Discovery & transfert de données

Le **Cabinet d'Avocats Mathias** publie ce Livre blanc afin de partager son expérience et son savoir-faire, avec les entreprises et administrations, toutes concernées par la protection des données à caractère personnel.

Les sujets choisis pour ce Livre blanc - *Discovery*, *computer forensics*, transferts internationaux de données - impactent en effet la protection du patrimoine informationnel. Des mesures doivent donc être mises en place au sein des structures et ce, de manière anticipée.

Nous sommes à votre disposition pour échanger à propos de ces mesures et vous accompagner dans leur mise en œuvre.

Nous vous souhaitons une bonne lecture.

Garance Mathias
Avocat à la Cour

Résumé

La protection des données est un enjeu majeur, pour l'ensemble des entreprises et des administrations.

Or, les données numériques ont une valeur commerciale mais aussi juridique. La procédure américaine de *Discovery,* consiste ainsi pour les parties à un procès à communiquer tous les éléments de preuves à leur disposition. Ces éléments contiennent bien souvent des données numériques.

L'objet de ce Livre blanc est de cerner les enjeux entourant le transfert de données dans le cadre de la procédure de *Discovery*. Le respect du droit à la vie privée des Européens ou du secret des affaires sont notamment concernés. Les entreprises tout comme les particuliers doivent en prendre conscience afin de mettre en œuvre les mesures nécessaires pour assurer la protection de leur patrimoine informationnel.

Abstract

Data protection clearly became a major issue over the past few years, as much for private individuals and public as for private corporations. This new digital and advanced technology era in which we are living from now on led to giving a considerable weight to digital data.

Thus, it is possible to stress out the fact that digital data now have a commercial value as well as a legal one, especially within the e-Discovery process.

The purpose of this Whitepaper is to get an overview of the issues surrounding the data transfer under the Discovery process. The rights to Privacy but also to trade secrets are particularly concerned. Therefore, private individuals and businesses must be aware of those issues in order to implement the needed measures to ensure a real protection of their resources.

Qu'est-ce que la *Discovery* ?

La *process Discovery* ou procédure de *Discovery* est une procédure propre aux pays de la Common Law et tout particulièrement aux États-Unis. Elle constitue la phase précontentieuse dans le cadre d'un procès civil ou commercial.

La procédure de *Discovery* est une obligation pour chacune des parties de livrer à la partie adverse tous les éléments de preuve dont elle dispose. Toute information est considérée pertinente pour la résolution du litige. Cela signifie que chaque partie se doit de divulguer toutes les informations, même les éléments de preuve qui lui sont défavorables.

Les finalités de ce procédé sont très simples :

- parvenir à réduire le temps du procès en délimitant notamment l'objet du litige ;
- réduire les coûts ;
- tenter de garantir une certaine égalité et une certaine justice entre les parties.

Cette phase d'investigation et d'instruction préalable est cruciale aux États-Unis et ce, d'autant plus que le refus de divulguer ces informations peut facilement entraîner un jugement défavorable. On notera alors que plusieurs types d'injonctions (notamment le « *subpoena* »[1]) pourront contraindre la partie adverse à fournir les éléments nécessaires à la bonne conduite de la procédure. Un refus de la part d'une partie de répondre à une question ou de produire des documents peut donner lieu à ce que l'on nomme « *motion to compel* ». Il s'agit de demander à la Cour d'ordonner à l'autre partie de s'exécuter.

Le cas de la *e-Discovery*

On parle de la *e-Discovery* lorsque la procédure est utilisée et se concentre tout particulièrement sur les éléments de preuves stockées sur des systèmes d'information. Ce sont par exemple des milliers de courriers électroniques de salariés d'une entreprise qui peuvent être concernés.

Bien souvent les courriels ont une valeur importante dans l'établissement de la preuve, que ce soit en matière civile ou pénale.

Cependant, de nombreuses personnes sont moins attentives au contenu de leurs échanges électroniques qu'à celui d'une correspondance manuscrite. Au-delà des simples courriels, la *e-Discovery* peut concerner un système d'information, voire même un réseau tout entier.

La nature des données électroniques est particulièrement intéressante dans le cadre d'un procès. Ces données peuvent en effet être recherchées beaucoup plus facilement que les informations se trouvant sur un format papier. Cela d'autant plus qu'il est plus complexe de détruire ces données sans laisser de traces.

[1] Injonction délivrée par le juge à un tiers afin qu'il témoigne ou communique un document.

L'intérêt de la *e-Discovery* réside donc dans le fait que toutes les données peuvent servir de preuve, que ce soit un simple texte, un fichier audio, des images ou un calendrier, voire les programmes informatiques.

Le *computer forensics*

A l'image de la médecine légale, une certaine informatique légale s'est développée dans le cadre de la *e-Discovery.*

Le *computer forensics* a été défini en 2002 comme « *la préservation, l'identification, l'extraction, la documentation et l'interprétation des données électroniques*[2] *».*

L'informatique légale est ainsi une technique d'enquête qui consiste à analyser et recueillir les preuves d'un matériel électronique afin de pouvoir les présenter par la suite au tribunal.

Les enquêteurs, dans le cadre de l'informatique légale, suivent une procédure particulière. Ils isolent tout d'abord l'appareil en question pour être sûr qu'il ne puisse plus être modifié. Ils opèrent ensuite une copie des disques durs du système concerné. L'instrument est alors conservé en sécurité et toutes les recherches seront effectuées sur la copie.

