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 10, Number 5 May 2010

French Court Of Appeals Ruling Upholding Competition Authority's Search And Seizure Of Company Employees' Emails

By Olivier Proust, of Hunton & Williams, Brussels.

Introduction

On February 19, 2010, the Court of Appeals of Versailles (the "Court") upheld the unlimited search and seizure of a company's emails by several agents ("Competition Authority agents") of the French Competition Authority ("Autorité de la Concurrence").[1] These agents had been authorized by a French "freedoms and custody judge"[2] to inspect the emails of several employees for the purposes of an investigation into an alleged abuse of a dominant position in the pharmaceutical market.

Under French law, Competition Authority agents may conduct on-site investigations on a company's premises if the company is suspected of anti-competitive practices (*e.g.,* being involved in a cartel or abusing its dominant position).[3] During their investigation, they may access and obtain copies of any books, invoices and other company documents, and any information that is relevant to their investigation, and may seize any documents or information support to this end.[4]

In the Janssen-Cilag case, the company under investigation and several of its employees challenged the validity of the search, on the grounds that the Competition Authority had seized all employee emails without selecting those relevant to the investigation, and that private documents belonging to employees and third parties were included in the search, in alleged violation of those individuals' privacy rights, of the right to the secrecy of correspondence and of the right to the protection of personal data. The Court ruled that the seizure of certain personal documents belonging to employees or documents that may be irrelevant to the investigation does not invalidate the entire search (which was pre-approved by a judge). The Competition Authority is required, however, to return the copies of these documents to their owners. The Court also ruled that, in this context, seizing computer files does not constitute a data processing activity and, therefore, the French Data Protection Act[5] does not apply.

The Janssen-Cilag case illustrates how the investigative powers of the Competition Authority may conflict with employees' right to privacy, and shows that there is a possible conflict of laws between data protection and competition law. In particular, this case raises the question as to whether the French Data Protection Act ap-

plies to the Competition Authority and whether a public investigation should be conducted within the limits and boundaries of data protection law.

1. Application of the French Data Protection Act to Public Investigations

1.1 The French Data Protection Act Applies to Public Authorities

When enacted in 1978, the purpose of the French Data Protection Act was to create an independent administrative authority (*i.e.*, the CNIL)[6] that would counterbalance certain activities of the State that were perceived as dangerous.[7] Since then, the Act has been amended,[8] but continues to regulate all data processing activities, both private and public. Indeed, the scope of the Act is broadly defined, so that it applies "to automatic processing of personal data as well as non-automatic processing of personal data that is or may be contained in a personal data filing system".[9]

Public authorities are clearly identified in the French Data Protection Act as a type of data controller.[10] Although there is no legal definition of a "public authority" under French law, this concept is commonly understood to mean governmental and administrative bodies, such as ministries, law enforcement authorities, judicial and administrative authorities, and local or regional councils. Independent administrative authorities, such as the Competition Authority,[11] may also qualify as public authorities, even though there is no clear definition of an "independent administrative authority" under French law.[12] The better view is, therefore, that the Competition Authority is a data controller, insofar as a public investigation is considered to be a data processing activity carried out in France.[13]

1.2 A Public Investigation May Constitute a Data Processing Activity

The Janssen-Cilag case raises the question as to whether a public investigation conducted by the Competition Authority constitutes a data processing activity. The plaintiffs in this case claimed that the Competition Authority agents had conducted their investigation in violation of the French Data Protection Act. The Court, however, ruled against the application of the French Data Protection Act in this case, on the grounds that the search and seizure of computer files by the Competition Authority did not constitute a data processing activity.[14] If this ruling were to be examined by the Court of Cassation, it is not clear that it would be confirmed, because it appears to ignore the legal definitions of "personal data" and "data processing".

