GIDE

GIDE LOYRETTE NOUEL

Compte rendu de la conférence

Règlement européen sur la protection des données

Quelles perspectives et orientations stratégiques pour les entreprises ?

15 mars 2016

Avec les interventions de

BRUNO GENCARELLI
Chef du service de la Protection des Données à la Commission Européenne

FLORENCE RAYNAL
Chef du service des Affaires Européennes et Internationales de la CNIL

ANNA POULIOU
Executive, Lead Attorney for European Privacy & Data Protection, GE Corporate

ANNE DEBET
Professeur en droit des nouvelles technologies à l'Université Paris Descartes

Débats animés par

BENOIT LE BRET et **THIERRY DOR**, Avocats associés de Gide Bruxelles et Paris

Compte rendu rédigé par les étudiants
de l'Université de Paris 2 Panthéon-Assas
Master 2 Droit de la communication
Master 2 Droit du multimédia et de l'informatique
Caroline d'Errico – Jenny Policarpo – Grégoire Froussart

Cette conférence avait pour objectif d'aborder le règlement et la protection des données sous le prisme de l'entreprise. Elle a fait écho à une première conférence organisée par le cabinet Gide en 2012 lors de la proposition du projet de règlement par la Commission européenne à laquelle participait Marie-Hélène BOULANGER, prédécesseur de Bruno GENCARELLI à la direction du service de la protection des données à la Commission européenne. Quatre ans de travail ont été nécessaires pour que le projet soit mené à son terme.

Veuillez noter que la numérotation des articles mentionnés dans ce compte rendu a été mise à jour pour correspondre à la version définitive du règlement général sur la protection des données publiée le 27 avril 2016.

Entré en vigueur le 24 mai 2016, le règlement sera applicable à partir du 25 mai 2018.

Quelles ont été vos principales difficultés dans la mise en place de ce règlement ? La montagne a-t-elle accouché d'une souris ?

Bruno GENCARELLI : La Commission européenne est satisfaite de la longue négociation menée pour rédiger ce règlement, dont l'application pourra être uniforme dans tous les Etats membres. Le règlement se substitue à une directive : ce changement d'instrument juridique a impliqué une réforme d'envergure qui nécessitait d'y consacrer du temps.

La montagne n'a pas accouché d'une souris. L'ensemble du paquet de la réforme relative à la protection des données personnelles a fait l'objet d'un accord politique en décembre dernier. La directive sur le traitement des données par les services de police et les autorités judiciaires en matière pénale est également un texte contribuant à cette réforme de fond, dont les événements récents ont souligné l'importance: nous avons besoin de règles communes également dans ce domaine pour assurer une coopération rapide et efficace entre autorités compétentes. L'Europe s'est ainsi dotée d'un cadre règlementaire complet en matière de protection des données. En outre, on retrouve dans le texte final du règlement tous les axes fondamentaux de la réforme : la rationalisation et la simplification du cadre européen en matière de protection des données, la suppression de certaines formalités, un effort de simplification et d'harmonisation ; la mise à jour des droits des individus et des devoirs des opérateurs ; l'ajout d'instruments nouveaux et utiles comme la portabilité, la notification des failles de sécurité ; l'introduction d'un nouveau système de gouvernance (avec la mise en place du guichet unique, de l'enquête commune et plus généralement la mise en réseau des autorités nationales); ainsi que le renforcement de l'"*enforcement*". Permettre aux consommateurs d'exercer un meilleur contrôle sur leurs données personnelles constitue l'une des pierres angulaires de la réforme et vise à créer un cercle vertueux entre un accroissement de la confiance des individus dans les services en ligne et le développement de la société numérique.

S'agissant des difficultés rencontrées, le début de la négociation a été particulièrement long, principalement en raison des implications institutionnelles d'un tel projet, qui est porteur d'importants changements tenant tant à l'instrument juridique qu'à la gouvernance à mettre en place. Puis, il y a eu une accélération : le trilogue a été rapide et s'est accompagné d'une véritable prise de conscience. Il est alors apparu impératif pour l'Europe de se doter d'un cadre uniforme.

