RLDI 1531

De plus en plus de sociétés européennes se trouvent confrontées à des demandes de *e-discovery* provenant des États-Unis. Cette question doit être analysée notamment au regard du droit de la vie privée et de la protection des données à caractère personnel. Mes Olivier Proust et Cédric Burton proposent une analyse pragmatique et pluridisciplinaire de ce conflit de droits, des risques et des enjeux auxquels sont confrontées les entreprises européennes.

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(1)

Par Olivier PROUST
Avocat au Barreau de Paris
Hunton & Williams

Par Cédric BURTON
Avocat au Barreau de Bruxelles
Hunton & Williams

INTRODUCTION

Le domaine de la protection des données à caractère personnel a déjà, par le passé, été la source de conflits de droits entre l'Europe et les États-Unis (transfert de données, affaire SWIFT, échange de données PNR, …). Le débat qui se déroule en ce moment autour de la question des règles de *e-discovery* (2) n'échappe pas à la règle.

À l'heure de la mondialisation, nombre de sociétés implantées en Europe ont leur société mère aux États-Unis ou appartiennent à un groupe de sociétés dont le siège social est situé aux États-Unis. Ces sociétés européennes doivent à la fois respecter le droit national du pays dans lequel elles sont implantées et appliquer les consignes qui leurs sont données par leur société mère. Dans ce contexte, les règles de *e-discovery* mettent en exergue un conflit juridique et philosophique entre les États-Unis et l'Europe. En effet, dans leur application, ces règles se heurtent aux principes européens sur la protection des données à caractère personnel et le respect de la vie privée. Dès lors, les sociétés européennes sont souvent prises entre le marteau et l'enclume, ne sachant pas s'il convient ou non d'appliquer ces règles, ni comment.
Dirigeants d'entreprise, avocats, magistrats et autorités nationales de protection des données à caractère personnel ont ainsi la lourde tâche de trouver un terrain d'entente entre deux systèmes juridiques qui se fondent sur des règles de procédure différentes et sur une conception de la protection des données à caractère personnel divergente. Après une présentation générale des règles de *e-discovery* (I), il conviendra d'analyser le conflit entre ces règles fondamentales de la procédure civile américaine et le droit européen de la protection des données à caractère personnel et de la vie privée (II) avant de s'interroger sur les éventuelles solutions applicables (III).

I. – LE CARACTÈRE FONDAMENTAL DES RÈGLES DE *E-DISCOVERY* EN DROIT AMÉRICAIN (3)

A. – Les règles de *discovery* aux États-Unis

Aux États-Unis, dans le cadre d'une procédure judiciaire civile, les entreprises ont l'obligation de conserver et de communiquer à la partie adverse l'ensemble des documents internes qui présentent un intérêt pour le litige en cours. À la différence des pays de tradition civiliste, les règles de procédure civile américaine (4)

(1) Les propos tenus dans le présent article n'engagent que les auteurs et pas l'institution à laquelle ils appartiennent. (2) « *Compulsory disclosure, at a party's request, of information that relates to the litigation. The primary discovery devices are interrogatories, depositions, requests for admissions, and requests for production. Although discovery typically comes from parties, courts also allow limited discovery from non-parties* », Dictionnaire *Black's Law*, 2004, 8° éd. (3) Le lecteur attentif voudra bien excuser les auteurs pour la vulgarisation des règles de procédure américaine, le but de cet article étant de présenter le conflit entre les règles de *e-discovery* et les règles européennes de protection de la vie privée et des données à caractère personnel. (4) La présente analyse se fonde sur les règles fédérales de procédure civile. Il convient de souligner que les règles de procédure civile aux États-Unis diffèrent d'un État à l'autre même si les règles fédérales sont de plus en plus utilisées comme modèle au sein de chaque état.

se fondent sur une mise en état de l'affaire par les parties au litige (principe de l'accusatoire) (5). La production de documents, la constitution du dossier, l'audition des témoins sont réalisées par les parties elles-mêmes. Cette phase du litige s'appelle « *pre-trial discovery* ».

Les règles de *discovery* ont ainsi pour but de permettre aux parties de mener une enquête, et notamment de collecter les informations pertinentes pour le dossier, de les analyser et de les communiquer à la partie adverse. Une partie au litige peut ainsi exiger la production puis l'examen de tous les documents indiqués dans sa demande. Les éléments non-contestés par les parties sont, ensuite, soumis au tribunal qui les reconnaîtra comme des faits. Durant cette phase, le juge ou le jury joue un rôle subsidiaire et n'intervient qu'en cas de litige relatif à la reconnaissance des faits ou à la production de documents.

En cas de non-respect des règles de *discovery*, les sociétés peuvent être lourdement sanctionnées (6) : jugement contraire à leur demande, inférence négative (7), condamnation à verser une indemnité financière suite à une action en responsabilité, sanctions pénales (amendes pénales, emprisonnement).