The concepts of "personal data" and "data processing" are clearly defined in the French Data Protection Act. "Personal data" is defined as "any information relating to a natural person who is identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him".[15] Whether or not an individual is "identified or identifiable" from the information available usually depends on a number of factors, such as the physical, psychological, mental, economic, cultural or social identity of the individual.[16] Some of the information contained in electronic documents, such as emails, is likely to qualify as personal data (*i.e.*, name, email address, and contact details of the sender and the recipient).[17]

The act of "processing" personal data is defined broadly as "any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction".[18] During their investigation, the Competition Authority agents accessed, retrieved and prepared an inventory of computers files, which were then burned onto a DVD for further analysis. Therefore, under data protection law, these operations are considered to be automatic data processing activities.

Furthermore, the EU Article 29 Working Party ("Working Party")[19] considers that any collection, use or storage of information about employees by electronic means will most likely fall within the scope of data protection legislation and that the monitoring of emails necessarily involves the processing of personal data.[20] In the private sector, employee monitoring activities (*e.g.*, monitoring of internet activities, whistleblowing procedures, or corporate investigations) are recognized by privacy practitioners[21] and data protection authorities[22] as data processing activities, which strongly suggests that public investigations may also fall within the scope of the French Data Protection Act.

2. Legitimacy of Processing for the Purpose of a Public Investigation

The protection of personal data is based on several principles aimed at protecting the fundamental rights and freedoms of individuals.[23] Assuming that a public investigation constitutes a data processing activity, this would mean that the Competition Authority agents must conduct their investigations in compliance with the data protection rules and principles.

2.1 Legitimate Basis for Conducting an Investigation

One of the fundamental principles for the processing of personal data is ensuring that it is carried out fairly and lawfully.[24] Personal data must be obtained for "specified, explicit and legitimate purposes".[25] In the context of a public investigation, there are only three relevant grounds on which personal data may be processed, namely 1) consent of the data subject, 2) compliance with a legal obligation to which the data controller is subject, and 3) the pursuit of a legitimate interest by the data controller.[26]

Consent

Article 2(h) of Directive 95/46/EC defines consent as "any freely given specific and informed indication of the wishes by which the data subject signifies his agreement to personal data relating to him being processed". In or-

   ISSN 1473-3579

der to be valid, consent must meet several requirements,[27] which are unlikely to be met in the context of a public investigation. Indeed, in some circumstances, consent is viewed as an inadequate legal basis for processing personal data. In particular, the Working Party considers that consent is not a valid legal basis in the employment context because employees must have an opportunity to withdraw their consent without being exposed to any penalty. Employees also have the right to withdraw their consent at any time if they change their mind,[28] which could potentially disrupt an ongoing investigation. It is also unlikely that the Competition Authority is able to obtain prior consent from third parties to whom personal data may relate (*e.g.*, recipients of emails, contractors, customers, business partners, *etc.*), thus limiting the lawfulness of the investigation. In some situations, however, the Working Party recognizes that consent may exceptionally be relied upon where the individual is able to give free, informed and specific consent.[29]

Necessary Compliance with a Legal Obligation

Compliance with a legal obligation is interpreted by the Working Party as a national legal statute or regulation.[30] In the context of a public investigation, the Competition Authority could argue that the collection and processing of personal data are necessary to enforce the competition rules in France and that its agents carry out on-site inspections to establish evidence of unlawful practices, in accordance with the provisions of the French Commercial Code.[31]

Necessary for the Pursuit of a Legitimate Interest by the Data Controller

An investigation carried out by the Competition Authority may also be found to be necessary for the purposes of maintaining free competition on the market. Therefore, the pursuit of a legitimate interest may be a valid legal basis to the extent that it does not override the interests and fundamental rights and liberties of the data subject.[32] In other words, the processing of personal data in the context of a public investigation must be balanced against the fundamental rights of the individuals, particularly the right to privacy (see Section 3 below). This balance of interests is particularly important with regard to third parties that may be involved in, but not directly concerned by, the scope of the investigation (*e.g.*, contractors, service providers, business partners, family members, *etc.*).

