan, deux ans après la loi Sapin II ?, 21/01/2019, Droit des affaires, Editions législatives. Seen on : https://www.editions-legislatives.fr/actualite/anticorruption-quel-bilan-deux-ans-apres-la-loi-sapin-ii

[8] Sapin II : des entreprises très loin de la conformité, Cécile Desjardins, 26/12/2018. Seen on : https://business.lesechos.fr/directions-financieres/comptabilite-et-gestion/gestion-des-risques/0600339265907-sapin-ii-des-entreprises-tres-loin-de-la-conformite-325934.php