De la même manière, certaines autorités administratives peuvent contraindre une société à produire des documents internes lorsque ceux-ci présentent un intérêt dans le cadre d'une enquête administrative (par exemple, pour les enquêtes menées par la *Security and Exchange Commission*, à savoir l'autorité de régulation financière).

Ainsi, les sociétés américaines ont l'obligation de conserver tous les documents pertinents en vue de les produire dans le cadre d'une éventuelle procédure judiciaire à laquelle elles seraient partie, ou dans le cadre d'une enquête administrative.

B. – L'apparition récente de la règle de *e-discovery*

Jusqu'à une date récente, les règles de *discovery* concernaient principalement les documents sur support papier. Une réforme des règles de procédure civile aux États-Unis en 2006 (8) a précisé les conditions dans lesquelles les entreprises américaines sont désormais tenues de conserver et de produire tous les documents et informations conservés sous forme électronique (e-mails des salariés, dossiers électroniques détenus par les responsables des ressources humaines, disques durs, serveurs partagés, logs de connexion, etc.) (9).

Concrètement, l'obligation de conserver et de communiquer les informations stockées sur un support électronique peut être subdivisée en plusieurs étapes. Premièrement, les entreprises ont l'obligation de préserver tout document *pouvant* contenir des éléments de preuve pour un litige qui peut être *raisonnablement anticipé*. Deuxièmement, les parties ont l'obligation de conserver les informations pertinentes à un litige dès qu'une partie est citée à comparaître ou lorsqu'une demande en ce sens leur est formulée par une autorité judicaire ou administrative. Troisièmement, une fois que ces données sont conservées, l'entreprise doit les rassembler et les analyser. Cette analyse est primordiale parce qu'une sélection des informations est, ensuite, réalisée par les parties afin de déterminer lesquelles sont pertinentes pour le litige et lesquelles doivent être communiquées à la partie adverse ou à l'autorité chargée de mener l'enquête. Enfin, la dernière étape consiste à communiquer ces informations à la partie adverse, puis au tribunal qui a été saisi du litige.

> Le conflit entre les règles américaines de *e-discovery* et le droit européen de protection des données à caractère personnel met en exergue une différence de conception de la protection des données personnelles entre les deux continents.

Afin d'éviter d'engager leur responsabilité du fait du non-respect des règles de *e-discovery*, certaines entreprises américaines ont décidé de mettre en place un système d'archivage automatique qui scanne tous les documents et toutes les communications électroniques conservés sur le réseau informatique de l'entreprise. Ces informations sont, ensuite, copiées et conservées sur les serveurs de l'entreprise en vue d'un éventuel litige. Bien souvent, les procédures judiciaires ou les enquêtes administratives dépassent le cadre national américain (10) et les sociétés américaines doivent se tourner vers leurs filiales européennes pour demander la communication de documents. Dès lors que les délais impartis sont très courts, les sociétés européennes sont souvent contraintes de répondre rapidement et peuvent être prises au dépourvu face à la complexité d'une telle demande.

II. – UNE MISE EN ŒUVRE COMPLEXE DES RÈGLES DE *E-DISCOVERY* EN EUROPE

Alors que les règles de *e-discovery* sont obligatoires outre-Atlantique, une société européenne peut rencontrer des difficultés à répondre à une demande de communication de documents en raison des nombreux obstacles juridiques en droit européen (11).

A. – Le conflit entre les règles de *e-discovery* et le droit européen de la protection des données à caractère personnel (12)

Le conflit entre les règles américaines de *e-discovery* et le droit européen de protection des données à caractère personnel met en exergue une différence de conception de la protection des données personnelles entre les deux continents. Aux États-Unis, la protection des données à caractère personnel est traitée de manière sectorielle (13) et il n'existe pas, en l'état actuel du droit, de cadre législatif fédéral à vocation universelle en matière de protection des données à caractère personnel. À l'inverse, au sein de l'Union européenne, la protection des données à

(5) Voir « *Rules 16, 26 and 34 of the US Federal Rules of Civil Procedure* ». Pour une comparaison des règles de procédure civile belge et des règles de procédure de *discovery* aux États-Unis, voir Van Leyseele P., Pour un modèle belge de la procédure de *Discovery*, J.T., n° 5837 - 13/1997, p. 225. **(6)** Le fait de ne pas se conformer à ces règles de procédure est appelé « *spoliation* ». **(7)** Lorsque des documents ont été détruits ou n'ont pas été produits, le juge ou le jury peut en déduire que ces documents détruits ou non produits étaient pertinents pour le litige et utiles au soutien de la prétention de l'une des parties. Cette conséquence s'appelle « *inférence négative* ». **(8)** Cette réforme est entrée en vigueur aux États-Unis, le 1er décembre 2006. **(9)** Voir « *Article 34 (a) (1) (A) of the US Federal Rules of Civil Procedure: Any designated documents or electronically stored information – including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations – stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form* ». Pour plus d'informations, voir <http://www.uscourts.gov/rules/supct1105/CV_Clean.pdf#page=7>. **(10)** Il convient de noter que si l'une des parties considère que des documents ou données détenus par une filiale européenne de son adversaire lui sont utiles au soutien de sa prétention, elle peut demander au juge d'ordonner à la société américaine mais également à ses filiales européennes de produire les documents pertinents pour le litige. **(11)** En vue de présenter la problématique de *e-discovery* dans un contexte de conflit américano-européen, il sera souvent fait référence dans l'article à la directive communautaire 95/46/CE. Le lecteur veillera donc à lire les présents développements à la lumière des lois nationales transposant la directive au sein de chaque État membre. **(12)** Pour une analyse du conflit juridique entre les règles de *e-discovery* et le droit européen de protection des données à caractère personnel, voir Fred H. Cate and Margaret P. Eisenhauer, « *Between a rock and a hard place : the conflict between European data protection laws and U.S. civil litigation document production requirements* », Privacy and Security Law, BNA Reporter, vol. 6, n° 6, 2 mai 2007, pp. 1-5. **(13)** Pour la protection des données médicales, voir « *Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. 164.501* ».