Sensitive Personal Data and Other Special Categories

Employee emails and computer files may also contain pieces of information deemed to be sensitive. Under the French Data Protection Act, additional restrictions apply to the processing of any personal data that identifies an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, sexual orientation, or is health-related. As a general rule, the processing of sensitive data is not permitted, except under certain limited circumstances, such as processing for which the data subject has given his express consent or processing that is necessary for the establishment, exercise or defence of a legal claim.[33] The latter condition could potentially apply to data collected by Competition Authority agents if it is used as evidence in a trial brought against the company undergoing the investigation. According to data protection law, the Competition Authority may have to demonstrate that the collection of sensitive data is necessary and relevant for the investigation.[34]

The processing of personal data relating to offences, convictions and security measures is also subject to legal restrictions, although public authorities are expressly authorized to process such data within the scope of their powers.[35]

2.2 Proportionality

In the Janssen-Cilag case, the plaintiffs argued that the competition agents had used unnecessary and disproportionate means to gather evidence, including global and massive seizures, which disrupted the normal functioning of the company. The plaintiffs claimed that the Competition Authority agents should have selected the messages that were relevant to their investigation instead of seizing entire inboxes. The Court cancelled the seizure of three computer files,[36] but validated the investigation on the grounds that there was no evidence that these agents had not selected in advance the documents seized, nor that the seizure was disproportionate. The Court also validated the investigation on the grounds that the Competition Authority agents had used the only method enabling them to preserve the accuracy and reliability of the relevant documents.[37]

Proportionality is one of the key principles under data protection law.[38] It requires any data controller processing personal data to maintain a balance between the purpose of the processing and the fundamental rights of the individuals concerned. Essentially, this means that a data controller may only collect personal data that is adequate, relevant and not excessive to achieve the purpose of data collection,[39] and necessary to achieve this purpose.[40] This may be viewed by investigators or agents, whose role is to search for and obtain evidence, as an obstacle to their investigation.

Recently, the Working Party issued guidelines on data processing in the context of pre-trial discovery procedures,[41] which could apply in the context of a public investigation. In particular, the Working Party states that "there is a duty upon data controllers . . . to take such steps as are appropriate . . . to limit the discovery of personal data to that which is objectively relevant to issues being litigated."[42] The CNIL also states, regarding e-discovery procedures, that "it is fundamental to verify the proportionality and quality of the data collected and disclosed, and this must be carried out objectively so as to guarantee that only legally authorized elements are disclosed".[43]

Consequently, the Competition Authority agents may need to implement specific measures to comply with the proportionality principle. Some of the measures recommended by the Working Party are already put in place by the Competition Authority. For example, the Competition Authority agents must determine in advance the

scope of their investigation and identify the information relevant to their investigation. When conducting an investigation, the agents must filter the data collected, for example, by using key words in their searches.[44] They may also identify in advance the individuals targeted by an investigation so as to limit the search to a specific period of time during which the facts have supposedly taken place.[45] Finally, when the identity of the individuals is not relevant to an investigation, it is recommended to anonymize or pseudonymize the data collected.[46]

2.3 Transparency

Transparency is another major principle of data protection law[47] and labor law,[48] because it requires data controllers to inform the data subjects prior to any processing of personal data relating to them. This may be viewed by investigators as counterproductive, since what they are trying to achieve is to preserve the secrecy of an investigation in order to avoid any destruction of evidence. As a general rule, the transparency principle requires data controllers to provide advance general notice of the possibility of personal data being processed[49] and a specific notice when the personal data is actually being processed.[50] The Working Party admits an exception to this rule when there is a substantial risk that such notification would jeopardize the ability to conduct an investigation properly or to gather the necessary evidence.[51] For example, in the context of internal whistleblowing schemes, the Working Party admits that the notification to individuals may be delayed in order to preserve evidence by preventing its destruction or alteration.[52]