Toutes les preuves trouvées sont ensuite reportées dans un rapport d'enquête puis vérifiées sur le matériel original. Le *computer forensics* n'est donc pas négligeable dans le cadre de la préparation des procédures judiciaires dont fait partie la *Discovery.*

Une procédure américaine qui a des incidences en Europe

La *process Discovery,* bien qu'américaine, concerne également l'Europe et notamment la France.

La Commission Nationale de l'Informatique et des Libertés (CNIL) avait ainsi constaté en 2009 une augmentation croissante des demandes de communication des données personnelles d'entreprises françaises vers les États-Unis. Ces données sont transmises aux autorités judiciaires américaines dans le cadre de la procédure de *Discovery*[3].

C'est souvent le cas lorsqu'une multinationale a des liens étroits à la fois avec les États-Unis et

[2] Warren G. Kruse, Jay G. Heiser, 2002 Computer forensics: incident response essentials. IEEE Security & Privacy

[3] CNIL, www.cnil.fr, Délibération n° 2009-474 du 23 juillet 2009 portant recommandation en matière de transfert de données à caractère personnel dans le cadre de procédures judiciaires américaines dite de « *Discovery* »

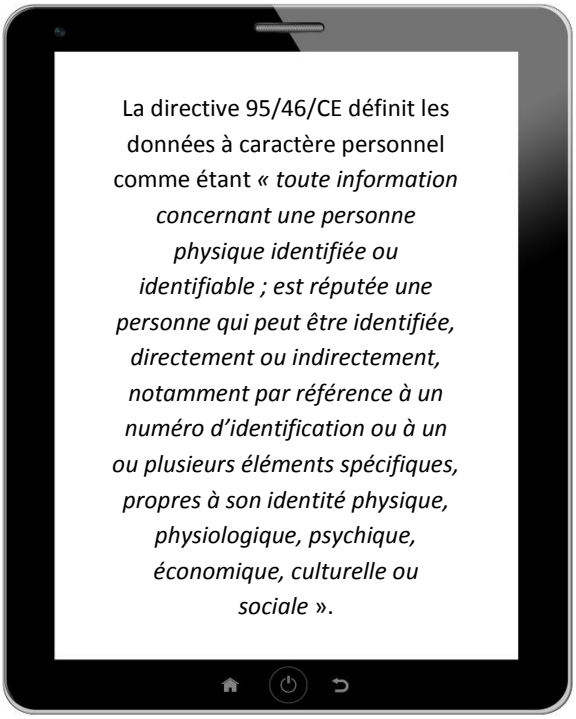
un État de l'Union européenne. Par exemple, lorsqu'une entreprise européenne a une filiale aux États-Unis ou qu'une entreprise dont le siège est aux États-Unis a besoin de données de ses filiales européennes dans le cadre d'un procès.

Un conflit entre le droit européen et le droit américain

Les obligations auxquelles sont soumises les multinationales françaises ou européennes dans le cadre de la procédure de *Discovery* sont en inadéquation avec les règles de protection des données personnelles mises en place par l'Union européenne. Cette opposition se retrouve tout particulièrement dans le cadre de la *e-Discovery*.

L'Union européenne a commencé à s'intéresser à ce sujet dès les années 1990, notamment avec l'adoption de la directive 95/46/CE. Cette directive constitue le socle de la protection des données personnelles au sein de l'Union européenne.

La directive a cependant été transposée d'une manière propre à chaque État membre et l'harmonisation totale sur cette question n'est donc pas encore réalisée. Certains États européens ont décidé d'appliquer un degré de protection des données personnelles plus important que le minimum imposé par la directive de 1995. C'est le cas de l'Allemagne et de la France par exemple.



Une proposition de Règlement européen en la matière est débattue. Ce Règlement devrait voir le jour en 2016 et permettrait notamment une réelle harmonisation des règles de transferts de données à caractère personnel vers un pays tiers à l'Union européenne.

L'Europe a une culture de la protection des données personnelles assez ancienne. L'Association Européenne des Droits de l'Homme (AEDH) rappelait ainsi en 2013 qu'il s'agissait d'un droit fondamental. C'est même un renforcement de cette protection[4] qu'elle réclame au niveau européen.

Il est par ailleurs possible de noter que cet intérêt pour la protection des données à caractère personnel se retrouve également à l'article 8 de la Charte des droits fondamentaux

[4] AEDH, communiqué de presse du 4 mars 2013, *L'AEDH réaffirme que la protection des données personnelles est un droit fondamental qui doit être renforcé.*

de l'Union européenne qui prévoit que « *toute personne a droit à la protection des données à caractère personnel la concernant* ».

Aux États-Unis, les données personnelles ne sont pas considérées de la même manière que dans l'Union européenne. Ainsi, des informations médicales ou les numéros de sécurité sociale par exemple sont considérées comme de simples données personnelles. Or, ces données sont traitées en Europe comme étant des données sensibles et bénéficient à ce titre, d'une protection spécifique.

On parle donc de données sensibles lorsque celles-ci incluent des informations hautement personnelles et qui révèlent la race de l'individu, l'ethnicité, l'opinion politique, la religion ou les croyances philosophiques, la santé physique ou mentale, la vie sexuelle, les sanctions civiles ou pénale, etc.