caractère personnel a une vocation universelle et a été érigée au rang de liberté fondamentale (14). Depuis la transposition en droit national de la directive 95/46/CE (15), le régime juridique de la protection des données à caractère personnel est harmonisé au niveau européen. D'un point de vue européen, la communication d'informations et de documents vers les États-Unis constitue un traitement de données à caractère personnel qui tombe sous le champ d'application de la directive 95/46/CE et des différentes lois nationales de transposition (16). En effet, toute opération qui consiste à analyser, conserver et communiquer des données à caractère personnel, ce qui est le cas dans le cadre d'une demande de *e-discovery*, constitue un traitement de données à caractère personnel (17). La notion de « *donnée à caractère personnel* » est définie de manière suffisamment large de sorte que la directive 95/46/CE puisse théoriquement s'appliquer à toute communication de documents (contrat, courriel, note interne, fichier, log file, carnet d'adresses, etc.). En effet, il suffit qu'une personne physique (salarié, cocontractant, fournisseur, etc.) (18) soit identifiée ou identifiable dans un document grâce à une ou plusieurs données personnelles (nom, adresse, courriel, etc.) pour que le régime de protection des données à caractère personnel s'applique (19).

B. – La recherche d'une base légale au traitement des documents d'entreprise

La communication de documents dans le cadre d'une procédure judiciaire ou administrative américaine couvre plusieurs opérations telles que la conservation, l'analyse, ou le transfert de données. Ce traitement de données à caractère personnel doit être mis en œuvre conformément aux principes énoncés dans la directive 95/46/CE et dans la loi nationale applicable. En particulier, les données doivent être traitées loyalement et licitement et le traitement doit respecter le principe de proportionnalité, à savoir que les données collectées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées.

> La communication de documents dans le cadre d'une procédure judiciaire ou administrative américaine couvre plusieurs opérations telles que la conservation, l'analyse, ou le transfert de données.

La première difficulté consiste à démontrer que le traitement de données est légitime (20). À ce titre, le consentement préalable des salariés ne permet pas systématiquement de légitimer un traitement de données à caractère personnel. Hormis le fait qu'il peut être difficile en pratique de recueillir le consentement des personnes, celui-ci n'est valable que si la personne concernée a manifesté une volonté libre, spécifique et informée (21). Or, le Groupe de travail de l'Article 29 (22) considère que, dans un contexte salarié, l'individu se trouve dans une relation de subordination et ne peut *a priori* donner un consentement libre (23). L'employé doit avoir la possibilité de refuser de donner son consentement sans préjudice ; ce qui est difficilement envisageable dans une situation de dépendance hiérarchique. Enfin, le consentement doit être révocable, ce qui semble *a priori* exclu une fois que le document a été communiqué à la personne ou à l'autorité qui en fait la demande.

Dès lors, le responsable du traitement doit se fonder sur l'une des autres bases légales énoncées à l'article 7 de la directive 95/46/CE pour légitimer le traitement. Sur la base de la doctrine du Groupe de l'Article 29, l'exception énoncée à l'article 7-c) de la directive 95/46/CE, à savoir le respect d'une obligation légale, doit s'interpréter comme s'appliquant uniquement aux obligations légales exécutées au sein de l'Union européenne. Dès lors, une société européenne ne pourrait pas se fonder sur cette exception pour exécuter une règle de procédure américaine. En conséquence, seul l'article 7-f) relatif à la poursuite d'un intérêt légitime, semble pouvoir s'appliquer en l'espèce. Le responsable du traitement doit ainsi démontrer que la communication de documents répond à un intérêt légitime, à savoir répondre à une obligation légale aux États-Unis, et que le traitement de données à caractère personnel est nécessaire à la poursuite de cet intérêt (24). En tout état de cause, il semble nécessaire d'analyser le traitement au cas par cas et de mettre en balance les intérêts en présence, à la lumière du principe de proportionnalité (25) et des risques de sanction aux États-Unis ou d'atteinte à la vie privée des personnes concernées (26).