The transparency principle also requires data controllers to notify the data protection authority (*i.e.*, CNIL) about their data processing activities. In some situations, which may apply to public investigations, a data controller must obtain the prior authorization of the CNIL, for example, for the processing of data relating to offences, convictions or security measures.[53] In addition, the processing of personal data carried out on behalf of the State and whose purpose is to prevent, investigate or obtain evidence of criminal offences, prosecute offenders or execute criminal sentences or security measures must be authorized by an order issued by the competent Minister or Ministers, after the release of an opinion by the CNIL.[54]

2.4 Data Security

The data security principle requires data controllers "to take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorized third parties".[55] In practice, this means that the Competition Authority agents must implement appropriate technical and organizational measures during and after their investigation to preserve the security and confidentiality of any personal data processed. This also requires the Competition Authority to train its agents and to use software that protects evidence from alteration or destruction.

3. The Exercise by Employees of Their Privacy Rights in the Context of a Public Investigation

Under privacy and data protection law, individuals are granted fundamental rights that may conflict with the confidential nature of an investigation.

3.1 The Right to Privacy

In France, the Civil Code states that "everyone has the right to respect for his private life".[56] Although the right to privacy is not stated *per se* in the French Constitution, the French Constitutional Court has ruled on several occasions that privacy is a constitutional right.[57] The plaintiffs in the Janssen-Cilag case argued that the Competition Authority agents had seized entire inboxes without selecting the emails that were relevant to their investigation. As a consequence, private emails belonging to employees and third parties may have been seized, which constitutes a violation of those individuals' right to privacy. The Court rejected this argument on the grounds that the seizure of personal documents belonging to employees, or documents irrelevant to the investigation, does not invalidate the investigation, since the latter had been authorized by a judge. Additionally, the Court found that if only a fraction of the emails seized pertains to the investigation, this justifies the global seizure of emails.

The Court's ruling raises the question as to whether employees have a right to privacy in the context of a public investigation. In the employment context, the Court of Cassation ruled in a landmark decision that "an employee has the right to the respect of his private life, including on the work premises and during working hours."[58] Since then, the Court of Cassation has refined its position and considers that emails and documents stored on a computer owned by the company are presumed to be professional by nature, unless they are identified as being "personal".[59] An employer who might investigate the activities of an employee suspected, for example, of being involved in anti-competitive behaviour cannot search that employee's emails and computer files marked "personal" in his absence, unless there is a particular threat or risk for the company.[60] It is not clear how these conditions apply in the context of a public investigation. The ruling in the Janssen-Cilag case seems to imply that the employees' right to privacy at the workplace is limited due to the overriding powers of the Competition Authority agents conducting the investigation.

3.2 The Right to the Secrecy of Correspondence

The right to the secrecy of correspondence results from employees' right to privacy.[61] In an employment context, electronic messages (*i.e.*, emails) are presumed to be professional by nature, unless they are marked "personal", in which case they are considered to be private correspondence.[62] The violation of the secrecy of correspondence is also viewed as a felony under the French Criminal Code,[63] including when public servants are acting while on duty.[64]

   ISSN 1473-3579

In the Janssen-Cilag case, the plaintiffs argued that the seizure of private emails violated their right to the secrecy of correspondence. According to the Court, however, the law authorizes competition agents to seize all correspondence, including those that are private, as long as they are relevant to their investigation. This raises the question whether the Competition Authority is authorized to search and seize private emails if there is a reason to believe that they may be used to conceal anti-competitive practices. Based on the rules of data protection, the Competition Authority agents would generally be required to single out correspondence that is relevant to their investigation and to avoid any disproportionate search of emails. According to the Janssen-Cilag ruling, however, the powers of the Competition Authority agents authorize them to override the rights of employees if the investigation so requires.

