Revue Le Lamy Droit des Affaires, Nº 87, 1er novembre 2013

L'entreprise et la protection des données personnelles

Les entreprises sont à la fois victimes potentielles de cyber-attaques et responsables des traitements de données personnelles engendrés par leurs activités. Cette situation particulière leur impose de mettre en œuvre une politique de gestion des risques tant internes qu'externes en matière de données personnelles, conciliant l'exigence sécuritaire aux intérêts légitimes de l'entreprise et aux droits fondamentaux de protection des données personnelles et de respect de la vie privée, à la faveur d'une nouvelle culture d'entreprise intégrant l'impératif de protection des données et sensibilisant tous les acteurs de l'entreprise aux rôles et responsabilités de chacun.

Emilie BAILLY

Avocat Cabinet Vigo

Clarisse LE CORRE

Avocat Cabinet Vigo

Les traitements de données à caractère personnel sont omniprésents pour les opérateurs économiques, *via* des réseaux internes et externes (*cloud computing*, big data, réseaux d'entreprise/intranet, bases de données, internet, etc.), et ce pour des finalités tant diverses qu'essentielles à l'entreprise (recrutement, géolocalisation, vidéosurveillance, contrôle de l'accès physique aux locaux, contrôle des horaires, messagerie électronique, transactions économiques et financières, transferts de données à l'étranger, etc.). Ces traitements visent tous les interlocuteurs de l'entreprise, internes comme externes à celle-ci – salariés, clients, consommateurs, prospects, concurrents, partenaires et autres tiers –.

Les entreprises sont, par conséquent, soumises aux dispositions de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, loi dite « *Informatique et Libertés* », et doivent composer avec l'impératif de protection des données personnelles.

Or, selon une enquête de l'IFOP pour MAKAZI GROUP, spécialiste du data marketing, seuls 14 % des 300 chefs d'entreprise interrogés estiment être parfaitement au fait de la législation en vigueur dans ce domaine. Si 47 % pensent la connaître « *assez bien* », près de deux sur cinq reconnaissent qu'ils la connaissent mal, voire très mal (<http://www.01net.com/editorial/603686/donnees-personnelles-39pour-cent-des-dirigeants-francais-connaissent-mal-la-legislation/> [dernière consultation : 10 oct. 2013]), méconnaissance de la règlementation qui est susceptible d'engager la responsabilité administrative, civile et pénale des personnes morales, en dépit de leur bonne foi.

La conformité à la règlementation applicable est d'autant plus difficile, notamment pour les TPE/PME, que les régimes de protection européens des données personnelles sont particulièrement évolutifs et fragmentés, ce qui place les opérateurs économiques dans une situation d'insécurité juridique préoccupante (Proposition de règlement du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union, 7 févr. 2013, COM(2013) 48 final, 2013/0027 (COD), disponible à : <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf> [dernière consultation : 10 nov. 2013], p. 2).

Seuls 14 % des 300 chefs d'entreprise interrogés estiment être parfaitement au fait de la législation en vigueur dans ce domaine.

Au-delà du risque interne qui résulte de la non-conformité à la loi « *Informatique et Libertés* », l'entreprise doit se prémunir contre le risque externe d'éventuelles intrusions frauduleuses dans ses systèmes informatiques susceptibles de provoquer la perte, le détournement ou encore l'altération des traitements de données à caractère personnel. Car si l'usage des nouvelles technologies constitue un outil pour l'accroissement de la compétitivité de l'entreprise, il la rend également plus vulnérable, « *ce qui l'oblige à repenser sa politique de sécurité pour parer notamment à des attaques venues de l'extérieur ou à la fuite d'information* » (Achilleas P., J.-CL. Libertés, Fasc. 820 : Internet et libertés, § 83).

Plus de six entreprises françaises sur dix ont subi au moins un accident de sécurité en 2011. Elles n'étaient qu'une sur trois en 2010. De fait, seuls 55 % des entreprises ont confiance en leur sécurité (« Global State of Information, Security Survey 2013, Tendances et enjeux de la sécurité de l'information », Étude réalisée par le cabinet PwC, publiée le 30 janv. 2013). Les attaques malveillantes et criminelles constituent la première cause de la violation des

données en France (42 % des cas). 31 % des violations de données résultent de négligences humaines (erreurs qui incluent notamment un mauvais traitement des données par les employés, un défaut de contrôle, le non-respect de la règlementation), 27 % résultant quant à elles d'erreurs système. En moyenne, 22 242 données sont compromises par incident (« Cost of Data Breach : France », Étude réalisée par Ponemon Institute, sponsorisée par Symantec, publiée le 5 juin 2013).

56 % des entreprises françaises victimes de fraude indiquent qu'elles ont été commises par un fraudeur interne.