Par ailleurs, le responsable du traitement doit délimiter la durée de conservation des données. Une conservation systématique des *backups* ou la conservation illimitée des documents dans une base de donnée afin d'anticiper toute demande de *e-discovery* (comme cela se fait souvent aux États-Unis) serait contraire au principe de pro- >

---

(14) Voir article 8 de la Charte des droits fondamentaux de l'Union européenne, article 8 de la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales et la jurisprudence de la Cour européenne des droits de l'Homme. **(15)** Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. **(16)** Voir par ex. « *Affaire Discovery : un nouveau dossier sensible avec les États-Unis* », CNIL, 28e Rapport d'activité 2007, p. 80. **(17)** Article 2-b) de la directive 95/46/CE : constitue un traitement de données à caractère personnel « *toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* ». **(18)** Ainsi, l'entreprise à laquelle il incombe de préserver, d'analyser et de communiquer l'ensemble des documents requis par une autorité judiciaire ou administrative américaine est susceptible de traiter des données personnelles sur des personnes autres que ses salariés. **(19)** Article 2-a) de la Directive 95/46/CE : constitue une donnée à caractère personnel « *toute information concernant une personne physique identifiée ou identifiable* (personne concernée) ; *est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* ». **(20)** Article 6 de la directive 95/46/CE : « *Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités* ». Il convient de noter que les données sensibles ne peuvent être traitées, sauf consentement de la personne concernée ou si le traitement remplit l'une des exceptions prévues par le droit national applicable. De plus de nombreuses autorités de protection des données vont considérer que leur transfert à l'étranger est interdit. Voir, par exemple, les articles 6, 7 et 8 de la loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Pour plus d'informations sur l'article 8 et les données dites judicaires, voir Burton C., Poullet Y., À propos de l'avis de la Commission de protection de la vie privée du 15 juin 2005 sur l'encadrement des listes noires, R.D.T.I., 23, pp. 79-122. **(21)** Article 2-h) de la Directive 95/46/CE : Le consentement de la personne concernée est défini comme « *toute manifestation de volonté, libre, spécifique et informée par laquelle une personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement* ». **(22)** Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, regroupant les autorités de protection des données personnelles des 27 pays membres de l'Union européenne. **(23)** Voir l'Avis 8/2001 du Groupe de l'Article 29 sur le traitement des données à caractère personnel dans le contexte professionnel ; voir aussi le guide de la CNIL, Transferts de données à caractère personnel vers des pays non-membres de l'Union européenne, 2007. **(24)** Article 7-f) de la directive 95/46/CE : « *le traitement de données à caractère personnel ne peut être effectué que si* (…) *il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement* (…) ». **(25)** Sur le principe de proportionnalité et son application en matière de protection des données à caractère personnel, voir Kuner C., « *Proportionality principle* », *Privacy and Security Law*, BNA reporter, vol. 7, n° 44, 10 nov. 2008, pp. 1615-1619. **(26)** Voir l'Avis 1/2006 du Groupe de l'Article 29 relatif à l'application des règles européennes de protection des données aux dispositifs internes d'alerte professionnelle (« *whistleblowing* ») dans les domaines bancaire, de la comptabilité, du contrôle interne des comptes, de l'audit, de la lutte contre la corruption et des infractions financières, pp. 7-8, <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_fr.htm>.

portionnalité qui impose de conserver les données personnelles pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont traitées (27). Au-delà d'une durée déterminée, les données personnelles doivent être effacées, sauf lorsque des dispositions légales imposent la conservation des documents pendant une certaine durée (par exemple, les documents comptables, les documents des ressources humaines, les contrats électroniques, etc.). Enfin, les personnes concernées doivent être informées du traitement de leurs données par le responsable du traitement et ont le droit d'accéder à leurs données, de les rectifier et, le cas échéant, de s'opposer au traitement dans les conditions définies par le droit national. Les personnes concernées doivent être en mesure d'exercer ces droits à tout moment.

C. – L'accomplissement des formalités préalables auprès de l'autorité nationale de protection des données à caractère personnel

En tant que responsable de traitement, chaque société doit déclarer les traitements qu'elle met en œuvre auprès de l'autorité nationale de protection des données à caractère personnel. Ces formalités peuvent varier d'un État membre à un autre (déclaration, demande d'autorisation, désignation d'un correspondant informatique et libertés). L'absence de déclaration peut être sanctionnée pénalement selon le régime applicable dans chaque pays (28). Ainsi, la société européenne qui entend communiquer des documents dans le cadre d'une procédure *e-discovery* doit avant tout s'assurer qu'elle a réalisé les formalités préalables auprès de l'autorité de protection des données à caractère personnel et que les déclarations réalisées couvrent cette finalité.