3.3 The Right to Access and to Rectify Personal Data

The Data Protection Act grants individuals the right to obtain confirmation as to whether personal data relating to them is processed and to obtain communication, in an accessible form, of the personal data relating to them.[65] This right is not absolute and may be restricted, for example, if it is necessary to safeguard the monitoring, inspection or regulatory function connected with the exercise of official authority in cases such as the prevention, investigation, detection and prosecution of criminal offences.[66] According to the CNIL, the data controller may, in certain circumstances, either postpone an individual's access to his data,[67] or ask a judge to prohibit the disclosure or destruction of personal data if it is necessary to preserve the confidential nature of an investigation.[68] There is, however, no general waiver of the rights to access or amend personal data.[69]

Access to personal data entitles individuals to rectify, complete, update, block, or delete personal data relating to them insofar as it is inaccurate, incomplete, equivocal, expired, or if its collection, usage, disclosure or storage is prohibited.[70] This right must not, however, affect or alter information that may be used as evidence in court.[71] It therefore seems that the right to rectify personal data is limited to specific situations where an individual may be involved in an investigation by mistake or where information about an individual was erroneously recorded.[72]

3.4 The Right to Object to the Processing of Personal Data

Individuals are also entitled to object, on legitimate grounds, to the processing of any data relating to them. This right, however, does not apply when the processing satisfies a legal obligation or when it is explicitly excluded by a decision authorizing the processing (*e.g.*, an authorization by the CNIL or a court order).[73] Consequently, it seems unlikely that employees involved in a public investigation may object to the seizure of their emails if a judge or public authority has authorized the investigation.

Conclusion

The Janssen-Cilag case reveals tensions between privacy law and competition law. Although the Competition Authority has strong investigative powers, it seems hard to justify that these powers cannot be balanced with the fundamental rights that are granted to citizens of the European Union. A balance, therefore, should be struck between the investigative powers of the Competition Authority and the data protection principles (legitimacy, proportionality, transparency, *etc.*), which may be achieved, for example, by incorporating these principles into the procedural rules applicable to public investigations.

In conclusion, the Janssen-Cilag case raises many questions that often do not have clear-cut answers, but in the end the outcome of this case will depend on how the Court of Cassation interprets the law.[74]

NOTES

[1] Cour d'appel de Versailles, 19 février 2010, Janssen-Cilag/Autorité de la concurrence et autres, available at: http://www.legalis.net.

[2] This judge belongs to the first instance court or "tribunal de grande instance".

[3] Article L.450-4, Commercial Code.

[4] Articles L.450-3 and L.450-4, Commercial Code.

[5] Act n°78-17 of January 6, 1978, on Data Processing, Data Files and Individual Liberties ("French Data Protection Act").

[6] Commission Nationale de l'Informatique et des Libertés (CNIL).

[7] The Data Protection Act was enacted in France with a view to block a project of the Government named SAFARI whose purpose was to interconnect all the public files (*i.e.*, intelligence, national security, law enforcement, *etc.*), enabling public authorities to merge all an individual's personal data by using his social security number. This project was viewed as an intrusion of the State and caused the National Assembly to adopt the Data Protection Act. For more information, see Report n°218 of March 19, 2003, by M. Alex Türk, prepared on behalf of the Senate's Commission of Laws, available at: http://www.senat.fr/rap/l02-218/l02-218.html.

[8] The Data Protection Act of 1978 was amended by the Act No. 2004-801 of August 6, 2004, relating to the protection of individuals with regard to the processing of personal data, which implements Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing if personal data and on the free movement of such data ("Directive 95/46/EC") into national law.

[9] Article 2, French Data Protection Act.

[10] Article 3 of the French Data Protection Act states: "The data controller means, unless expressly designated by legislative or regulatory provisions relating to this processing, a person, public authority, department or any organization who determines the purposes and means of the data processing".

[11] Article L.461-1 of the French Commercial Code defines the Competition Authority as an "independent administrative authority".