Les conséquences de ces failles de sécurité sont lourdes pour les entreprises. Des conséquences commerciales, d'une part. La France est le pays où les conséquences commerciales des violations de données sont les plus lourdes, avec un taux d'attrition des clients de 4,4 %, et un coût relevant des pertes d'activité ou de contrats (perte de clients, difficulté à acquérir des nouveaux clients, dégradation de l'image) établi à 1,19 millions d'euros en 2012. Des conséquences financières, d'autre part, puisque le coût lié aux violations de données a augmenté de 11 % en France pour s'établir à 2,86 millions d'euros, contre 2,55 millions d'euros en 2011. Le coût moyen par donnée compromise s'élève à 127 euros en 2012, contre 122 euros en 2011, soit une augmentation de 4,1 % (« Cost of Data Breach : France », préc.).

L'enjeu de la mise en œuvre d'une politique de sécurité efficiente par les opérateurs économiques est d'autant plus conséquent que les données personnelles collectées et traitées par ceux-ci ont une valeur patrimoniale qui attise les convoitises. Le *Financial Times* a d'ailleurs récemment mis en ligne un simulateur permettant d'évaluer le prix de nos données personnelles (<http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html#axzz2h9t2kGZ5> [dernière consultation : 17 oct. 2013]).

Les données à caractère personnel peuvent constituer une part non négligeable du patrimoine d'une entreprise. Il existe dès lors un véritable « *marché* » des données personnelles, lesquelles se monnaient entre les différents acteurs de la vie économique – la FNAC a acquis récemment, dans le cadre de la liquidation de VIRGIN, le fichier-clients du distributeur culturel comportant près de 1,6 millions de noms, pour la somme de 54 000 euros. Corollaire de cette valorisation économique des données personnelles, il s'est créé un « *marché noir* » des données personnelles obtenues grâce à des activités illicites sur les réseaux informatiques, notamment des intrusions frauduleuses dans les systèmes informatiques d'entreprises insuffisamment protégées.

L'entreprise constitue aujourd'hui un levier fondamental de l'effectivité de la politique de protection des données personnelles. Il est dès lors indispensable que l'entreprise compose avec le nouveau rôle qui est le sien, ce qui implique une gestion des risques tant internes (I) qu'externes (II) à l'entreprise en matière de protection des données à caractère personnel. La présente étude vise à appréhender, outre le cadre juridique existant et les obligations qui en découlent pour les entreprises, la politique sécuritaire des entreprises en matière de collecte, traitement et conservation des données à caractère personnel.

I. – *L'IMPÉRATIF DE PROTECTION DES DONÉES PERSONELLES DANS L'ENTREPRISE : LA GESTION DU « RISQUE INTERNE » À L'ENTREPRISE*

56 % des entreprises françaises victimes de fraude indiquent qu'elles ont été commises par un fraudeur interne. Le cyber-fraudeur serait ainsi « *un employé dans 85 % des cas, qui dispose de moins de cinq ans d'ancienneté au sein de l'entreprise dans 51 % des cas et est âgé de moins de 40 ans dans 65 % des cas* » (La fraude en entreprise : tendances et risques émergents », 6e éd., Global Economic Crime Survey 2011, Étude réalisée par le cabinet PwC, 2011).

En matière de protection des données personnelles, la gestion du risque interne, c'est-à-dire du risque résultant de l'organisation et du fonctionnement de l'entreprise, suppose une parfaite connaissance de la loi « *Informatique et Libertés* » et surtout la sensibilisation des salariés aux problématiques liées à la protection des données personnelles, précisant notamment les rôles et les responsabilités de chacun (A).

La maîtrise du risque interne justifie par ailleurs la mise en place de dispositifs de surveillance des salariés et le recours accru aux nouvelles technologies pour endiguer notamment le développement des fraudes aux systèmes d'information en interne. Les dispositifs de surveillance des salariés sont toutefois très encadrés et doivent être pertinents, proportionnés et s'opérer dans le respect de la vie privée des salariés et des données personnelles ainsi collectées (B).

A. – *La sensibilisation, à tous les niveaux de l'entreprise, aux problématiques liées à la protection des données à caractère personnel*

1. L'émergence d'une culture d'entreprise intégrant l'impératif de protection des données personnelles

Les entreprises ont mis en place un ensemble de dispositifs techniques, normatifs et organisationnels, de façon à diffuser les bonnes pratiques en leur sein, assurer leur conformité à la règlementation applicable en matière de protection des données personnelles et, ainsi, réduire le coût et l'impact de la violation des données.

Cette réactivité des entreprises se traduit par des mesures organisationnelles et process visant à prévenir la violation des systèmes d'information : élaboration ou renforcement de la politique de sécurité des systèmes d'information, programme de lutte et d'identification des incidents de sécurité, création d'une cellule de crise en interne pour gérer les violations de données, formation et information des salariés, communication interne et externe sur la politique de sécurité de l'entreprise, autant d'éléments qui mettent en exergue le rôle dorénavant prépondérant des RSSI / DSI au sein de l'entreprise, mais également celui du correspondant informatique et libertés (CIL), dont l'action peut prendre plusieurs formes – conseil, recommandations, sensibilisation, médiation et alerte en cas de disfonctionnement.

Il s'agit aussi pour l'entreprise de mieux gérer les violations de données lorsqu'elles se réalisent (définition en amont des mesures techniques et organisationnelles à mettre en œuvre, reporting immédiat, modalités de la communication au public sur l'incident, etc.).