ACCOUNTABILITY

Aux termes du principe d'*accountability* *("responsabilité")* qui apparait à l'article 5.2 du règlement, le responsable du traitement doit garantir et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect du règlement.

Est-ce que le principe de l'*accountability* va changer l'équilibre actuel et quelles étaient les motivations de la Commission pour adopter cette nouvelle forme de responsabilité ?

Bruno GENCARELLI : On retrouve là l'un des objectifs principaux du texte qui démontre sa maturité : le passage d'un système *ex ante* à un système *ex post*, et de ce fait une simplification du cadre réglementaire et une réduction significative des charges administratives. Les mécanismes de notification et d'autorisation préalable peuvent être coûteux, lourds et ne garantissent pas l'effectivité de la protection. Les notifications donnaient lieu au mieux à un contrôle, qui n'était pas toujours suivi d'effets. Certaines opérations (par ex. transferts) étaient soumises à des autorisations dans certains Etats membres et ne l'étaient pas dans d'autres. Cela retardait l'offre de certains produits et services sur le marché. Il était donc opportun de passer à un système *ex post* reposant davantage sur l'*accountability* et l'*enforcement*, y compris à travers des sanctions en cas de violation de ces règles.

Qu'est-ce que cela change pour la CNIL ?

Florence RAYNAL : Au cours des trente dernières années, les entreprises se sont beaucoup focalisées sur le récépissé CNIL. L'allègement des formalités est vu d'un œil favorable par la CNIL, et le dispositif prévu va bien encourager les entreprises à aller au-delà de la simple déclaration de fichier qui est aujourd'hui obsolète. Ainsi, la CNIL a soutenu ce changement en passant d'une optique statique à une optique dynamique. Depuis deux ans, l'organisation de l'autorité a été adaptée pour anticiper au mieux l'arrivée du règlement : à titre d'exemple, une nouvelle direction de la conformité ("*accountability department*") a notamment été créée. La CNIL aura désormais vocation à intervenir *a priori*, en développant ses activités de sensibilisation et d'accompagnement auprès des entreprises, mais également à développer le contrôle *a posteriori*.

Bien que ce changement s'opère au sein des 28 Etats membres, l'harmonisation ne sera toutefois pas absolue : certaines dispositions nationales de clarification, permises par le règlement, ont vocation à subsister. Au sein du G29, la mise en place d'une certaine uniformisation est dès lors fondamentale. La mise en réseau des différentes autorités sera capitale, par le recours au système du guichet unique et par la transformation du G29 en comité européen de la protection des données ("CEPD"), qui pourra prendre des décisions contraignantes. Le principal enjeu du règlement est sa mise en œuvre effective, il faut que les autorités fassent vivre ce texte, entre les autorités mais également vis-à-vis des entreprises. Ainsi, le G29 a adopté un plan d'action, une feuille de route pour 2016 et va notamment développer des lignes directrices pour les entreprises sur :

- la notion de risque, véritable pierre angulaire du règlement ;
- le *data protection officer* ;
- la portabilité ;
- la certification.

Le monde de l'entreprise va-t-il gagner en sécurité juridique avec la fin du formalisme, ou est-il perdant du fait de l'accroissement des sanctions ?

Anna POULIOU : Le principe de responsabilité n'est certes pas une nouveauté, mais il ne s'est développé que récemment dans l'ordre interne européen. La CNIL a émis des standards en 2015 concernant la responsabilité. Du point de vue de la documentation, il convient de mettre en place une conformité des systèmes respectant l'approche du *privacy by design*.

C'est une grande opportunité pour les entreprises : en prenant des mesures très concrètes, elles peuvent raffermir la relation de confiance qui les lie d'une part aux consommateurs, mais également aux autorités.