Les degrés de perception différents en ce qui concerne les données personnelles aux États-Unis et en Europe conduit donc à une incompréhension entre Américains et Européens sur la question de la protection de celles-ci.

La Convention de la Haye de 1970

La CNIL a rendu une délibération[5] sur la procédure de *Discovery* en juillet 2009. Ce document faisait suite à l'adoption d'un document de travail de février de la même année par le groupe européen des autorités de protection, aussi appelé le « G29 ». Ce fut alors l'occasion de rappeler le cadre juridique dans lequel s'inscrivent les demandes américaines en *Discovery*.

Trois textes ont alors été mis en avant : la Convention de la Haye du 18 mars 1970, la loi informatique et libertés de 1978 et la loi du 26 juillet 1968[6].

[5] Délibération n°2009-474 du 23 juillet 2009 portant recommandation en matière de transfert de données à caractère personnel dans le cadre de procédures judiciaires américaines dite de « Discovery ».

[6] Cité dans l'article L363-1 du code des assurances et l'article L511-25 du code monétaire et financier.

L'objectif de la Convention de la Haye est de gérer la communication des preuves entres les différents États parties. Une commission rogatoire est alors possible afin que l'autorité judiciaire d'un État demande toute instruction à l'autorité équivalente de l'autre État. On parlera alors de « *pre-trial discovery of documents* ».

Lorsque la France est concernée, il faudra alors qu'il existe un lien précis et direct avec l'objet du litige. En ce qui concerne les différents documents sollicités, ces derniers devront être limitativement énumérés.

Dans cette situation, il reviendra ensuite à la juridiction compétente de trancher sur la recevabilité des demandes d'obtention de preuves. L'article 743 du Code de procédure civile dispose ainsi que « *le juge commis peut refuser, d'office ou à la demande de toute personne intéressée, l'exécution d'une commission rogatoire s'il estime qu'elle ne rentre pas dans ses attributions. Il doit la refuser si elle est de nature à porter atteinte à la souveraineté ou à la sécurité de l'État français.*

Les personnes intéressées peuvent également, dans ces mêmes cas, demander au juge commis de rapporter les mesures qu'il a déjà prises et d'annuler les actes constatant l'exécution de la commission rogatoire ».

Le juge judiciaire devra ensuite se pencher sur la production des pièces détenues par une partie ou un tiers[7].

Si la procédure n'est pas respectée en France, les injonctions américaines concernant la transmission de preuves localisée en France seraient considérées comme irrecevables.

Une Convention bien souvent écartée par les Américains

L'article 23 de la Convention de la Haye de 1970 dispose que « *tout État contractant peut, au moment de la signature, de la ratification ou de l'adhésion, déclarer qu'il n'exécute pas les commissions rogatoires qui ont pour objet une procédure connue dans les États de Common Law sous le nom de « pre-trial Discovery of documents* ».

Les États-Unis ont clairement opté pour cette réserve et l'importance accordée à la Convention par la Cour suprême américaine est moindre. Cette dernière a ainsi fait savoir dès 1987[8] que le recours à la Convention de la Haye n'était qu'une simple option.

Par ailleurs, l'article 5 de ce texte met en avant le fait que « *Si l'Autorité centrale estime que les dispositions de la Convention n'ont pas été*

[7] Article 138 du Code de procédure civile.

[8] US Supreme Court, Affaire Société Nationale Industrielle Aérospatiale c.United States district Court for the Southern Disctrict of Iowa, 15 juin 1987.

respectées, elle en informe immédiatement l'autorité de l'État requérant qui lui a transmis la commission rogatoire, en précisant les griefs articulés à l'encontre de la demande ».

Les sanctions prévues par cet article 5 sont loin d'être dissuasives et il n'est donc pas étonnant que le juge américain n'ait aucun mal à écarter l'application de la Convention.

La non-application de cette Convention conduit donc à une prééminence de la procédure de *Discovery*. Or, la non-communication des preuves qu'elles soient matérielles ou immatérielles peut avoir un impact très négatif pour la partie qui s'y refuse (jugement défavorable, perte de marché du fait d'une interdiction de toute activité sur le territoire concerné, sanctions pécuniaires, etc.).

Les Américains s'imposent donc facilement et il n'est pas étonnant que l'Union européenne et ses États membres aient pris des mesures allant dans le sens de la protection des données personnelles et du secret des affaires.

Le secret des affaires : un enjeu important

La loi du 26 juillet 1968[9] interdit en substance, à toute personne physique et représentant d'une personne morale de communiquer, sous quelle que forme que ce soit, à des autorités publiques des documents d'ordre économique, commercial, industriel, financier ou technique. Il en va de même des communications tendant à la constitution de preuves dans la perspective de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci.

On l'aura compris, l'objectif premier de cette loi de blocage est de conduire à une certaine protection du secret des affaires. Néanmoins, on a pu le voir, la loi de blocage de 1968, malgré sa modification en 1980, a une application pour le moins limitée.

C'est donc dans ce cadre que l'Union européenne et la France ont choisi de se prononcer en faveur de nouvelles législations en matière de protection du secret des affaires.

Ainsi, un projet de directive européenne en date du 28 novembre 2013 sur la protection des savoir-faire et des informations commerciales non divulgués (secret d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, est actuellement en cours de discussion à Bruxelles.

Le 5 mai 2014, le Conseil de l'Union européenne a ainsi adopté l'approche générale de la directive.