Il s'opère par ailleurs un développement des chartes de protection des données personnelles, chartes informatiques et codes éthiques relatifs à la sécurité des données personnelles et au respect de la vie privée des salariés et des consommateurs. Ces derniers formalisent les bonnes pratiques afin de les uniformiser, les diffuser dans l'entreprise, et augmenter leur applicabilité par les collaborateurs concernés, permettant « *non seulement de présenter au personnel une ligne de conduite claire et précise en la matière, mais aussi de communiquer de manière positive sur ces bonnes pratiques auprès des clients et du public* ». De même, les entreprises développent en partenariat avec la CNIL des « *règles d'entreprise contraignantes* » ou BCR (Binding Corporate Rules), codes de conduite internes qui définissent la politique d'un groupe en matière de transfert de données hors de l'Union européenne, visant à assurer un niveau de protection suffisant aux données transférées vers un pays tiers.

Il résulte de cette évolution des pratiques que la protection des données personnelles fait aujourd'hui partie intégrante de la culture d'entreprise, constituant dorénavant un facteur avec lequel les acteurs économiques doivent impérativement composer.

La sécurité des données est un enjeu stratégique et social pour les entreprises (La protection des données : un enjeu stratégique et social, Questions à Isabelle Falque-Pierrotin, Présidente de la CNIL, Hebdo édition affaires n° 309, 20 sept. 2012) et s'intègre progressivement au volet social de la responsabilité sociale de ces dernières (RSE). Les principes directeurs de l'OCDE à l'intention des entreprises multinationales, par lesquels l'OCDE émet des recommandations pour une conduite responsable des entreprises dans le contexte international, visent désormais expressément la sécurité des données à caractère personnel collectées, conservées, traitées ou diffusées par les entreprises (Principes directeurs de l'OCDE à l'intention des entreprises multinationales, révisés par réunion ministérielle de l'OCDE le 25 mai 2011). Il en va de même pour la norme internationale d'application volontaire ISO 26000 : 2010, ainsi que la norme ISO/IEC 27002 : 2013 relative à la gestion de la sécurité de l'information au sein de tout organisme.

Comme le souligne Isabelle Falque-Pierrotin, Présidente de la CNIL, ce développement a pour origine « *une vision utilitariste dans laquelle l'éthique n'a que peu de place : il s'agit de donner à l'entreprise un avantage concurrentiel, en suscitant la motivation des salariés ou en prévenant les atteintes à la réputation de l'entreprise* » (La protection des données : un enjeu stratégique et social, préc.). Il n'en demeure pas moins que l'impératif de protection des données personnelles figure aujourd'hui au rang des préoccupations éthiques de l'entreprise et impose aux opérateurs économiques davantage de transparence envers leurs salariés, clients et partenaires, dans la collecte et le traitement de leurs données personnelles.

2. La consécration du rôle moteur des entreprises en matière de protection des données personnelles par le projet de réforme du cadre juridique européen

La proposition de règlement d'application directe dans l'ensemble des États membres de l'Union européenne, appelé à remplacer la Directive européenne de 1995 (Proposition de règlement du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union, 7 févr. 2013, COM(2013) 48 final, 2013/0027 (COD)) et dont le texte définitif devrait être adopté en 2014 pour une entrée en vigueur deux ans plus tard, prévoit la fin des formalités administratives pesant jusqu'alors sur les entreprises et, dans le même temps, le développement de la gouvernance des normes internes des entreprises.

L'article 22 du projet de règlement stipule que « *le responsable du traitement adopte des règles internes et met en œuvre les mesures appropriées pour garantir, et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect du présent règlement* ». Cela implique que l'entreprise, au même titre que tout responsable de traitements de données, devra pouvoir justifier de la conformité des traitements au règlement européen et mettre en œuvre des mesures telles que :

- la tenue d'une documentation permettant de conserver la trace de tous les traitements effectués et leurs caractéristiques ;
- la mise en œuvre d'obligations en matière de sécurité des données ;
- la réalisation d'analyses d'impact des traitements de données jugées à risque ;
- l'adoption de règles contraignantes internes visant notamment à encadrer les transferts transfrontaliers de données ;
- la désignation d'un délégué à la protection des données (équivalent du CIL dans le dispositif français, dont la désignation est aujourd'hui facultative) ;
- l'élaboration de codes de bonne conduite, facultative mais encouragée par le projet de règlement.

Le projet de règlement européen n'a pas d'incidence sur les sanctions pénales applicables aux manquements aux règles en matière de protection des données personnelles. Il en va différemment pour les sanctions administratives susceptibles d'être prononcées, dans la mesure où l'article 79 du projet de règlement prévoit des amendes allant de 0,5 % à 2 % du chiffre d'affaires mondial pour les personnes morales et de 250 000 euros à 1 million d'euros pour les personnes physiques, soit une augmentation considérable du montant susceptible d'être prononcé (pour mémoire, les entreprises peuvent aujourd'hui être condamnées, en application de l'article 47 de la loi « *Informatique et Libertés* », à des sanctions pécuniaires pouvant atteindre au maximum 150 000 euros – 300 000 euros en cas de récidive). Il sera précisé que le montant de l'amende administrative est fixé en tenant compte de la nature, de la gravité et de la durée de la violation, du fait que l'infraction ait été commise délibérément ou par négligence, du degré de responsabilité du mis en cause et des éventuelles violations commises antérieurement, des mesures et procédures techniques et d'organisation mises en œuvre ainsi que du degré de coopération avec l'autorité de contrôle en vue de remédier à la violation.

