Commission nationale de l'informatique et des libertés (Cnil)

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

JORF n°0190 du 19 août 2009 - Texte n°27
NOR: CNIA0900018X

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la 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 ;

Vu l'article 23 de la convention de La Haye du 18 mars 1970 ;

Vu l'article 1er bis de la loi n° 68-678 du 27 juillet 1968, créé par la loi n° 80-538 du 16 juillet 1980 relative à la communication de documents ou renseignements d'ordre économique, commercial ou technique à des personnes physiques ou morales étrangères ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu la délibération de la Commission nationale de l'informatique et des libertés n° 2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel ;

Vu l'avis WP 158 du groupe de travail dit de l'« article 29 » adopté le 11 février 2009 ;
Après avoir entendu MM. Bernard PEYRAT, Georges de LA LOYÈRE, en leur rapport, et Mme Elisabeth ROLIN, commissaire du Gouvernement, en ses observations,

La Commission nationale de l'informatique et des libertés constate un accroissement des dossiers concernant des transferts de données personnelles vers les Etats-Unis, déposées principalement soit par des filiales françaises de sociétés américaines soit par des sociétés françaises ayant des liens commerciaux avec les Etats-Unis, en raison de procédures de « ***Discovery*** » devant des juridictions américaines.

Pour rappel, la procédure dite de « ***Discovery*** » ou de « ***pre-trial Discovery*** » est une phase d'investigation et d'instruction préalable au procès civil ou commercial, essentielle pour toute action en justice aux Etats-Unis, faisant obligation à chaque partie de divulguer à l'autre tous les éléments de preuve pertinents au litige dont elle dispose, même si elles lui sont contraires, quelles

que soient leur localisation et leur forme. Sont ainsi exclues, les communications d'informations dans le cadre d'affaires pénales.

Le périmètre de ces échanges d'informations peut être très large et le refus de communication peut aboutir à un jugement défavorable à la partie s'opposant à cette communication.

La convention de La Haye organise la communication entre Etats contractants de preuves situées à l'étranger dans le cadre de procédures judiciaires nationales. Cette convention prévoit qu'« *en matière civile ou commerciale, l'autorité judiciaire d'un Etat contractant peut, conformément aux dispositions de sa législation, demander par commission rogatoire à l'autorité compétente d'un autre Etat contractant de faire tout acte d'instruction, ainsi que d'autres actes judiciaires (...)* » (art. 1er).

La convention de La Haye est la seule convention internationale qui lie la France et les Etats-Unis et constitue un pont entre les systèmes juridiques romano-germaniques et ceux issus de la common law.

Plus particulièrement concernant les relations avec les Etats-Unis, il est prévu que « *tout Etat 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 Etats de common law sous le nom de " pre-trial Discovery documents "* » (art. 23).

En France, l'exécution des commissions rogatoires en cas de « ***pre-trial Discovery of documents*** » n'est autorisée que « *si les documents sont limitativement énumérés dans la commission rogatoire et ont un lien direct et précis avec l'objet du litige* » (déclaration faite par la France le 19 janvier 1987 dans le cadre de l'article 23 précité).

Dans cette hypothèse, la juridiction à laquelle la commission rogatoire a été transmise doit trancher sur la recevabilité des demandes d'obtention de preuve, conformément aux dispositions des articles 743 et suivants du code de procédure civile.

Il revient alors au juge judiciaire de statuer, conformément aux articles 138 et suivants du nouveau code de procédure civile, sur la production des pièces (y compris les documents dématérialisés) détenues par un tiers ou par une partie en ordonnant la production de l'acte ou de la pièce « *dans les conditions et sous les garanties qu'il fixe, au besoin à peine d'astreinte* » (1).

La plupart des pays ayant ratifié la convention de La Haye ont émis eux aussi des réserves ou ont refusé la communication d'informations dans le cadre de « ***pre-trial Discovery*** » (art. 23).
En l'absence de respect de cette procédure en France, les injonctions émises par les autorités américaines concernant des preuves localisées en France sont donc irrégulières.

En effet, le non-respect de la convention de La Haye entraîne, en France, l'application de la loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et de renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.

La loi du 26 juillet 1968 est une loi « ***bouclier*** » adoptée pour la défense des intérêts économiques français, pour la protection des données stratégiques des entreprises, contre les actions abusives engagées par les autorités étrangères pour collecter des informations économiques.
Celle-ci prévoit que, « *sous réserve des traités ou accords internationaux et des lois et règlements en vigueur, il est 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* ».