Le 15 décembre 2015, les représentants du Parlement européen, du Conseil de l'Union européenne et de la Commission européenne sont parvenus à un accord sur le projet de directive « Secret des affaires » qui devrait être formellement adopté au printemps 2016. Avant toute publication au Journal Officiel, le Parlement européen doit en effet voter ce texte.

Le projet de directive vise à doter l'Union européenne d'une protection harmonisée des secrets d'affaires dans l'ensemble des Etats membres. Le secret des affaires est défini, pour l'instant, dans les termes suivants : « *une information secrète, qui a une valeur commerciale du fait de ce caractère secret, et qui a fait l'objet de dispositions raisonnables pour être gardée secrète par la personne la détenant* ».

La protection du secret des affaires est donc prise en considération tant par les institutions nationales qu'européennes. La protection de celui-ci sera possible notamment en passant

[9] Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères

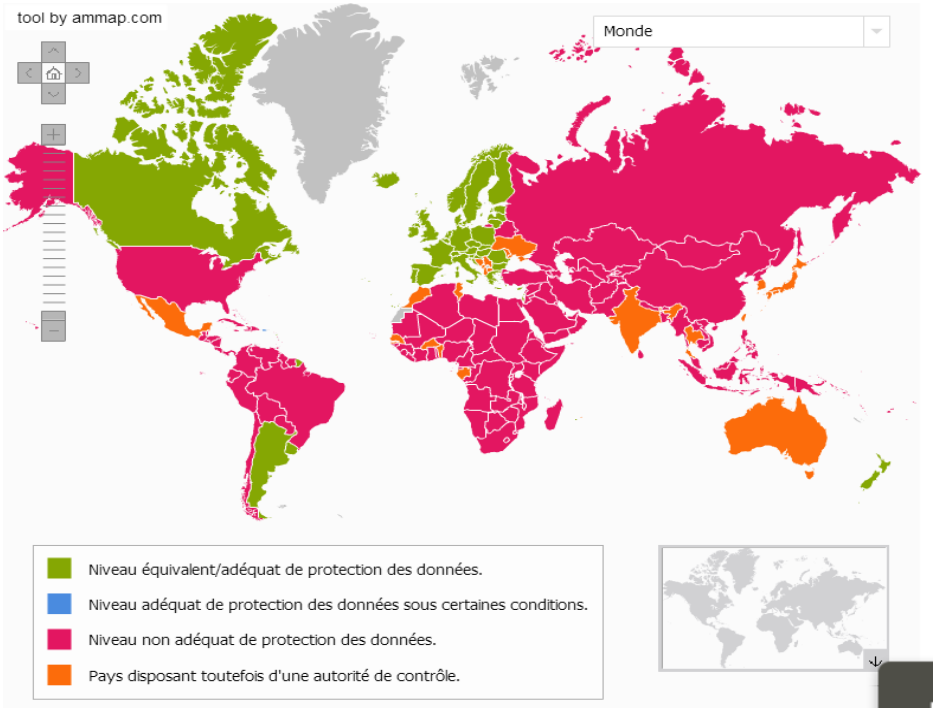
par un encadrement certain du transfert des données vers l'étranger.

L'interdiction du transfert des données hors UE comme principe

Les transferts de données personnelles en dehors de l'Union européenne sont interdits à moins qu'il y ait un niveau de protection dit adéquat. L'Islande, le Liechtenstein et la Norvège bien qu'ils ne soient pas membres de l'Union européenne ont tout de même transposé la directive de 1995 dans leur droit national si bien que cette interdiction de transfert ne s'appliquent pas à leur égard. Ils constituent avec les États membres de l'Union européenne, l'Espace économique européen (EEE).

En sus des membres de l'EEE, la Commission européenne a reconnu certains pays comme ayant une législation « *adéquate* » car suffisamment protectrice dans le cadre de transferts de données à caractère personnel. Comme le montre la carte (ci-dessous de la CNIL[10]), c'est le cas par exemple de la Nouvelle-Zélande, de l'Argentine, du Canada, d'Israël, de l'Uruguay, de la Suisse ou bien encore des îles Féroé.

A l'inverse, ce n'est pas le cas des États-Unis dont le niveau adéquat de protection des données n'est pas jugé suffisant.



[10] CNIL.fr, Carte des autorités de protection des données dans le monde, législations nationales en matière de protection des données personnelles, CNIL.fr

Le « *Safe Harbor program* »

Les États-Unis ne font pas partie des États considérés comme ayant des niveaux équivalents ou adéquats de protection des données. Il va donc de soi que la procédure de *Discovery* s'en voit directement affectée.

C'était d'ailleurs la raison de la mise en place du *Safe Harbor Program*. Celui-ci consistait en un ensemble de principes de protection des données personnelles auxquelles des entreprises américaines pouvaient adhérer de manière volontaire. Cela permettait ainsi de faciliter le transfert des données à caractère personnel en provenance des États membres de l'Union européenne. Ces principes étaient basés sur la directive 95/46/CE du 24 octobre 1995. Il s'agissait des principes suivants :

- l'information des personnes ;
- la possibilité accordée à la personne concernée de s'opposer à un transfert à des tiers ou à une utilisation des données pour des finalités différentes ;
- le consentement explicite des personnes pour le recueil de données sensibles ;
- le droit d'accès, de rectification ;
- la sécurité.