Ainsi, le projet de règlement européen met fin à la possibilité pour l'entreprise de se retrancher derrière l'accomplissement des formalités administratives pour tenter de s'exonérer de sa responsabilité et confère aux opérateurs économiques un rôle fondamental et proactif en matière de protection des données personnelles,

notamment pour mieux sécuriser les flux transfrontaliers de données et prévenir de façon effective la cybercriminalité.

Si ce projet de refonte du cadre juridique européen s'inscrit dans la continuité du développement de la gouvernance des normes internes d'entreprise, il est indispensable pour les opérateurs économiques d'anticiper les obligations qui devraient très rapidement s'imposer à elles en matière de protection des données personnelles. Ces obligations auront, de toute évidence, un impact sur la gestion des risques internes à l'entreprise, notamment en matière de surveillance et de gestion de l'activité des salariés.

B. – *La surveillance des salariés*

Le salarié bénéficie du principe général du droit au respect de sa vie privée, en application de l'article 9 du code civil et de l'article 8 de la Convention européenne des droits de l'Homme. La Cour européenne des droits de l'Homme retient ainsi qu' « *aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de vie privée* » (CEDH, 4 mai 2000, aff. 28341/95, Rotaru c/ Roumanie, D. 2001., p. 1988, obs. Lepage A.), la Cour de cassation considérant au même titre que « *le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée* » (Cass. soc., 2 oct. 2001, nº 99-42.942, Sté Nikon France, Bull. civ. V, nº 291).

En définitive, la protection des systèmes informatiques et des données personnelles qu'ils contiennent contre d'éventuels agissements déloyaux d'employés constitue un intérêt légitime de l'entreprise.

Des aménagements à ce principe général sont possibles pour répondre aux intérêts légitimes de l'entreprise, le Code du travail précisant que « *nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* » (C. trav., art. L. 1121-1).

En d'autres termes, l'utilisation de procédés de surveillance susceptibles de porter atteinte aux droits et libertés des personnes, notamment au droit au respect de la vie privée, doit reposer sur un motif légitime (1) et respecter une condition de proportionnalité (2), outre le formalisme imposé par le Code du travail (3).

1. L'intérêt légitime de l'entreprise

La notion d'intérêt légitime de l'entreprise n'est définie par aucun texte légal. Toutefois, il est communément admis que l'intérêt légitime de l'entreprise est caractérisé lorsque l'employeur, à des fins disciplinaires, effectue une surveillance de ses employés, pour des motifs tombant dans l'une des deux catégories suivantes :

la sécurité des biens ou des personnes (vol, vandalisme, agression ou harcèlement, etc.) ;
des motifs économiques (exécution du travail des salariés et leur rendement).

En définitive, la protection des systèmes informatiques et des données personnelles qu'ils contiennent contre d'éventuels agissements déloyaux d'employés constitue un intérêt légitime de l'entreprise.

L'employeur dispose de divers moyens techniques pour surveiller l'activité des salariés : cybersurveillance (contrôle des connexions internet et de la messagerie électronique), géolocalisation, vidéosurveillance, autocommutateur téléphonique, contrôle d'accès par badgeage ou biométrie, système d'alertes professionnelles, etc.

Ces dispositifs sont autant de traitements de données personnelles, dès lors qu'ils enregistrent de nombreuses informations sur les salariés visés. À ce titre, ces derniers sont soumis à la réglementation relative à la protection des données personnelles (conditions de validité de la collecte et du traitement de données à caractère personnel, formalités administratives préalables, obligation d'information des personnes sur l'existence du traitement et les droits y afférents, obligation de sécurité et de confidentialité des données, etc.).

Ils doivent notamment se conformer au principe de proportionnalité, lequel impose que les données collectées soient « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* » (L. nº 78-17, 6 janv. 1978, art. 6, loi dite « *Informatique et Libertés* »). En d'autres termes, l'employeur ne peut pas, au nom de la protection des systèmes informatiques de l'entreprise et des données personnelles qu'ils contiennent, porter atteinte au droit à la protection des données personnelles et au respect de la vie privée dont les salariés peuvent eux-aussi se prévaloir.

2. Le principe de proportionnalité

La loi « *Informatique et Libertés* » et le Code du travail imposent à l'employeur de ne traiter, dans les dispositifs de surveillance des salariés, que les informations pertinentes et nécessaires au regard des objectifs poursuivis. L'impératif de sécurité doit ainsi s'accorder aux droits fondamentaux : il s'agit de trouver un équilibre entre la protection des intérêts de l'entreprise et la protection de la vie privée des salariés.