Le non-respect de cette disposition est sanctionné par une peine d'emprisonnement de 6 mois et / ou par une amende de 18 000 €.

Comme la communication de données personnelles dans le cadre d'un procès à l'étranger peut engendrer la mise en cause de la personne concernée devant une juridiction étrangère, il est essentiel de s'assurer que l'ensemble des règles juridiques applicables à ce type de situation, et notamment les règles de conflit de lois de droit international privé, sont respectées afin de protéger au mieux le citoyen français et de lui garantir un procès équitable.

A ce titre, la convention de La Haye et la loi n° 68-678 du 26 juillet 1968 relative à la communication de documents ou renseignements d'ordre économique, commercial ou technique à des personnes physiques ou morales étrangères réglementant la communication d'informations à des autorités étrangères doivent être respectées en cas de recherche d'informations sur le territoire français. Toute communication d'information dans le cadre d'une procédure de « ***Discovery*** » doit se faire conformément à la convention de La Haye.

Au demeurant, la CNIL n'a pas compétence pour apprécier la conformité d'un transfert « ***Discovery*** » au regard de la convention de La Haye ou de la loi de 1968, dite « loi de blocage ».

De la même façon, l'obtention d'une autorisation du juge français à l'envoi de documents aux Etats-Unis (procédure de la « ***letter of request*** » adressée à la chancellerie) ne dégage pas l'entité française de l'obligation de respecter les dispositions de la loi informatique et libertés, notamment s'agissant de la question du flux de données personnelles hors de l'Union européenne, les deux réglementations étant complémentaires. Rappelons qu'en France, les sanctions pénales qui s'attachent au non-respect des principes de la loi du 6 janvier 1978 modifiée sont significativement plus lourdes que celles prévues en cas de non-respect de la loi de blocage de 1968.

Les communications de données personnelles dans le cadre des procédures de « ***Discovery*** » nécessairement effectuées dans le cadre de la convention de La Haye doivent également être en conformité avec les principes de la loi du 6 janvier 1978 modifiée. Cependant, ces demandes éventuelles de communication de données personnelles ne doivent pas conduire à la création de bases de données destinées à répondre spécifiquement à ces procédures américaines. En effet, elles doivent être abordées comme des fonctionnalités de finalités principales telles que la gestion des ressources humaines ou les fichiers clients-prospects.

La loi du 6 janvier 1978 modifiée s'applique aux procédures de « ***Discovery*** » dès lors qu'elles impliquent des transferts de données personnelles ; cependant, il ne convient pas de procéder à des déclarations spécifiques « ***Discovery*** » dans la mesure où ces données ont dû précédemment faire l'objet de déclarations pour leurs finalités principales dans laquelle il est fait état d'une durée de conservation par types de données collectées et traitées. Enfin, les applications techniques visant à sélectionner les données dans le cadre des procédures de « ***Discovery*** » n'ont pas vocation à faire l'objet de déclarations.

Néanmoins, les flux internationaux de données doivent, quant à eux, faire l'objet de déclarations à la CNIL, qui pourra les requalifier en demandes d'autorisation en fonction de l'encadrement juridique entourant ces transferts.

Enfin, la Commission rappelle l'intérêt pour les entreprises de désigner des « ***correspondants informatique et libertés*** », pour aider à résoudre ce type de problématiques.

La présente recommandation ne traite pas des cas liés aux enquêtes menées par les autorités fédérales américaines, telles que la ***Security Exchange Commission (SEC)*** ou la ***Federal Trade Commission (FTC)*** ; en outre, elle ne prend pas en compte les problématiques liées aux sanctions des autorités américaines relatives à la destruction prématurée de données.

1. Responsabilité du traitement

Conformément à l'article 5 de la loi Informatique et libertés, le responsable de traitement est la personne morale ou la personne physique qui décide de la communication de données personnelles dans le cadre d'une procédure judiciaire américaine et, par là même, de la finalité et des moyens du traitement.

Le responsable de traitement peut être l'entité française ou étrangère établie sur le territoire français ou l'entité étrangère utilisant des moyens de traitements sur le sol français selon l'article 5 de la loi Informatique et libertés.

2. Légitimité du traitement et des finalités

Sur la légitimité du traitement :

Au-delà du respect de la convention de La Haye et de la loi de 1968, la CNIL considère que l'intérêt légitime du responsable de traitement est un motif permettant le traitement de données à caractère personnel dès lors qu'est garanti le respect des droits des personnes.