Il est possible de consulter la liste des entreprises qui y ont adhéré sur le site du département du commerce américain[11]. Cependant, le *Safe Harbor* ne concernait pas toutes les entreprises. Seules celles qui relèvent de la juridiction du département du commerce étaient concernées, ce qui excluait les sociétés financières et de télécommunication.

Le 6 octobre 2015, la Cour de Justice de l'Union Européenne a invalidé la décision[12] par laquelle la Commission européenne avait constaté que les Etats-Unis assurent un niveau de protection suffisant des données à caractère personnel des citoyens européens[13].

[11] US-EU Safe Harbor List, www.safeharbor.export.gov

[12] http://www.avocats-mathias.com/donnees-personnelles/invalidation-safe-harbor

[13] http://www.cnil.fr/linstitution/actualite/article/article/invalidation-du-safe-harbor-par-la-cour-de-justice-de-lunion-europeenne-une-decision-cl/

La Cour a rappelé que « *l'Union est une Union de droit dans laquelle tout acte de ses institutions est soumis au contrôle de la conformité avec, notamment, les traités, les principes généraux du droit ainsi que les droits fondamentaux (…). Les décisions de la Commission (…) ne sauraient donc échapper à un tel contrôle*. ». La Cour a également reconnu que « *le niveau de protection assuré par un pays tiers est susceptible d'évoluer.* ». Dès lors, « *il incombe à la Commission (…) de vérifier de manière périodique si la constatation relative au niveau de protection adéquat assuré par le pays tiers en cause est toujours justifié en fait et en droit.* ». Et la Cour d'ajouter qu'une « *telle vérification s'impose, en tout état de cause, lorsque des indices font naître un doute à cet égard*. »[14].

A la suite de cette décision, les transferts de données vers les Etats-Unis ne sont plus considérés comme réalisés vers un pays offrant une « *protection adéquate des données personnelles* ».

Les entreprises seraient ainsi dans l'obligation de procéder à des demandes d'autorisation auprès de la CNIL[15]. Toutefois, la demande risque d'être forte. Restent les clauses contractuelles types[16], ce qui impliquerait une renégociation des contrats en cours. Pour un même groupe, en cas de transfert de données entre les filiales, les Binding Corporate Rules[17] peuvent également être mises en œuvre.

Le Groupe de l'article 29 s'est réuni le 15 octobre 2015 afin de tirer les conséquences de l'arrêt rendu par la Cour de justice de l'Union européenne le 6 octobre dernier invalidant la décision de la Commission européenne instaurant la sphère de sécurité. Les institutions européennes et les autorités américaines étaient invitées à trouver des solutions avant la fin du mois de janvier 2016. A défaut, les autorités de protection pourraient procéder à des actions répressives coordonnées[18].

La Commission européenne a annoncé le 2 février 2016 avoir trouvé un accord avec les Etats-Unis afin d'encadrer les transferts de données personnelles outre-Atlantique, à savoir le « *Privacy Shield* » (en français,

[14] http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117fr.pdf

[15] http://www.cnil.fr/vos-obligations/declarer-a-la-cnil/mode-demploi/comment-declarer/la-demande-dautorisation/

[16] http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/contrats-types-de-la-commission-europeenne/

[17] http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/les-bcr/

[18] http://www.avocats-mathias.com/donnees-personnelles/safe-harbor-g29

« bouclier protecteur »)[19]. Cet accord a vocation à remplacer le « *Safe Harbor* ». Selon le communiqué de presse de la Commission européenne, le « *Privacy Shield* » reflèterait les exigences formulées par la Cour de Justice.

Trois catégories de garanties devraient figurer dans l'accord. D'abord, les entreprises américaines qui importent des données personnelles seront soumises à des obligations renforcées sur les modalités de traitement des données ainsi que sur les moyens mis en œuvre pour garantir les droits des personnes. Ce renforcement se matérialisera également par les contrôles effectués par le Département du commerce américain. Ensuite, l'accès aux données par les agences de renseignements américaines devrait être conditionné et contrôlé. Enfin, les citoyens européens devraient bénéficier de recours en cas de mauvaise utilisation de leurs données personnelles. Des délais de réponse aux plaintes seraient imposés aux entreprises. Les autorités de protection européennes pourraient par ailleurs collaborer avec le Département du commerce américain. Le recours aux modes alternatifs de règlement des litiges serait gratuit et un médiateur serait désigné.

L'accord ferait en outre l'objet d'une révision annuelle conjointe y compris sur les questions d'accès aux données par les autorités américaines pour les besoins de la sécurité nationale. Les autorités de protection

[19] http://europa.eu/rapid/press-release_IP-16-216_en.htm

européennes seraient associées à cette révision.

A noter que le « *Privacy Shield* » prendrait la forme d'un échange de lettres. Nous pouvons ainsi nous interroger sur son caractère contraignant. Nous nous interrogeons également sur l'effectivité des droits des ressortissants européens. Quand bien même des recours leur sont proposés, il est toujours délicat d'engager une action de l'autre côté de l'Atlantique lorsque l'on est simple particulier.

Le vice-président de la Commission européenne Andrus Ansip et la commissaire Věra Jourová en charge de la justice doivent préparer un projet de décision d'adéquation dans les semaines à venir. Le texte sera ensuite soumis au G29 pour avis ainsi qu'à un comité composé des représentants des Etats membres de l'Union européenne.