Faisant application du critère de proportionnalité, la CNIL est ainsi revenue sur la possibilité pour les entreprises de mettre en œuvre des dispositifs biométriques reposant sur le contour de la main aux fins de gestion des horaires des salariés, aux motifs que « (...) *son recours implique d'utiliser une partie de son corps, ce qui en soi est disproportionné au regard de la finalité de gestion des horaires* » – le recours à la biométrie est toutefois toujours autorisé s'agissant du contrôle d'accès des salariés et visiteurs ainsi que de la restauration sur les lieux de travail.

L'essentiel des contrôles et sanctions de la CNIL portent d'ailleurs sur la vidéosurveillance, la géolocalisation et la biométrie. La CNIL a ainsi prononcé une amende de 10 000 euros à l'encontre d'une société pour avoir, en dépit de la mise en demeure de mise en conformité adressée par la CNIL, manqué à l'obligation de proportionnalité du dispositif de vidéosurveillance (la société ayant placé au moins un de ses salariés sous une surveillance permanente et constante, situation qui a perduré en dépit de la mise en demeure pour mise en conformité adressée par la CNIL), à l'obligation d'information des salariés visés par le traitement, ainsi qu'à l'obligation d'assurer la sécurité des données (la CNIL relève notamment « *la brièveté des mots de passe* [permettant l'accès aux ordinateurs et aux

données personnelles contenues dans ces derniers], *leur déductibilité, leur simplicité et l'absence de renouvellement* » : CNIL, Délib. formation restreinte n° 2013-139, 30 mai 2013, SAS Professional service consulting). Une sanction pécuniaire d'un montant de 10 000 euros a également été prononcée à l'encontre d'une société ayant refusé de communiquer à l'un de ses salariés les données dont il demandait communication (données collectées par le système de géolocalisation mis en place sur son véhicule de service), ce refus constituant un manquement à l'obligation de garantir le droit d'accès (CNIL, Délib. formation restreinte n° 2013-213, 22 juin 2013, Sté Équipements Nord Picardie).

De même, la CNIL s'est récemment inquiétée de l'emploi par certaines entreprises de logiciels espions particulièrement intrusifs, les « *keyloggers* », capables d'enregistrer toutes les actions effectuées par les salariés sur leur poste informatique sans que ceux-ci s'en aperçoivent. La CNIL a ainsi rappelé que de telles pratiques, qui permettent une surveillance constante et permanente sur l'activité professionnelle des salariés concernés mais aussi sur leur activité personnelle résiduelle, sont totalement disproportionnées et ne se justifient que par un « *fort impératif de sécurité* », par exemple dans les domaines d'activité sensibles ou à très haute valeur ajoutée, pour lutter contre l'espionnage industriel (Fiche pratique CNIL, Keylogger : des dispositifs de cybersurveillance particulièrement intrusifs, 20 mars 2013).

Enfin, la mise en place de dispositifs de surveillance des salariés doit être accompagnée d'une information spécifique, par l'employeur, des personnes concernées.

3. Le formalisme imposé par le Code du travail

La mise en œuvre de dispositifs de surveillance des salariés par l'entreprise doit faire l'objet d'une information préalable de ces derniers.

Le Code du travail prévoit qu'aucune information concernant personnellement un candidat à un emploi ou un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance (C. trav., art. L. 1221-9 et L.1222-4). De même, le comité d'entreprise doit être (i) informé de tous traitements automatisés de gestion du personnel, préalablement à leur introduction dans l'entreprise, et toute modification de ceux-ci, et (ii) informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés (C. trav., art. L. 2323-32).

Bien qu'étroitement encadrée par le législateur, la surveillance des salariés contribue à la maîtrise du risque interne à l'entreprise en matière de protection des données personnelles.

La jurisprudence retient ainsi que l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés durant le temps du travail, seul l'emploi de procédés clandestins de surveillance étant jugé illicite (Cass. soc., 14 mars 2000, n° 98-42.090, Bull. civ. V, n° 101).

L'employeur ne peut mettre en œuvre un dispositif de contrôle des salariés qui n'a pas été préalablement porté à la connaissance de ces derniers (Cass. soc., 22 mai 1995, n° 93-44.078, Bull. civ. V, n° 164 ; Cass. soc., 15 mai 2001, n° 99-42.219, Bull. civ. V, n° 167), et ce même s'il ne pouvait être sérieusement allégué que le salarié ignorait l'existence du dispositif de contrôle (Cass. soc., 7 juin 2006, n° 04-43.866, Bull. civ. V, n° 206).

Bien qu'étroitement encadrée par le législateur, la surveillance des salariés contribue à la maîtrise du risque interne à l'entreprise en matière de protection des données personnelles. Le cadre juridique qui vient d'être décrit constitue dès lors un socle pour l'entreprise dans la définition de mesures de prévention des atteintes internes aux données personnelles traitées par cette dernière.

Outre les menaces internes, l'entreprise doit se prémunir contre un risque externe d'atteinte aux données personnelles, prévention qui constitue par ailleurs une obligation légale, dont le non-respect est susceptible d'engager sa responsabilité.