En effet, conformément à l'article 7-5 de la loi Informatique et libertés, la communication des données personnelles dans l'intérêt légitime du responsable de traitement ne peut être réalisée que si l'intérêt ou les droits et libertés fondamentaux de la personne concernée sont assurés.
Ainsi, le respect des conventions internationales et des dispositions nationales applicables, telles que la convention de La Haye et la loi du 26 juillet 1968, est nécessaire afin de protéger les droits fondamentaux de la personne concernée.

Par ailleurs, conformément à l'article 38 de la loi Informatique et libertés, la personne concernée bénéficiera en toutes circonstances d'un droit d'opposition sur la base de motifs légitimes concernant la communication de ses données personnelles dans le cadre d'une procédure judiciaire aux Etats-Unis.

Dans des cas exceptionnels, la commission reconnaît qu'il peut y avoir des situations où la personne a la possibilité de donner un consentement libre, éclairé et spécifique, et est même impliquée dans la procédure contentieuse. Son consentement peut alors constituer une base légale au sens de l'article 7 de la loi Informatique et libertés. Cependant, la preuve de ce consentement libre, éclairé et spécifique doit être apportée. Un consentement est considéré comme étant donné librement lorsqu'il a été obtenu sans pression, ni risque de représailles sur la personne concernée.

Sur le traitement de données sensibles :

Selon l'article 8 de la loi Informatique et libertés, le traitement de données sensibles est en principe interdit et ne doit être réalisé que si la personne concernée a donné son consentement exprès ou s'il est nécessaire à la constatation, la sauvegarde ou la défense d'un droit en justice pour le responsable de traitement. Des mesures particulières, notamment de sécurité, doivent être mises en place afin de protéger de manière adéquate ces informations.

S'agissant du consentement au traitement de données sensibles, la preuve d'un consentement libre, spécifique et éclairé doit pouvoir être apportée.

3. Qualité et proportionnalité des données

Conformément à l'article 6 de la loi Informatique et libertés, les données collectées dans le cadre d'une procédure dite de « ***Discovery*** » doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles le traitement est mis en œuvre.

Une vérification sérieuse concernant la proportionnalité et la qualité des données collectées et communiquées est fondamentale et doit être effectuée de manière objective afin de garantir que seuls les éléments légalement autorisés sont communiqués à la partie adverse et au juge étranger dans le cadre du procès. Ceci peut se faire par la mise en place d'un filtre dont les mots-clés sont définis en collaboration avec le service juridique et des conseils spécialisés. Cette opération de filtrage doit avoir lieu au niveau local, c'est-à-dire dans le pays où se trouvent les données personnelles.

Cette balance d'intérêts doit prendre en compte les problématiques de proportionnalité, la pertinence des données dans le cadre du procès, et les conséquences pour les personnes concernées.

La communication ne peut intervenir que dans le respect des obligations légales de secret et de confidentialité telles que le secret professionnel et la loi du 26 juillet 1968.

La CNIL recommande également le recours à un tiers de confiance dans l'appréciation de la proportionnalité des données traitées dans le cadre de la procédure.

Enfin, dans de nombreux cas, la communication d'informations ne nécessite pas la communication de données personnelles. A cet effet, l'équipe en charge de la recherche et de la communication d'informations devra alors mettre en œuvre des procédures d'anonymisation et de pseudonymisation (permettant la réidentification par la suite) des informations pour éviter la communication de données personnelles inutiles ou accessoires au procès.

Si la communication de données est limitée, la démarche visant à anonymiser les données ne sera pas nécessaire. En revanche, s'il s'agit d'un flux important de données, l'opération d'anonymisation devra être envisagée.

Il est ainsi apparu, au cours des auditions, qu'une autorité américaine (en l'espèce, la Security Exchange Commission) avait demandé à une société française la communication d'un nombre très important de données personnelles. Après discussion avec la SEC, il s'est avéré que cette dernière n'avait pas besoin de données personnelles ; la société française a donc pu adresser des données anonymisées.

Si, toutefois, des données personnelles sont nécessaires, les catégories de données pouvant être communiquées doivent se limiter à :
— identité, fonctions, coordonnées de la personne concernée ;
— éléments strictement relatifs au contentieux en cours.
Par ailleurs, les données doivent être exactes et complètes.

La procédure américaine intègre le principe de proportionnalité. En effet, lorsque le juge américain émet des « ***stipulative court orders*** », il le fait en appréciant la qualité des données nécessaires dans le cadre du procès en question.

Les « ***stipulative court orders*** » sont des ordonnances publiées par le juge américain garantissant que les pièces communiquées dans le cadre de la procédure de « ***Discovery*** » 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.