Ce changement annonce-t-il également plus de protection pour les individus ?

Anne DEBET : L'appréciation générale du principe d'*accountability* est portée depuis 2010 par le G29. En effet, les 70.000 déclarations annuelles faites à la CNIL ne faisaient pas l'objet d'un examen très détaillé.

Par ailleurs, si dans la directive de 1995 les états membres devaient mettre en place des mesures de publicité des traitements tenus par les autorités de contrôle, la documentation tenue par les entreprises sera désormais accessible aux seules autorités de contrôle.

Depuis la genèse du règlement, le principe a été étendu à plusieurs domaines, notamment aux notifications des failles de sécurité.
Les codes de conduite n'ont jusqu'à présent pas rencontré un grand succès. Le code européen sur le marketing direct a été adopté en cinq ans. C'est bien trop long pour un outil qui se veut souple. Les codes de conduite nationaux prospèrent davantage. Le développement des mécanismes de certification est également une bonne chose : c'est un moyen d'inverser la charge de la preuve pour le responsable du traitement.

La saisine de l'autorité de contrôle et la mise en œuvre de la responsabilité sont prévues à l'article 82 du règlement aux termes duquel toute personne ayant subi un dommage matériel ou immatériel peut se prévaloir de son préjudice. Ce principe apparaissait déjà dans la directive de 1995, cependant très peu d'actions pénales ont été entreprises sur ce fondement, le contentieux se développant davantage sur les terrains du droit social et du droit de la preuve.

Du point de vue des individus, l'article 80 du règlement consacre timidement une action de groupe au moyen de laquelle des poursuites pourront être engagées contre les entreprises responsables. Le système prévoit qu'en l'absence de mandat, aucune saisine n'est possible. Le Projet de loi pour la République numérique va peut-être étendre ce régime à des actions de groupe sans mandat.

RESPONSABILITÉ DU SOUS-TRAITANT

Alors que la directive 95/46/CE ne prévoyait pas la possibilité d'invoquer directement la responsabilité des sous-traitants, l'article 82 du règlement institue un régime de responsabilité conjointe entre les responsables du traitement et les sous-traitants en cas de manquement à leurs obligations respectives prévues par le règlement.

La Commission a-t-elle voulu imposer davantage de contraintes aux sous-traitants afin d'épargner les responsables du traitement ou bien afin d'organiser une responsabilité collective ?

Bruno GENCARELLI : La Commission souhaitait mieux prendre en compte les évolutions du secteur depuis 1995. En effet, la réalité des chaînes de responsabilité fait intervenir de plus en plus d'acteurs et il est plus difficile de comprendre la responsabilité effective de chacun d'entre eux. Ainsi, l'article 82 propose à tout individu un point d'entrée de son choix dans ce système. Par ce biais, le sous-traitant peut désormais être tenu responsable de la violation de certaines obligations spécifiques qui restent limitées à la sécurité, au transfert de données au niveau international et aux violations des instructions du responsable du traitement.

Comment la CNIL accueille-t-elle la responsabilité nouvelle prévue à l'article 82 et quelles actions le G29 a-t-il entrepris sur ce thème ?

Florence RAYNAL : la CNIL a vu très favorablement l'introduction d'un statut légal du sous-traitant. En effet, la CNIL était gênée par les dispositions de la loi de 1978 qui ne prévoyait que la responsabilité contractuelle du sous-traitant. Cela a parfois conduit la CNIL à contrôler plusieurs responsables du traitement qui recouraient pourtant au même sous-traitant, sans toutefois que ce dernier ne voit sa responsabilité engagée. La situation était donc relativement injuste et le règlement s'est attaché à rétablir un certain équilibre entre les acteurs.

Comment voyez-vous ces évolutions et quelles en sont les conséquences sur les contrats entre les responsables du traitement et les sous-traitants ?