De plus, le responsable du traitement doit accomplir les formalités applicables au transfert de données vers les États-Unis, au risque d'encourir des sanctions pénales (29). En effet, l'article 25 de la directive 95/46/CE prévoit que « *le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement* (…) *ne peut avoir lieu que si* (…) *le pays tiers en question assure un niveau de protection adéquat* ». Or, les États-Unis ne figurent pas sur la liste des pays reconnus par la Commission européenne comme assurant un niveau de protection adéquat. Néanmoins, le transfert de données vers les États-Unis peut être autorisé sur la base de l'une des exceptions limitativement énoncées dans la directive 95/46/CE. Celle-ci prévoit notamment le cas où le transfert est nécessaire ou juridiquement obligatoire « *pour la constatation, l'exercice ou la défense d'un droit en justice* » (30). Il est légitime de se demander si le transfert de données dans le cadre d'une procédure *e-discovery* peut se fonder sur cette exception. Or, le Groupe de l'Article 29 considère que cette exception ne s'applique qu'aux litiges qui se déroulent dans un État membre de l'Union européenne, sur le fondement d'une disposition législative nationale, et exclut donc son application aux règles de *e-discovery* (31). Le responsable du traitement semble donc contraint de recourir à d'autres moyens, tels que les clauses contractuelles standards ou les règles internes (BCR) (32) pour légitimer le transfert. Précisons enfin que, s'agissant des États-Unis, les transferts de données émis à partir de l'Union européenne vers une entreprise américaine ayant adhéré au *Safe Harbor* (33) bénéficie d'un régime de formalités plus souple dans la plupart des États membres.

> Le transfert de données vers les États-Unis peut être autorisé sur la base de l'une des exceptions limitativement énoncées dans la directive 95/46/CE.

D. – Le risque d'atteinte à la vie privée des salariés

Dans le contexte de *e-discovery*, il est parfois demandé aux sociétés de communiquer le contenu du disque dur d'un ou plusieurs salariés et les copies de leurs messageries électroniques. Aux États-Unis, l'accès aux courriers électroniques et aux documents contenus sur le disque dur d'un salarié est souvent considéré comme un droit de l'employeur car ces documents sont par nature des « *business documents* » (34). En revanche, en Europe, l'accès au disque dur ou aux archives d'un salarié se heurte à deux principes fondamentaux que sont le droit au respect de la vie privée (35) et le secret des correspondances (36) et des communications électroniques (37). Ces différents traitements devront dès lors respecter les dispositions nationales relatives à la protection de la vie privée.
En France, par exemple, un employeur ne peut, sans violation de ces libertés fondamentales, prendre connaissance des messages personnels émis et reçus par ses salariés grâce à l'outil informatique mis à leur disposition pour leur travail, au risque de porter atteinte au droit au secret des correspondances (38). Cette

---

(27) Article 6-e) de la Directive 95/46/CE : « *les données à caractère personnel doivent être* (…) *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement* ». **(28)** Par exemple, en France, l'absence de déclaration d'un traitement est punie de 5 ans d'emprisonnement et de 300 000 euros d'amende (C. pén., art. 226-16). **(29)** En France, le fait de procéder à un transfert de données à caractère personnel vers un État n'appartenant pas à la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la CNIL est puni de 5 ans d'emprisonnement et de 300 000 euros d'amende (C. pén., art. 226-22-1). **(30)** Article 26-d) de la Directive 95/46/CE : « *Par dérogation à l'article 25 et sous réserve de dispositions contraires de leur droit national régissant des cas particuliers, les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquate au sens de l'article 25 paragraphe 2 peut être effectué, à condition que* (…) *le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice* ». **(31)** Voir l'Avis n° 12 du Groupe de l'Article 29 sur les transferts de données personnelles vers des pays tiers : Application des articles 25 et 26 de la directive relative à la protection des données, 24 juillet 1998. **(32)** Article 26-2 de la Directive 95/46/CE : « *Sans préjudice du paragraphe 1, un État membre peut autoriser un transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants ; ces garanties notamment résultent de clauses contractuelles appropriées* ». **(33)** Pour plus d'informations sur le *Safe Harbor,* voir : <http://www.export.gov/safeHarbor/>. **(34)** Documents appartenant à la société. **(35)** Article 8 de la Convention européenne de sauvegarde des droits fondamentaux ; Article 7 de la Charte européenne des droits fondamentaux. En Belgique : Constitution, art. 22 ; en France : C. civ., art. 9. **(36)** En France : C. pén., art. 226-15 ; en droit belge, les communications électroniques ne sont pas protégées par le secret de la correspondance (voir C. Trav. Liège, 23 mars 2004, R.R.D., 2004, liv. 110, p.73). **(37)** En Belgique, le secret des communications électroniques est protégé par l'article 124 de la loi relative aux communications électroniques du 13 juin 2005 et par l'article 314 bis du Code pénal. Alors que la doctrine et la jurisprudence semblent d'accord sur le fait que la protection accordée par l'article 314 *bis* du Code pénal s'arrête à la fin de la communication (c'est-à-dire concernant les e-mails, lorsque l'e-mail est présent sur le serveur de l'entreprise et a été lu par le destinataire ou aurait dû être lu par le destinataire : Corr. Louvain, 4 déc. 2007, T. Strafr. 2008, liv.3, 223, note Ceulemans L., *De Kennisname van e-mails « tijdens de overbrenging ervan, een verduidelijking van het telecommunicatiegeheim?* »), le champ d'application et la durée de la protection accordée par l'article 124 de la loi relative aux communications électroniques fait l'objet d'un débat. Nous penchons pour une interprétation de l'article 124 raisonnable et pragmatique, limitant le champ de cette disposition à la transmission de la communication (voir en ce sens, Docquir B., Le droit de la vie privée, pp. 81 et 82, n° 35 ; pour un avis contraire, voir Boulanger M.-H., La surveillance des communications électroniques des employés, Ubiquité, 2003/51, p. 54 ; Leduc P., Le contrôle des communications données ou reçues par l'employeur, Ubiquité, 2000/5, p. 42 ; Rijckaert O., Surveillance des travailleurs : nouveaux procédés, multiples contraintes, Orientations, L'employeur et la vie privée du travailler, n° spécial 35, 2005, 41 et ss.). **(38)** Cass. soc., 2 oct. 2001, *Nikon France c/ M. Frédéric Onof* : « *Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée* » ; voir aussi : Cass. soc., 12 oct. 2004, n° 02-40392.