Le G29 demande à la Commission européenne que le *Privacy Shield* lui soit transmis d'ici à la fin du mois de février 2016[20]. Le G29 se prononcera également sur l'utilisation des clauses contractuelles types et des règles internes d'entreprises pour effectuer des transferts de données personnelles aux Etats-Unis. Pour l'heure, les entreprises peuvent continuer à utiliser ces instruments.

En dernier lieu, il n'est pas exclu que la CNIL préfère l'option de l'autorisation unique[21]. En effet, certains fichiers ou traitements de données personnelles sensibles ou à risques, qui visent une même finalité et des catégories de données et de destinataires identiques, sont autorisés par la CNIL au travers de décisions-cadre, appelées autorisations uniques. Si un traitement est conforme à l'une de ces autorisations, l'organisme peut effectuer un engagement de conformité.

Une France très protectrice

Au-delà des exceptions vues ci-dessus, il convient de préciser que le transfert de données personnelles vers les États-Unis a toujours été pour le moins assez « *conflictuel* », notamment car la protection des données à caractère personnel intéresse tout particulièrement la France. A l'instar de l'Allemagne ou de l'Italie, elle fait partie des États membres de l'Union européenne qui ont une législation en ce domaine qui va au-delà des exigences de la directive 95/46/CE.

[20] http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf

[21] http://www.cnil.fr/documentation/deliberations/autorisations-uniques/

La France n'a pas attendu la directive 95/46/CE qui impose la création d'une autorité administrative indépendante pour la protection des données. La Commission Nationale de l'Informatique et des Libertés a en effet été créée avec la loi n°78-17 relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978.

Cette même loi fait savoir que les données collectées - de manière générale et donc également dans le cadre de la *Discovery* - doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles le traitement est effectué.

La France a donc une certaine tradition de protection des données personnelles. La CNIL a ainsi déjà pu donner une opinion assez tranchée sur la question du transfert des données vers les États-Unis dans le cadre de la *process Discovery*.

L'autorité administrative donne ainsi des conseils pratiques pour aider à réduire les risques en vertu du droit français lorsqu'un responsable de traitement transfère des données vers les États-Unis.

Une recommandation de la Cnil sur la procédure de Discovery

La délibération n°2009-474 du 23 juillet 2009 portant recommandation en matière de transfert de données à caractère personnel dans le cadre de procédures judiciaires américaines dite de *Discovery* exprime la position de la CNIL dans ce domaine.

La CNIL rappelle que la Convention de la Haye de 1970 est la seule voie légale pour le transfert de telles données de la France vers les États-Unis : « *la Convention de la Haye est la seule convention internationale qui lie la France et les États-Unis et constitue un pont entre les systèmes juridiques romano-germaniques et ceux issus de la Common law* ».

La délibération souligne que la partie produisant les données à caractère personnelles doit procéder à un réel contrôle de proportionnalité afin de définir si le transfert de données envisagé est indispensable à la résolution du litige. Il faudra par ailleurs voir si une anonymisation des différentes données est possible et, le cas échéant, se limiter à la communication d'un nombre restreint d'informations.

Dans la plupart des cas, il est souligné que la personne concernée par le transfert de données doit donner son consentement libre et éclairé. A noter qu'un « *consentement est considéré comme étant donné librement lorsqu'il a été obtenu sans pression, ni risque de représailles sur la personne concernée* ». Cela n'est donc pas toujours aisé, notamment dans la situation où l'on se trouve en présence d'un

salarié d'une filiale et que le lien de subordination est important.

Par ailleurs, il conviendra de noter que les lois de blocages sont également mises en avant très régulièrement dans cette recommandation, tout comme la loi Informatique et Libertés.

Loi n°78-17 du 6 janvier 1978 modifiée

Article 68

Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à la Communauté européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.
Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées.

Article 69

Toutefois, le responsable d'un traitement peut transférer des données à caractère personnel vers un Etat ne répondant pas aux conditions prévues à l'article 68 si la personne à laquelle se rapportent les données a consenti expressément à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes :
1° A la sauvegarde de la vie de cette personne ;
2° A la sauvegarde de l'intérêt public ;
3° Au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;
4° A la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;
5° A l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ;
6° A la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers (…).

Loi de blocage

La France et certains de ses voisins ont mis en place des « *blocking statutes* » ou lois de blocage afin de se prémunir contre l'application abusive permettant la communication de documents dans le cadre de la *Discovery*.

En ce qui concerne l'Hexagone, la loi n°80-538 du 16 juillet 1980 relative à la communication de documents et renseignements d'ordre économique, commercial ou technique à des personnes physiques ou morales étrangères, et modifiant la loi n°68-678 du 26 juillet 1968 a permis de fixer le cadre des lois de blocages françaises.

Celles-ci sont restées bien longtemps lettre morte mais un arrêt de la Cour de cassation du 12 décembre 2007[22] a permis de remettre sur le devant de la scène cette législation. En l'espèce, un avocat français avait été sollicité par un avocat américain en vue d'obtenir des informations sur la manière dont les décisions étaient prises au sein du conseil d'administration d'une société française.

Il souhaitait les transmettre à son confrère américain afin de pouvoir les inclure dans le cadre d'une procédure pendante aux États-Unis. Il a alors été reconnu coupable de vouloir transmettre des informations d'ordre économique. Il ressort donc que tout ressortissant français ne respectant pas les procédures de coopération prévues par la Convention de la Haye de 1970 ou par les lois de blocage peut s'exposer à des sanctions. La condamnation en l'espèce s'élevait à 10 000€.