[12] According to the State Council ("Conseil d'Etat"), independent administrative authorities have in common that they act on behalf of the State without being under the authority of the Government and they benefit from guarantees that enable them to act autonomously in order to carry out their mission, without any influence or censorship, except from a judge. See "Conseil d'Etat, Rapport public 2001, Les autorités administratives indépendantes", available at: http://www.conseil-etat.fr/cde/node.php?articleid=432.

[13] Pursuant to Article 5, the French Data Protection Act applies to the processing of personal data "if the data controller is established on French territory". The data controller who carries out his activity on French territory within an establishment, whatever its legal form, is considered to be established on French territory. According to Recital 19 of Directive 95/46/EC, an "establishment on the territory of a

Member State implies the effective and real exercise of activity through stable arrangements".

[14] The Court justifies this position on the grounds that the seizure was authorized by a judge on the basis of Article L.540-4 of the French Commercial Code, which defines the investigation powers of the Competition Authority agents.

[15] Article 2, French Data Protection Act.

[16] Article 2(a), Directive 95/46/EC.

[17] See Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, adopted on September 13, 2001, available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2001_en.htm.

[18] Article 2, French Data Protection Act.

[19] The Working Party was established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. Its tasks are laid down in Article 30 of Directive 95/46/EC and in Article 15 of Directive 2002/58/EC.

[20] See above, note 17.

[21] See, for example, Dan Cooper, "Corporate Investigations and EU data privacy laws: what every in-house counsel should know", World Data Protection Report, December 2008; Christiane Féral Schuhl, "Cyberdroit - Le Droit à l'épreuve de l'Internet", 5th edition, 2008, p. 193.

[22] See CNIL "La cybersurveillance sur les lieux de travail", report presented by M. Hubert Bouchet, December 18, 2004, available at: http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/91/le-controle-de-lutilisation-dinternet-et-de-la-messagerie/; Garante per la protezione dei dati personali, "Guiding Principles Applying to the Processing of Employees' Personal Data for the Purpose of Managing Employment Relations in the Private Sector", December 2006; Datainspektionens, "Personal data processing for the purpose of monitoring employees", June 2003, both available at: http://ec.europa.eu/justice_home/fsj/privacy/policy_papers/policy_papers_topic_en.htm#employment.

[23] See Recital 10 of Directive 95/46/EC: "Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human rights and Fundamental Freedoms and in the general principles of Community law."

[24] Article 6, French Data Protection Act.

[25] Article 6, French Data Protection Act.

[26] Article 7, French Data Protection Act.

[27] In order for the individual's consent to be valid, it must be 1) clear and unambiguous (*i.e.*, there must be no doubt as to whether the individual consented to the processing of his or her personal data); 2) freely given (*i.e.*, the individual concerned must not be pressured or threatened to give his or her consent); 3) specific (*i.e.*, the consent must relate to a specific data processing activity); and 4) informed (*i.e.*, the individual concerned must be informed about the data processing activity, *prior* to giving consent).

[28] See above, note 17, p. 23.

[29] See Article 29 Data Protection Working Party, Working Document 1/2009 on pre-trial discovery for cross border civil litigation, adopted on February 11, 2009, available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm; see also CNIL, "Délibération n°2009-474 du 23 juillet 2009 portant recommandation en matière de transfert de données à caractère personnel dans le cadre de procédures judiciaires américaines dite de Discovery", August 21, 2009, available at: http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/209/.

[30] See Article 29 Data Protection Working Party, Working Document 1/2009 on pre-trial discovery for cross border civil litigation, adopted on February 11, 2009, available at: http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/209/.

[31] In particular, Article L.450-1 of the French Commercial Code refers to Sections II and III of the Commercial Code regarding anti-competitive practices and abuse of dominant positions.

[32] Article 7-5°, French Data Protection Act.

[33] Article 8, French Data Protection Act.

[34] Article 6-4°, French Data Protection Act.