4. Durée de conservation

Conformément à l'article 6 de la loi Informatique et libertés, les données relatives à la personne concernée ne peuvent être conservées que pour une durée pertinente au regard de la finalité du traitement qui a justifié cette procédure.

Ainsi, les données utilisées dans le cadre d'une procédure de « ***Discovery*** » sont conservées pour la durée de la procédure. Il est donc recommandé de ne pas créer une nouvelle durée de prescription.

5. Destinataires des données

Conformément aux articles 6 et 34 de la loi Informatique et Libertés, les personnes spécialement chargées, par le responsable de traitement et au sein de la partie adverse, du recueil ou du traitement des données personnelles dans le cadre de procédure « ***Discovery*** » ne sont destinataires de tout ou partie des données visées ci-dessus que dans la mesure où ces données sont nécessaires à l'accomplissement de leurs missions et à la finalité du traitement.

6. Information des personnes concernées

Une information générale, claire et complète de toute personne potentiellement concernée doit être réalisée préalablement à la mise en place du traitement de données pouvant faire l'objet d'un transfert de leurs données personnelles à l'étranger dans le cadre de procédures judiciaires. En outre, une information spécifique doit être faite au moment du transfert de données hors de l'Union européenne.

Par conséquent, la personne qui fait l'objet d'une recherche est, conformément aux articles 6 et 32 de loi du 6 janvier 1978, informée par le responsable du traitement dès l'enregistrement, informatisé ou non, de données la concernant afin de lui permettre de s'opposer pour des motifs légitimes au traitement de ses données.

Cette information, qui est réalisée selon des modalités permettant de s'assurer de sa bonne délivrance à la personne concernée, précise notamment l'entité responsable du traitement, les faits du procès et le lien existant nécessitant la communication de ses données personnelles, le caractère facultatif ou non du traitement, les conséquences pour la personne concernée en cas de refus de communication, les services éventuellement chargés de la recherche, les éventuels transferts de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne ainsi que les modalités d'exercice de ses droits d'accès, d'opposition et de rectification.

Sauf cas exceptionnels prévus à l'article 32-III de la loi Informatique et libertés, les personnes doivent également être informées lorsque les données sont collectées par un tiers et indirectement. Dans cette hypothèse, les personnes concernées doivent être informées par le responsable de traitement aussi vite que les circonstances le permettent après le traitement des données.

Une exception au principe de transparence doit cependant être prise en compte dans des cas exceptionnels. En effet, lorsqu'il existe un risque que l'information de la personne concernée mette en danger la possibilité pour la partie au procès de mener une enquête ou de rassembler des preuves, l'information à la personne concernée ne peut être effectuée qu'une fois ce risque écarté.

Ainsi, lorsque des mesures conservatoires sont nécessaires, notamment pour prévenir la destruction de preuves, l'information de cette personne intervient après l'adoption de ces mesures.

7. Respect des droits d'accès et de rectification

Conformément aux articles 39 et 40 de la loi du 6 janvier 1978 modifiée, le responsable du traitement garantit à toute personne concernée le droit d'accéder aux données la concernant et d'en demander, si elles sont inexactes, incomplètes, équivoques ou périmées, la rectification ou la suppression. Cependant, il pourrait être demandé à un juge, y compris en référés, l'interdiction de communiquer et/ou de détruire ces informations afin de préserver la confidentialité d'une enquête.

8. Mesures de sécurité

Conformément aux articles 34 et 35 de la loi Informatique et libertés, l'accès aux données personnelles doit être limité aux seules personnes qui, dans le cadre de leur fonction, peuvent légitimement en avoir connaissance au regard de la finalité du traitement.

Le responsable du traitement doit dès lors prendre toutes précautions utiles pour préserver la sécurité de ces données.

A ce titre, et conformément à la recommandation n° 2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel, la CNIL recommande :

— s'agissant des archives intermédiaires (données qui présentent encore un intérêt administratif pour les services concernés), l'accès à celles-ci doit être limité à un service spécifique (par exemple un service du contentieux) et il doit être procédé, a minima, à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations) ;
— s'agissant des archives définitives (exclusivement les données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction), celles-ci doivent être conservées sur un support indépendant, non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à consulter ce type d'archives (par exemple la direction des archives de l'entreprise).

En outre, la CNIL recommande, afin de garantir l'intégrité des données archivées, de mettre en œuvre des dispositifs sécurisés lors de tout changement de support de stockage des données archivées.