II. – *L'IMPÉRATIF DE PROTECTION DES DONÉES PERSONELLES DANS L'ENTREPRISE : LA GESTION DU « RISQUE EXTERNE » À L'ENTREPRISE*

Malgré l'amélioration des politiques de sécurité des systèmes et réseaux d'informations, les entreprises sont régulièrement victimes de vols de données, qui sont ensuite revendues à d'autres, concurrents ou non. Le deuxième opérateur mobile en Allemagne, Vodafone GmbH, a ainsi récemment été victime d'un piratage de grande ampleur, permettant à un ou plusieurs cybercriminels de voler les noms, adresses, dates de naissance, sexes et coordonnées bancaires de près de deux millions d'abonnés.

Dans une position arrêtée en première lecture le 4 juillet 2013, le Parlement européen indique que « *des cyberattaques à grande échelle sont susceptibles de provoquer des dommages économiques notables, tant du fait de l'interruption des systèmes d'information et des communications qu'en raison de la perte ou de l'altération d'informations confidentielles importantes d'un point de vue commercial ou d'autres données. Il y a lieu en particulier de veiller à sensibiliser les petites et moyennes entreprises innovantes aux menaces liées à ces attaques et à leur vulnérabilité à cet égard, en raison de leur dépendance accrue à l'égard du bon fonctionnement et de la disponibilité des systèmes d'information et de leurs ressources limitées en matière de sécurité de l'information* » (Proposition du Parlement européen arrêtée en première lecture le 4 juill. 2013 en vue de l'adoption de la directive 2013/40/UE du Parlement européen et du Conseil relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil).

Le constat d'un tel risque externe à l'entreprise conduit à faire peser sur les opérateurs économiques une obligation de protection des systèmes d'informations et des données (A). Le droit pénal vient par ailleurs apporter un

ensemble de réponses en cas de réalisation d'attaques à l'intégrité des données personnelles, par la définition de qualifications pénales (B).

A. – *L'obligation de protection des données personnelles par l'entreprise*

1. Le cadre légal de l'obligation de protection des données personnelles par l'entreprise

L'obligation de sécurisation des données résulte de l'article 226.17 du code pénal (l'article 226-17 du code pénal dispose que « *le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende* »), lequel renvoie à l'article 34 de la loi « *Informatique et Libertés* », qui prévoit l'obligation à la charge de tout responsable de traitement de « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».

Ainsi, le fait de ne pas prendre toutes les « *précautions utiles* » pour protéger un traitement comportant des données personnelles est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

L'obligation de sécurisation des données personnelles ainsi définie demeure imprécise, s'agissant notamment de la définition des « *précautions utiles* » à adopter par le responsable de traitement. En définitive, il s'agit pour les entreprises de mettre en œuvre des mesures appropriées et efficaces en vue de garantir la protection des données personnelles, et d'être en mesure de justifier la mise en œuvre de ces dernières.

Pour aider les entreprises à assurer leur conformité aux dispositions susvisées et prévenir les failles de sécurité, la CNIL a publié en 2010 un guide présentant les précautions élémentaires à mettre en place pour améliorer la sécurité d'un traitement de données à caractère personnel (Guide CNIL, La sécurité des données personnelles, éd. 2010), en matière d'authentification des utilisateurs (mot de passe individuel, complexe et secret), de gestion des habilitations et de sensibilisation des utilisateurs, de sécurité des postes de travail (verrouillage automatique des postes de travail inactifs), de sécurisation de l'informatique mobile, de maintenance, de sécurité des locaux (vérification des habilitations et des accès par badge nominatif, digicode, contrôle des prestations de gardiennage, etc.), de sécurité du réseau informatique interne (gestion des accès et habilitations informatiques), de sécurité des serveurs et des applications (sauvegardes régulières), d'archivage et de sous-traitance.

Deux guides complémentaires ont été publiés par la CNIL en 2012 pour améliorer la maîtrise des traitements complexes, proposant une méthode pour identifier et traiter les risques ainsi qu'un ensemble détaillé de mesures et de bonnes pratiques (Guide CNIL, Gestion des risques vie privée, Parties I « La méthode » et II « Catalogue de mesures », éd. 2012). La CNIL formule notamment des recommandations en termes de modalités de sauvegarde des données, de protection des archives, de contrôle de l'intégrité des données, de traçabilité de l'activité sur le système informatique, de gestion des atteintes à la sécurité, de contrôle des accès logiques et physiques, de lutte contre les codes malveillants et de réduction des causes de vulnérabilité des réseaux et systèmes informatiques.

2. Les enjeux du respect de la protection des données personnelles par l'entreprise

Les enjeux de la sécurisation des systèmes d'information de l'entreprise sont considérables. Toute violation de l'intégrité de ces derniers emporte des risques lourds pour l'entreprise – entrave au bon fonctionnement de l'entreprise, atteinte aux éléments constitutifs du patrimoine de l'entreprise (vols de fichiers, vols d'informations, contrefaçons, concurrences déloyales et parasitismes économiques), violation des secrets de l'entreprise (espionnage industriel), conséquences commerciales et financières.