interdiction ne s'applique qu'aux seuls e-mails qui sont identifiés par le salarié comme personnels (39). Il existe donc une présomption du caractère professionnel des échanges réalisés à partir du poste de travail fourni par l'entreprise. En pratique, une entreprise ne serait autorisée à communiquer que les e-mails non identifiés comme personnels, ce qui implique de mettre en place un processus fiable d'identification et de classification des e-mails selon leur nature personnelle ou professionnelle. Une communication généralisée de tous les e-mails d'un salarié serait donc contraire au principe de respect de la vie privée des salariés et pourrait engager la responsabilité civile et pénale de l'employeur.

Il n'est pas davantage permis à l'employeur d'accéder à l'intégralité du disque dur d'un salarié sans lui laisser l'opportunité de retirer ses fichiers personnels (40). Un employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels, contenus sur le disque dur de l'ordinateur, mis à sa disposition par l'entreprise qu'en présence de ce dernier, sauf s'il existe un risque ou événement particulier (41). *A contrario*, tous les fichiers non identifiés comme personnels sont présumés être de nature professionnelle de sorte que l'employeur peut y avoir accès librement (42). Dans le cadre d'une procédure *e-discovery*, une société française devra donc analyser tous les fichiers contenus sur le disque dur de l'employé et ne communiquer que ceux qui ne sont pas identifiés comme personnels.

En Belgique, l'employeur désirant accéder aux données électroniques stockées sur le disque dur d'un de ses salariés veillera à respecter les principes de proportionnalité et de transparence. Par conséquent, une information préalable doit être réalisée, sauf si des besoins impérieux pour la préservation des preuves l'impose ou si ce cas de figure a été prévu dans la politique d'utilisation des moyens informatiques. De plus, en application du principe de proportionnalité, l'employeur veillera à limiter l'accès à ce qui est strictement nécessaire, à poursuivre une finalité légitime et à restreindre l'accès aux données professionnelles (les données marquées privées ne pourront être copiées qu'en présence ou avec l'accord de l'employé).

E. – Le respect des règles de droit du travail

Le responsable du traitement devra également s'assurer qu'il a respecté les dispositions nationales en matière de droit du travail. En France, aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance (43). Ainsi, les salariés dont les données à caractère personnel sont communiquées aux États-Unis dans le cadre d'une procédure *e-discovery* doivent en être préalablement informés individuellement (règlement intérieur, notes de service, affichage) ou collectivement (représentants du personnel ou syndicats). De plus, le comité d'entreprise doit être informé et consulté pour les questions relatives à l'organisation, la gestion et la marche de l'entreprise (44), ou pour toute décision de mise en œuvre de moyens ou techniques permettant de contrôler l'activité des salariés (45). Enfin, l'employeur doit respecter le principe de proportionnalité qui interdit d'apporter des restrictions aux droits et libertés des salariés qui ne sont pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché (46).

Les salariés dont les données à caractère personnel sont communiquées aux États-Unis dans le cadre d'une procédure *e-discovery* doivent en être préalablement informés individuellement ou collectivement.

En Belgique, la convention collective de travail n° 81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électronique prévoit une procédure particulière pour la surveillance des systèmes informatiques et l'individualisation des données. Cette convention collective prévoit également une procédure d'information individuelle et collective relative aux possibilités de contrôle des moyens informatiques par l'entreprise. Cependant, les modalités d'accès et/ou d'utilisation des moyens de communication électronique au sein de l'entreprise reste de la prérogative de l'employeur et ne sont pas soumis au régime de la convention collective mentionnée ci-dessus (47).