Loi n°80-538 du 16 juillet 1980 relative à la communication de documents et renseignements d'ordre économique, commercial ou techniques à des personnes physiques ou morales étrangères.

Article 2

I- L'article 1er de la loi Article 1er de la loi n°68-678 du 26 juillet 1968 susvisé est ainsi rédigé :

« Art.1er - Sous réserve des traités ou accords internationaux, il est interdit à toute personne physique de nationalité française ou résidant habituellement sur le territoire français et à tout dirigeant, représentant, agent ou préposé d'une personne morale y ayant son siège ou un établissement de communiquer par écrit, oralement ou sous tout autre forme, en quelque lieu que ce soit, à des autorités publiques étrangères, les documents ou les renseignements d'ordre économique, commercial, industriel, financier ou technique dont la communication est de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public, précisés par l'autorité administrative en tant que besoin »

II- Il est inséré, après l'article1er de la loi n°68-678 du 26 juillet 1968 susvisée, un article 1er bis ainsi rédigé

« Art.1er bis – Sous réserve des traités ou accords internationaux et des lois et règlements en vigueur, il est interdit à toute personne de demander, de recherche ou de communiquer par écrit, oralement ou sous tout 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. ».

[22] Cass. crim. ,12 décembre 2007, n°07-83.228

Il faut tout de même souligner ici que la Cour de cassation n'a pas fait de cette décision un arrêt de principe. Si cela avait été le cas et si la décision devait être confirmée, un impact clair sur la mise en œuvre de la procédure de *Discovery* par le juge aux États-Unis aurait lieu.

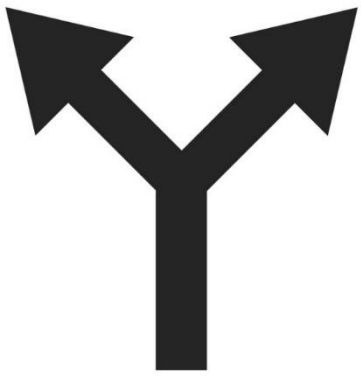
Il convient dès lors de s'intéresser aux deux situations possibles concernant cette question du transfert de données.

Deux situations à distinguer

Actuellement, et comme le précise la CNIL dans sa délibération de 2009, il faut se référer aux dispositions spécifiques de la loi du 6 janvier 1978 en matière de transfert de données à caractère personnel. Dans ce cadre et dans le cas des transferts vers les États-Unis, il faut distinguer deux situations : celle où les données en France sont transférées et celle où les données ont déjà été transférées.

- **Données personnelles en France directement transférées**

Dans cette situation, il faut également prendre en compte le type de transfert.



Ainsi, l'exception de l'article 69-3° (voir encadré p. 15) pourra justifier le transfert de données personnelles afin d'assurer « *la constatation et l'exercice ou la défense d'un droit en justice* ». A noter que la proposition de Règlement européen sur la protection des données à caractère personnel reprend également cette exception[23].

En revanche, s'il s'agit de transferts massifs et répétés, il est préférable que le transfert de données personnelles s'effectue :

- lorsque le destinataire des données personnelles a signé des clauses contractuelles types adoptées par la Commission européenne avec le responsable de traitement français ;

- lorsque le destinataire des données personnelles a mis en place des règles internes contraignantes au sein de son établissement (des « *Binding Corporate Rules* »).

- **Données personnelles déjà transférées vers un territoire n'offrant pas la protection adéquate, sans finalité légitime et sans autorisation préalable**

Dans ce cas et pour tout transfert ultérieur vers une autorité judiciaire, le responsable de traitement devra apporter une protection adéquate aux données communiquées par la mise en œuvre d'outils d'encadrement (la CNIL donne l'exemple de « *stipulative court order* », qui « *sont des ordonnances publiées par le juge américain garantissant que les pièces communiquées dans le cadre de la procédure de « Discovery »*

[23] Article 44 Derogations for specific situations, Proposition de Règlement en sa dernière version au mois de janvier 2016.

seront utilisées selon des conditions définies entre les parties et conservées de manière confidentielle. Elles peuvent limiter le périmètre des pièces à communiquer et peuvent être utilisées pour limiter la collecte de données personnelles en fonction du cas d'espèce, spécifier les conditions liées à l'utilisation et la communication à des tiers des données personnelles collectées et prévoir des mesures de sécurité et de confidentialité à respecter »[24]).

Pour tout transfert ultérieur vers une partie au procès ou vers des tiers, il faudra prévoir la conclusion de clauses contractuelles types avec la partie recevant les informations.

On notera par ailleurs que la CNIL insiste sur le fait que la personne concernée par le transfert de données personnelles doit en être informée de manière claire et doit pouvoir refuser la communication sur la base de motifs légitimes tel que le secret des affaires par exemple.

Un réel besoin d'affirmation européen face aux États-Unis

La facilité avec laquelle s'effectuent désormais les échanges est un avantage réel pour les entreprises et les administrations. Néanmoins, de réelles problématiques se posent, notamment en ce qui concerne la protection du patrimoine immatériel des entreprises. On a pu le voir, la protection du secret des affaires et la protection des données lors de transferts à l'étranger sont des enjeux majeurs, en particulier dans le cas de la *e-Discovery*.