Enfin, elle recommande de mettre en œuvre des dispositifs de traçabilité des consultations des données archivées.

En cas de recours à un prestataire de service, pour gérer tout ou partie de ce dispositif, le responsable de traitement doit imposer, par voie contractuelle, au prestataire de ne pas utiliser les données pour des fins détournées, de s'assurer de leur confidentialité, de respecter la durée de conservation limitée des données et de procéder à la destruction ou à la restitution de tous les supports manuels ou informatisés de données à caractère personnel au terme de sa prestation.

Dans tous les cas, les personnes chargées du recueil et du traitement des données sont en nombre limité, spécialement formées et astreintes à une obligation renforcée de confidentialité contractuellement définie.

9. Formalités relatives aux transferts de données à caractère personnel vers les Etats-Unis

Les transferts de données à caractère personnel doivent s'opérer conformément aux dispositions spécifiques de la loi du 6 janvier 1978 modifiée relatives aux transferts internationaux de données, et notamment ses articles 68 et 69. Sur ce point, il convient de rappeler que les Etats-Unis ne disposent pas d'un niveau de protection adéquat en matière de protection des données à caractère personnel, au sens de la directive européenne du 24 octobre 1995.

Deux cas doivent être distingués :

1. L'hypothèse où les données personnelles sont en France et directement transférées aux Etats-Unis pour des finalités contentieuses :

S'agissant d'un transfert unique et non-massif d'informations pertinentes, l'exception de l'article 69-3° peut être utilisée pour justifier le transfert de données personnelles à des fins de constatation, sauvegarde ou défense d'un droit en justice pour le responsable de traitement. Dès lors que ce transfert est encadré par l'exception visée à l'article précédemment visé, il ne doit pas faire l'objet d'une autorisation de la CNIL, mais doit néanmoins être déclaré.

Lorsqu'il s'agit de transferts massifs et répétés, le transfert de données personnelles peut avoir lieu:

— lorsque le destinataire des données personnelles est une entité établie aux Etats-Unis et qui a auto-adhéré aux principes du ***Safe Harbor*** ;
— lorsque le destinataire des données personnelles a signé des clauses contractuelles types adoptées par la Commission européenne avec le responsable de traitement en France ;
— lorsque le destinataire des données personnelles a mis en place des règles internes contraignantes (ou « ***Binding Corporate Rules*** ») au sein de son groupe.

2. L'hypothèse où les données personnelles ont déjà été transférées sur le territoire américain ou sur un territoire n'offrant pas de protection adéquate pour une finalité légitime et préalablement autorisée (ex. : centralisation de la base de données des ressources humaines de la filiale française d'un groupe américain) :

Lorsque les données font l'objet d'un transfert ultérieur vers une autorité judiciaire, le responsable de traitement devra apporter une protection adéquate aux données communiquées aux autorités américaines et à la partie adverse par la mise en œuvre d'outils d'encadrement appropriés tels que la définition d'un « ***stipulative court order*** » prenant en compte la protection des données personnelles.

Lorsque les données font l'objet d'un transfert ultérieur vers une partie au procès ou vers des tiers, il conviendra alors de prévoir la conclusion de clauses contractuelles appropriées avec la partie recevant communication des informations, ou le cas échéant l'engagement de la partie de respecter les principes portant sur les transferts ultérieurs tels que prévus dans l'accord ***Safe Harbor***.

En effet, le programme ***Safe Harbor*** prévoit que pour divulguer des informations à un tiers dans le cadre d'un transfert ultérieur, les sociétés sont tenues d'appliquer les principes de notification et de choix. Les organisations qui le souhaitent peuvent transférer des informations à un tiers agissant en qualité de mandataire si elles certifient auparavant que le tiers souscrit aux principes du ***Safe Harbor*** ou est soumis aux dispositions de la directive ou d'un autre mécanisme attestant le niveau adéquat de la protection ou encore si elle passe un accord écrit avec ce tiers dans lequel celui-ci s'engage à assurer au moins le même niveau de protection que les principes.

Conformément aux dispositions des clauses contractuelles types adoptées par la Commission européenne et aux principes du ***Safe Harbor***, il est impératif qu'un travail exhaustif soit opéré par le responsable de traitement situé à l'étranger concernant la pertinence, la légitimité et l'exactitude des données devant être communiquées dans le cadre du procès.

Par ailleurs, la personne concernée doit en être informée de manière claire et doit avoir la possibilité de refuser la communication sur la base de motifs légitimes.

La présente délibération sera publiée au Journal officiel de la République française.

Le président,

A. Türk