F. – L'obstacle des lois nationales en matière d'entraide judiciaire internationale

Certains pays en Europe (la France, la Suisse par exemple) ont adopté des lois qui interdisent de communiquer des documents ou des informations à l'étranger (48) dans le cadre d'un litige transnational (49). En France, l'article 1 *bis* de la loi du 26 juillet 1968 (50) interdit « *à toute personne de demander, de rechercher ou de communiquer, par écrit, oralement ou sous toute autre forme, des documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci* ».

Toute personne qui est saisie d'une demande de communication de documents dans le cadre d'une procédure judiciaire ou administrative internationale doit en informer sans délai le ministère de la Justice (51). L'autorité judiciaire ou administrative étrangère à l'origine de la demande de documents doit se conformer aux dispositions de la Convention de La Haye du 18 mars 1970 (52) qui prévoit plusieurs mécanismes permettant d'introduire un acte d'instruction dans un autre État contractant (commission rogatoire, voie diplomatique, >

(39) Cass. soc., 30 mai 2007, n° 05-43102. **(40)** CA Versailles, 2 avr. 2003, *M. Pierre Delort c/ Salustro Reydel Management*. **(41)** Cass. soc., 17 mai 2005, *M. Philippe X c/ Sté Cathnet-Science*. **(42)** Cass. soc., 18 oct. 2006, *M. X c/ Sté Jalma emploi et protection sociale* ; Cass. soc., 18 oct. 2006, *M. X c/ Sté Techni-soft*. **(43)** C. trav., art. L. 1222-4 : « *Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance* ». **(44)** C. trav., art. 2323-6 : « *Le comité d'entreprise est informé et consulté sur les questions intéressant l'organisation, la gestion et la marché générale de l'entreprise et, notamment, sur les mesures de nature à affecter le volume ou la structure des effectifs, la durée du travail, les conditions d'emploi, de travail et de formation professionnelle* ». **(45)** C. trav., art. L. 2323-32, al. 3 : « *Le comité d'entreprise est 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* ». **(46)** C. trav., art. L.11121-1 : « *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* ». **(47)** Voir sur ce sujet, Van Eeckhoutte W., Neuprez V., Compendium Droit du travail contenant des annotations fiscales 06-07, Kluwer, Tome 1, n° 1305 ; Rijckaert O., précité. **(48)** Cette interdiction ne s'applique pas aux litiges qui se déroulent entre deux États membres de l'Union européenne (voir Règlement n° 1206/2001 du Conseil du 28 mai 2001 relatif à la coopération entre les juridictions des États membres dans le domaine de l'obtention de preuves en matière civile ou commerciale). **(49)** En anglais, une telle loi s'appelle « *blocking statute* ». **(50)** L. n° 68-678, 26 juill. 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères, modifiée par la loi n° 80-538 du 16 juillet 1980. **(51)** L. n° 68-678, 26 juill. 1968, art. 2, modifiée. **(52)** Convention sur l'obtention des preuves à l'étranger en matière civile ou commerciale, conclue, le 18 mars 1970, entrée en vigueur, le 7 octobre 1972. La France et les États-Unis ont ratifié cette convention mais pas la Belgique ; pour plus d'informations, voir <http://www.hcch.net>.

désignation d'un commissaire). Par conséquent, lorsque le ministère de la Justice est saisi d'une commission rogatoire qui lui est adressée par un État étranger, il transmet celle-ci au ministère public dans le ressort duquel celle-ci doit être exécutée (53). Le non-respect de ces dispositions légales peut aboutir à des sanctions pénales (54). En effet, dans une affaire récente (55), la Cour de cassation a confirmé la condamnation à 10 000 euros d'amende d'un avocat en France dont les démarches pour connaître les circonstances dans lesquelles le conseil d'administration de la société MAAF a pris la décision d'acquérir la société Executive Life, en l'absence de mandat délivré en application de la Convention de La Haye du 18 mars 1970, constituait un délit réprimé par l'article 3 de la loi du 26 juillet 1968.

III. – VERS UNE ÉBAUCHE DE SOLUTION AU CONFLIT

À l'instar des précédents conflits relatifs à la protection des données à caractère personnel (SWIFT, données PNR, etc.), la problématique de *e-discovery* ne semble pouvoir être résolue que par le biais de négociations entre les autorités américaines et européennes (56). Face à l'augmentation des demandes de *e-discovery* en Europe, le Groupe de l'Article 29 a annoncé qu'une analyse est en cours parmi les autorités européennes de protection des données à caractère personnel, et qu'un avis serait rendu en 2009 (57). Des négociations ont également lieu entre les représentants de la Commission européenne et le « *Department of Homeland Security* » aux États-Unis. Enfin, au niveau national, la CNIL a annoncé qu'elle avait attiré l'attention du gouvernement sur ce point et qu'une réflexion interministérielle devrait prochainement être engagée (58).

Aujourd'hui, faute de ligne directrice claire sur la manière de gérer une demande de *e-discovery* en Europe, la sécurité juridique des sociétés européennes est mise en péril. Par conséquent, les sociétés européennes sont invitées à adopter une démarche prudente avant d'entreprendre toute action.

À cette fin, un certain nombre de recommandations (59) peuvent être formulées.