Par ailleurs, les révélations liées à l'affaire Snowden ont eu de nombreuses répercussions. Outre la prise de conscience générale par la population européenne, l'affaire a conduit l'Union européenne à demander des garanties concernant la protection des données à caractère personnel des ressortissants européens. Néanmoins, un autre accord sur la question de la protection des données fait aussi l'objet de vives négociations entre l'Union européenne et les États-Unis : le *Data Protection Umbrella Agreement*. Ce traité devrait être davantage tourné vers la coopération policière et judiciaire.

La Commission européenne et les États-Unis ont affirmé être parvenus à définir un cadre garantissant un « *haut niveau* » de protection des données personnelles des citoyens européennes transférées outre-Atlantique et inversement en matière de coopération judiciaire (prévention, détection, recherche et poursuites judiciaires). Il ne s'agit

[24] Délibération n°2009-474 du 23 juillet 2009 portant recommandation en matière de transfert de données à caractère personnel dans le cadre de procédures judiciaires américaines dite de « *Discovery* ».

pas d'autoriser le transfert à proprement parler mais de renforcer la protection des individus.

Dès lors, l'entrée en vigueur de cet accord aura pour effet d'assurer aux citoyens européens que leurs droits relatifs à leurs données personnelles pourront être protégés par les juridictions américaines.

L'accord prévoit en effet que les citoyens européens puissent agir devant les juridictions américaines dans les deux hypothèses suivantes :

- l'atteinte portée par les autorités américaines à leurs droits d'accès ou de rectification;
- la divulgation illégale de leurs données personnelles.

Nous nous interrogeons toutefois sur la saisine par les ressortissants européens des autorités américaines puisque cela nécessite des moyens financiers importants. Engager une action judiciaire est déjà une démarche à laquelle on pense à deux fois plutôt qu'une. Lorsqu'il s'agit de le faire outre-Atlantique, cela paraît encore plus compliqué pour les citoyens.

Plusieurs garanties sont consacrées par l'accord afin que les données personnelles des citoyens européens soient protégées, dont la plupart existent déjà dans le cadre européen de protection.

A noter que la loi américaine devra être modifiée pour intégrer les droits reconnus aux citoyens européens avant que le texte soit adopté par le Parlement européen et le Conseil de l'Union européenne. Plusieurs étapes

seront donc encore nécessaires avant l'entrée en vigueur de l'Umbrella Agreement.
L'importance des données, que ce soit au niveau de leur conservation ou de leur transfert est désormais telle que les Européens n'ont d'autres choix que de mettre en place des mesures de protection suffisantes en ce qui concerne les données de leurs ressortissants.

Cette mise en avant de la protection des données sera-t-elle constitutive d'une réelle attractivité pour les entreprises internationales ?

Les bonnes pratiques

Pour ne pas faire d'erreur et faire en sorte que l'entreprise ou l'administration soit prête en cas de demande de transfert de données dans le cadre de la *process Discovery*, de bonnes pratiques doivent être mises en place.

- **La mise en place d'une politique pour répondre à la *Discovery***

L'internationalisation des échanges et des affaires conduit à ce que la procédure de *Discovery* a un réel impact en dehors des frontières des États-Unis d'Amérique. Une véritable politique de prévention doit être mise en place, ne serait-ce qu'avec la définition d'un calendrier de conservation et de suppression de certaines données.

Être accompagné par un avocat, spécialisé sur les questions relatives à la protection des données s'avère donc important pour l'organisme souhaitant être en parfaite conformité avec les dispositions relatives au transfert de données à caractère personnel. De même, un avocat spécialisé permettra à l'entreprise de définir les bonnes pratiques, les règles à inclure dans la Charte informatique ainsi que de préparer le personnel aux mesures à prendre si la société se voit concernée par une telle procédure.

- **La participation des employés**

Il est primordial de faire participer pleinement les employés dans le cadre de la *Discovery*. De cette manière, une certaine responsabilisation est opérée, d'autant plus que pour appréhender la *Discovery* de manière effective, il est nécessaire que les politiques, les bonnes pratiques, les procédures et les différentes technologies de la société soient connues de tous. Chacun, au sein de l'entreprise ou de l'administration doit donc être formé à la conservation des informations importantes dans le cadre de la politique définie par l'organisme.

- **La coordination des services informatiques et juridiques**

Si l'entreprise ou l'administration doit faire face à une demande de transfert de données à caractère personnel dans le cadre de la procédure de *Discovery*, la bonne coordination

entre les services informatiques et juridiques doit être effective.

Pour ce faire, une véritable coordination entre les deux services doit être instaurée. Par ailleurs, les juristes se doivent d'être parfaitement formés quant aux problématiques susceptibles d'être soulevées par une telle procédure. À titre d'exemple, ils devront savoir qui (dans le service informatique) est en charge des questions d'archivage et quelle est la procédure à suivre au niveau des déclarations et des autorisations de la CNIL.

- **Prévenir les éventuels contentieux**

Avoir conscience du risque potentiel de contentieux permet à l'entreprise d'identifier toutes les données pouvant être importantes lors d'une procédure de *Discovery*.

Par ailleurs, la position française sur cette procédure conduit à formuler l'exigence d'un réel encadrement quant à la communication des documents. Nous l'avons déjà précisé, toute information est potentiellement saisissable et une réelle protection des données doit être mise en place. Et ce, tant au niveau technique que juridique.