[35] Article 9 of the French Data Protection Act states: "Processing of personal data relating to offences, convictions and security measures may be put in place only by the courts, public authorities and legal entities that manage public services, within the framework of their legal remit . . .".

[36] The Court ruled that these files were not explicit enough to justify why they were relevant to the investigation.

[37] The Court ruled that the disputed emails coming from the Microsoft Outlook 2003 software were stored in a unique folder for all the services provided to the user (mail, calendar, contacts . . .). The selection by message suggested by the company Janssen-Cilag would have the effect of altering the electronic index of the displaced files and would affect both the reliability and integrity of the concerned files. Furthermore, it is not contested that it is technically impossible to extract parts of calendars and contacts; consequently, it is in this sense that the email system is indivisible by nature.

[38] See Christopher Kuner, Proportionality in European Data Protection Law and Its Importance for Data Processing by Companies, BNA's Privacy & Security Law Report, Vol. 7, No. 44, 11/10/2008, p. 1615.

[39] Article 6-3°, French Data Protection Act.

[40] The proportionality principle also appears in the French Labor Code. In particular, Article L.1121-1 states: "One may not restrict the rights nor the individual and collective freedoms of an individual if it is not justified by the nature of the assignment to be carried out or is disproportionate to the intended purpose."

[41] See above, note 30; see also Olivier Proust & Cédric Burton, "Le conflit de droits entre les règles américaines de e-discovery et le droit européen de la protection des données à caractère personnel . . . entre le marteau et l'enclume", Revue Lamy Droit de L'Immatériel, February 2009 ; Olivier Proust & Cédric Burton, "Les autorités européennes prennent position sur le conflit de droits entre les règles de e-discovery et la protection des données à caractère personnel", Revue Lamy Droit de L'Immatériel, March 2009.

[42] See above, note 30.

[43] See CNIL, "Délibération n°2009-474 du 23 juillet 2009 portant recommandation en matière de transfert de données à caractère personnel dans le cadre de procédures judiciaires américaines dite de Discovery", August 21, 2009, available at: http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/209/. See also, Olivier Proust, "E-discovery: French Data Protection Authority Issues New Guidelines", The Privacy Advisor, IAPP, Volume 9, Number 10, November 2009.

[44] It is interesting to note that, in the Janssen-Cilag case, the Competition Authority agents used a forensic software named Encase, which is also used by law enforcement agencies for the purpose of electronic discovery. They also conducted their search using keywords; however, the Court ruled that, in the course of their investigation, the Competition Authority agents are not obliged to reveal to the company under investigation what keywords or search engines are used to identify the documents seized.

[45] See Dan Cooper, "Corporate Investigations and EU data privacy laws: what every in-house counsel should know", World Data Protection Report, December 2008.

[46] See above, note 29.

[47] Article 32, French Data Protection Act.

[48] Pursuant to Article L.1222-4 of the French Labor Code, "no personal information about an employee may be collected with a device that has not been brought previously to his attention".

[49] One can also discuss whether the Works Council should be consulted in this context. According to Article L.2323-32 of the French Labor Code, "the Works Council must be informed and consulted prior to any decisions regarding the implementation within the company of any means or techniques enabling to control the activity of the employees".

[50] See above, note 29.

[51] See above, note 30, p. 12.

[52] See Article 29 Data Protection Working Party, 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, available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm; see also CNIL, "Délibération n°2005-305 du 8 décembre 2005 portant autorisation unique de trait-

   ISSN 1473-3579

ements automatisés de données à caractère personnel mis en oeuvre dans le cadre de dispositifs d'alerte professionnelle", available at: http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/83/.

[53] Article 25, French Data Protection Act.

[54] Article 26, French Data Protection Act.

[55] Article 34, French Data Protection Act.

[56] Article 9, French Civil Code.