1. Mettre en œuvre une procédure interne (ou intra-groupe) définissant les différentes étapes à suivre par les départements de l'entreprise concernés par une demande de *e-discovery*. La mise en œuvre d'une telle procédure doit s'accompagner d'une concertation préalable avec les instances représentatives du personnel et une information individuelle des salariés.
2. Vérifier que les formalités préalables (déclaration, demande d'autorisation, mécanisme légitimant les transferts de données, etc.) ont été réalisées pour les traitements de données à caractère personnel qui sont mis en œuvre au sein de l'entreprise et vérifier que ces déclarations autorisent le responsable du traitement à communiquer des données dans le cadre d'une procédure *e-discovery* (finalité légitime, durée de conservation déterminée, salariés informés, etc.).

> Faute de ligne directrice claire sur la manière de gérer une demande de *e-discovery* en Europe, la sécurité juridique des sociétés européennes est mise en péril.

3. Ne pas s'exécuter précipitamment et prendre le temps d'analyser la demande de *e-discovery* avec les principaux acteurs de l'entreprise (direction générale, service juridique, ressources humaines, correspondant informatique et libertés).
4. Délimiter le champ de l'enquête ou les personnes concernées par celle-ci afin de limiter le risque d'atteinte à la vie privée des salariés. Ceci peut se faire en distinguant les différentes opérations menées (accès, conservation, analyse des documents, transfert des données aux États-Unis, communication des données à un tiers, etc.) et en cherchant à restreindre chaque opération au département ou aux personnes concernés.
5. En cas de doute, concerter l'autorité nationale de protection des données à caractère personnel. Ces autorités sont généralement ouvertes à toute discussion et prêtes à trouver une solution négociée lorsque la procédure suivie par l'entreprise paraît « *prudente, diligente, et attentive aux enjeux liés à la protection des données* » (60).
6. Tenter de limiter le champ d'application d'une injonction américaine en présentant le conflit de droit à l'autorité judiciaire ou administrative ayant prononcé l'injonction. Certaines autorités américaines ont déjà été confrontées à ce genre de situation. Ainsi, par le passé, les autorités américaines ont échangé des courriers à propos des systèmes d'alerte interne (61) ou dans le cadre de l'affaire SWIFT (62). Certains juges ont également accepté de restreindre le champ d'application d'une injonction dans le cadre d'une procédure judiciaire.
7. Privilégier l'analyse et la recherche de preuves dans le pays d'origine des données. À ce titre, la société européenne doit s'assurer que l'enquête est réalisée conformément aux dispositions nationales du pays dans lequel le traitement est réalisé, en particulier les dispositions relatives à la protection des données à caractère personnel, au respect de la vie privée des salariés, au droit du travail, et à la procédure civile. Ainsi, il est de plus en plus fréquent que l'enquête soit menée sur le sol européen par un avocat américain en collaboration avec son correspondant européen.
8. Ne transférer aux États-Unis que ce qui est pertinent et strictement nécessaire au litige conformément aux dispositions légales sur les transferts de données. Le cas échéant, s'assurer que la communication de documents est réalisée conformément aux dispositions de la Convention de La Haye lorsque celle-ci a été ratifiée par le pays émetteur.

CONCLUSION

Le conflit de droit entre les règles de *e-discovery* et la protection des données à caractère personnel demeure un sujet complexe sur lequel il n'existe pas pour l'instant de réponse parfaite. En l'absence de solution globale, une approche « *sur mesure* », au cas par cas, doit être privilégiée. Pour ce faire, une concertation entre les différents acteurs (représentants de la société, magistrats, avocats) et une approche à la fois pédagogique et négociée avec les autorités européennes et américaines permettent dans bien des cas, sinon de résoudre le conflit, du moins de limiter le risque juridique. ◆

(53) CPC, art. 736. **(54)** L'article 3 de la loi n° 68-678 du 26 juillet 1968 modifiée prévoit six mois d'emprisonnement et 18 000 euros d'amende. **(55)** Cass. crim., 12 déc. 2007, n° 07-83228. **(56)** Indépendamment de toute décision politique, il est important de rappeler que les tribunaux américains restent indépendants au nom du principe de séparation des pouvoirs. **(57)** Voir communiqué de presse du Groupe de l'Article 29, <http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_10_12_08_en.pdf>. **(58)** Voir CNIL, Les entreprises inquiètes du développement des règles leur imposant la communication de données personnelles aux États-Unis, 15 janv. 2008, <www.cnil.fr>. **(59)** Ces recommandations sont énoncées à titre indicatif et n'ont pas vocation à être exhaustives. **(60)** Voir la décision de la Commission de la protection de la vie privée belge du 9 décembre 2008 relative à la société SWIFT : <http://www.privacycommission.be/fr/static/pdf/cbpl-documents/swift–projet-de-d-cision-modifications-09-12-200.pdf>. **(61)** Pour plus d'informations, voir <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006-others_en.htm>. **(62)** Pour plus d'informations, voir <http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:166:SOM:EN:HTML>.