L'entreprise qui laisse courir en son sein des risques d'atteinte à la protection des données personnelles et à la sécurité de ses systèmes d'informations s'expose à des sanctions administratives publiques ou non publiques – avertissement ou sanction pécuniaire (sur l'année 2012, 13 sanctions ont été prononcées dont 9 avertissements et 4 sanctions pécuniaires oscillant entre 1 000 et 10 000 euros. Les manquements retenus par la CNIL ont été, pour l'essentiel, la collecte déloyale de données, le défaut des formalités préalables, le défaut de sécurité et de confidentialité des bases de données, le défaut d'information de la personne visée par le traitement, le non-respect du droit d'accès, ainsi que le non-respect du principe de proportionnalité du dispositif : Rapport d'activité CNIL, 2012, p. 58) – ainsi que des sanctions pénales (C. pén., art. 226-16 à 226-24) et civiles, la responsabilité civile de l'entreprise pouvant être engagée par tout tiers (salarié, client, partenaire) justifiant d'atteinte à la protection de ses données personnelles lui causant un préjudice et dont il est sollicité réparation (Griguer M., Protection des données personnelles : conformité et bonnes pratiques des entreprises, Cah. dr. entr. n° 1, janv. 2013, prat. 5).

Plus encore, les manquements à la protection des données comportent des risques substantiels d'atteinte à l'image et la réputation de l'entreprise, dont les conséquences économiques peuvent se révéler désastreuses notamment pour les sociétés cotées, les failles de sécurité étant de ce fait considérées comme des « *risques systémiques* » pour les entreprises (Griguer M., préc.). Pour mémoire, la cyber-attaque de la multinationale Sony, au cours du mois d'avril 2011, qui a exposé les données personnelles (notamment les coordonnées bancaires et les identifiants) des 77 millions d'utilisateurs du PlayStation Network, a entraîné une chute du cours de bourse immédiate de près de 5 %, à laquelle s'est ajouté le coût de la maintenance, de la sécurisation du réseau et des compensations pour les consommateurs, ainsi qu'une sanction pécuniaire de 250 000 livres prononcée en janvier 2013 par l'Information Commissioner's Office (ICO), l'équivalent britannique de la CNIL.

B. – *Les réponses du droit pénal en cas de réalisation du risque d'atteinte à l'intégrité des données personnelles*

Les entreprises sont ciblées par les cybercriminels en raison des nombreuses données parfois sensibles que contiennent leurs systèmes. Le vol ou la manipulation de données suppose le plus souvent, le « *piratage d'un système* », c'est-à-dire l'accès illégal à ce dernier (1).

La dénomination sociale, le logo, la marque ou l'enseigne des opérateurs économiques peuvent également être usurpés afin de tromper des clients ou prospects et obtenir de ces derniers la communication d'informations personnelles (2).

1. Les réponses du droit pénal en cas d'atteinte aux systèmes informatiques des entreprises

Les systèmes informatiques centralisent et agrègent de nombreuses données et constituent de ce fait une cible tentante pour qui s'intéresse à ces informations parfois insuffisamment protégées qui, on l'a vu, sont susceptibles d'être utilisées à des fins lucratives.

En France, l'accès illégal à un système informatique est une infraction pénale : la loi nº 88-19 du 5 janvier 1988 sur la fraude informatique, dite loi « *Godfrain* », permet de sanctionner toutes les intrusions non autorisées dans un système informatique. Les sanctions prévues varient en fonction du degré d'incidence de l'intrusion sur le système en cause :

> l'article 323-1 du code pénal sanctionne les intrusions dans un système de traitement automatisé de données de trois ans d'emprisonnement et de 30 000 euros d'amende. L'alinéa 2 du même article prévoit une aggravation de peine lorsque l'accès frauduleux au système a entraîné la suppression ou la modification des données ou l'altération du fonctionnement du système. L'accès frauduleux est constitué dès lors qu'une personne non habilitée pénètre dans un système de traitement automatisé de données tout en sachant qu'elle est dépourvue d'autorisation ;
> l'article 323-2 du code pénal incrimine le fait de fausser ou d'entraver le fonctionnement du système informatique, passible de cinq ans d'emprisonnement et de 75 000 euros d'amende. Peu importe qu'il y ait eu accès, autorisé ou non, au système informatique de la victime ; il s'agit ici de réprimer des dégâts causés volontairement aux données et au système ;
> l'article 323-3 du code pénal vise la modification frauduleuse de données. Il sanctionne l'introduction, la suppression ou la modification frauduleuse de données de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Les peines d'emprisonnement et d'amende des infractions prévues aux articles 323-1, 323-2 et 323-3 du code pénal susvisés ont été aggravées par la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Cette dernière a par ailleurs inséré un nouvel article 323-3-1 dans le code pénal permettant de réprimer le trafic de moyens destinés à commettre des infractions en matière informatique, en sanctionnant l'importation, la détention, l'offre, la cession et la mise à disposition des moyens techniques, matériels ou logiciels permettant de telles attaques.