[57] See Olivier Proust, "French Constitutional Court Rules on the Balance Between Privacy and Public Safety", March 16, 2010, Privacy & Information Security Law Blog, available at: http://www.huntonprivacyblog.com/2010/03/articles/european-union-1/french-constitutional-court-rules-on-the-balance-between-privacy-and-public-safety/.

[58] Cour de cassation, chambre sociale, 2 octobre 2001, Nikon France/M. Frédéric Onof, pourvoi n°99-42942; Cour de cassation, chambre sociale, 12 October 2004, Mme X./société Sulzer orthopédie Cedior, pourvoi N°02-40392.

[59] Cour de cassation, chambre sociale, 18 October 2006, M. X./société Jalma emploi et protection sociale, pourvoi n°04-47400; Cour de cassation, chambre sociale, 18 October 2006, M. X./société Techni-Soft, pourvoi n°04-48025; Cour de cassation, chambre sociale, 21 October 2009, Jean Michel X./Seit Hydr'Eau, pourvoi n°07-43877; see also "French High Court Rules Computer Folder Identified Only With Worker Initials Isn't Personal", BNA's Privacy & Security Law Report, Vol. 8, No. 47, 12/7/2009, p. 1726.

[60] Cour de cassation, chambre sociale, 17 mai 2005, M. Philippe X/société Cathnet-Science, pourvoi n°03-40017; Cour de cassation, chambre sociale, M. X/The Phone House, 30 May 2007, pourvoi n°05-43102; Cour de cassation, chambre sociale, 15 December 2009, Bruno B./Giraud et Migot, pourvoi n° 07-44264; Cour de cassation, chambre sociale, 8 December 2009, M. X./Fédération nationale des groupements de défense sanitaire du bétail (FNGDSB), pourvoi n°08-44840.

[61] Cour de cassation, chambre sociale, 2 octobre 2001, Nikon France/M. Frédéric Onof, pourvoi n°99-42942; Cour de cassation, chambre sociale, 12 October 2004, Mme X./société Sulzer orthopédie Cedior, pourvoi N°02-40392.

[62] Cour de cassation, chambre sociale, M. X/The Phone House, 30 May 2007, pourvoi n°05-43102; Cour de cassation, chambre sociale, 6 June 2007, société Eliophot/M. X., pourvoi n°05.43996; TGI de paris, 12ème chambre, jugement du 1er juin 2007, Oddo et Cie/Trinh Nghia T. et Trung T., available at: http://www.legalis.net/jurisprudence-decision.php3?id_article=2179#.

[63] Pursuant to Article 226-15 of the French Criminal Code, "the act of maliciously opening, destroying, delaying or diverting a correspondence sent to a third party, whether or not it arrives at its destination, or fraudulently gaining knowledge of it, is punishable by one year's imprisonment and a fine of €45,000".

[64] Pursuant to Article 432-9 of the French Criminal Code, "the fact for a person holding public authority, who is acting in the course of or on the occasion of his office or duty, to order, commit or facilitate the misappropriation, deletion or opening of correspondence, and to disclose the contents of such correspondence, except where provided for by law, is punishable by three years' imprisonment and a fine of €45,000".

[65] Article 39, French Data Protection Act.

[66] Article 13, Directive 95/46/EC.

[67] CNIL, FAQ on whistleblowing procedures, available at: http://www.cnil.fr/nc/dossiers/travail/que-dit-la-cnil-sur/faq-sur-les-dispositifs-dalerte-professionnelle/.

[68] See above, note 43.

[69] See above, note 30.

[70] Article 40, French Data Protection Act.

[71] See above, note 30.

[72] See above, note 67.

[73] Article 38, French Data Protection Act.

[74] The Janssen-Cilag company filed a lawsuit before the Court of Cassation on February 22, 2010.

Olivier Proust is an Associate with Hunton & Williams, Brussels, in the firm's Global Technology, Outsourcing, and Privacy Group. He is also a member of the Paris Bar. He may be contacted at oproust@hunton.com.