La tentative de commission des délits susvisés est punie des mêmes peines, en application de l'article 323-7 du code pénal. L'article 323-4 du même code permet en outre de réprimer les associations de malfaiteurs, dès leurs premiers efforts accomplis en vue de l'intrusion dans un système de traitement automatisé de données. Enfin, le recel d'informations obtenues suite à une intrusion frauduleuse dans un système de traitement automatisé de données est puni par l'article 321-1 du code pénal de cinq ans d'emprisonnement et de 375 000 euros d'amende.

2. Les réponses du droit pénal en cas d'usurpation d'identité d'entreprises dans le cadre d'un hameçonnage (« phishing ») ou de pratiques analogues

Parmi les techniques préférées des cybercriminels figure le hameçonnage, qui consiste à tromper l'internaute *via* un courriel semblant émaner d'une entreprise de confiance (banque, site de commerce ou de paiement en ligne, réseau social, etc.) et renvoyant vers un site web pour l'inviter à révéler ses identifiants personnels (un faux site à en-tête d'une banque, par exemple). Les données personnelles sont ensuite dérobées et mises sur le « *marché noir* » des données personnelles précédemment évoqué.

La Caisse d'allocations familiales (CAF) a ainsi été victime d'une campagne de hameçonnage, aux termes de laquelle un courriel frauduleux invitait son destinataire à cliquer sur un lien pour se rendre sur le site de l'organisme afin qu'il puisse percevoir des droits dont il était censé bénéficier. Le lien figurant dans le courriel redirigeait la personne visée vers un site web localisé en Hongrie imitant le site web de la CAF et encourageait l'utilisateur à s'identifier et à entrer ses coordonnées bancaires.

D'après la note d'orientation nº 4 du Comité de la Convention Cybercriminalité (T-CY), une usurpation d'identité se décompose en trois étapes :

> phase 1 : l'obtention des renseignements personnels par des moyens divers tels que le vol physique, l'utilisation de moteurs de recherche, des attaques de l'intérieur ou de l'extérieur (accès illicite aux systèmes informatiques, Trojans, « keyloggers », logiciels espions et autres programmes malveillants), par le recours au hameçonnage ou à d'autres techniques d'ingénierie sociale ;
> phase 2 : la possession et la cession des renseignements personnels (par ex., la vente de ces informations à des tiers) ;
> phase 3 : l'utilisation des renseignements personnels pour se livrer à des activités frauduleuses ou commettre d'autres infractions, par exemple en prenant l'identité d'une autre personne pour exploiter des comptes en banque ou des cartes de crédit, ouvrir de nouveaux comptes, contracter des prêts et crédits, commander des biens et services ou diffuser des programmes malveillants.

Ainsi, l'usurpation d'identité (y compris le hameçonnage et les conduites analogues) sert généralement à la préparation de nouveaux agissements criminels, tels que la fraude informatique.

En France, la loi dite *LOPPSI II* (L. nº 2011-267, 14 mars 2011, d'orientation et de programmation pour la performance de la sécurité intérieure, JO 15 mars) a introduit dans le Code pénal un délit spécifique d'usurpation d'identité s'étendant aux réseaux numériques. Le nouvel article 226-4-1 du code pénal sanctionne ainsi « *le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération* ».

Cette incrimination comble un vide juridique en permettant de répondre à des actes malveillants qui ne pouvaient, jusque-là, tomber sous le coup d'aucune qualification pénale. Le délit d'usurpation numérique ainsi défini ne vise pas seulement le nom de la victime (personne physique ou morale), mais son identité et plus largement n'importe quelle donnée « *permettant de l'identifier* ». Les informations relatives à l'identité d'une personne morale susceptibles d'être considérées comme des données « *identifiantes* » sont nombreuses : dénomination sociale, nom commercial, sigle, marque, logo, enseigne, nom de domaine, adresse IP, adresse e-mail interne, etc.

***

La cadre juridique de la protection des données à caractère personnel est en profonde mutation, avec pour objectif la définition d'« *une politique plus globale et plus cohérente à l'égard du droit fondamental à la protection des données à caractère personnel* » (Proposition de règlement, préc., p. 2.), impératif qui se couple avec l'exigence de sécurité des réseaux et de l'information (Proposition de Directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union, 7 févr. 2013, COM(2013) 48 final, 2013/0027 (COD)).

De telles évolutions impliquent une adaptation permanente des acteurs économiques, adaptation indispensable pour prévenir les failles de sécurité mais pourtant peu évidente notamment pour les TPE/PME, pour lesquelles le risque de non-conformité est plus sensible.

De fait, l'entreprise constitue aujourd'hui un levier fondamental de l'effectivité de la politique de protection des données personnelles, rôle initialement imposé par les pouvoirs publics mais que l'entreprise a su s'approprier, en intégrant progressivement l'impératif de protection des données personnelles à la « *culture d'entreprise* », jusqu'à en faire une arme concurrentielle.

Il est dès lors indispensable que l'entreprise compose avec le nouveau rôle qui est le sien, ce qui implique une gestion des risques tant internes qu'externes à l'entreprise en matière de protection des données. Plus encore, il s'agit pour les opérateurs économiques de prendre part aux débats et défendre leurs intérêts dans la redéfinition du cadre juridique et politique de la protection des données à caractère personnel.