Anna POULIOU : Forte de mon expérience en tant que responsable du traitement, mais

également en tant que sous-traitant, il me paraît effectivement intéressant de revoir les contrats. La responsabilité nouvelle des sous-traitants doit faire l'objet d'une clause de responsabilité. Cela conduit également à redéfinir les rôles des acteurs ainsi que toutes les obligations légales prévues dans le contrat. Le délai de 72h pour faire une déclaration en cas de faille de sécurité est très court. Il faut donc bénéficier d'un maximum d'informations, ce qui passe par la mise en place d'une collaboration accrue entre les acteurs.

De plus, le règlement prévoit de nouveaux droits pour les individus, comme celui de refuser le *profiling*, d'accéder à ses données personnelles ou de demander que certaines données personnelles soient effacées. Si la répartition des rôles entre chaque type d'acteur n'est pas clairement définie, il semble compliqué de savoir lequel est responsable juridiquement en cas de manquement. L'une des solutions, en pratique, serait de développer des mécanismes d'évaluation technique. Le mieux reste tout de même de prévoir la répartition des cas de responsabilité dans le contrat.

Le système actuel repose sur le principe de responsabilité d'un seul acteur, le responsable du traitement, ce qui a le mérite de la simplicité, alors que le système prévu à l'article 82 du règlement met en place une forme de coresponsabilité plus complexe : cela risque-t-il de poser un problème de lisibilité ?

Anne DEBET : la responsabilité conjointe est actuellement absente du droit français. Le règlement est un élément de clarification de cette responsabilité, même si la CNIL a déjà procédé à un rapprochement dans l'affaire des dossiers pharmaceutiques. Le texte précise que, s'agissant de l'allocation de la responsabilité, le requérant peut exercer un recours alternatif contre le responsable du traitement ou le sous-traitant. Toutefois, le texte ne prévoit pas si cette responsabilité est solidaire. L'article 82 demeure ambigu. Cela conduit à se demander si la responsabilité d'un seul acteur n'était pas plus simple à mettre en œuvre.

GUICHET UNIQUE ET COOPÉRATION

Le mécanisme du guichet unique, qui a progressivement évolué en mécanisme de coopération entre les autorités nationales de contrôle, est une innovation très sophistiquée qui apparaît aux articles 60 et suivants du règlement. Un Comité européen de la protection des données ("CEPD") sera créé afin de garantir l'application uniforme du règlement.

La Commission n'a-t-elle pas renoncé à certaines de ses ambitions en laissant davantage de place au souverainisme des Etats membres pour faire adopter le règlement ?

Bruno GENCARELLI : La façon dont a évolué la question du guichet unique est intéressante du fait même qu'il touche aux libertés fondamentales. La proposition initiale avait pour principale vertu sa simplicité : la Commission prévoyait initialement un système de guichet unique "absolu" en vertu duquel, dans les cas transfrontaliers, seule l'autorité de contrôle de l'Etat membre de l'établissement principal était compétente pour trancher. Néanmoins, ce dispositif a été considéré comme trop strict par les co-législateurs. Ce ne sont pas tant les souverainismes nationaux que l'affirmation du droit des individus à avoir accès à leur autorité et leur juridiction nationale qui a fait évoluer le projet. Le règlement permet aux particuliers d'avoir accès à leur autorité nationale en application d'un principe de proximité. Le système absolu du guichet unique a donc été quelque peu "édulcoré".

Toutefois, les objectifs fixés et les garanties voulues sont maintenus. Une interprétation commune du règlement s'appliquera à tous les cas transfrontaliers. En outre, en cas de divergences entre autorités nationales, un système de règlement des différends contraignant a été introduit pour assurer une interprétation uniforme des règles. C'est extrêmement important : la directive donnait lieu à des interprétations divergentes, y compris au sujet de notions centrales comme celle du consentement. Il faut arriver à une interprétation uniforme et unique du texte au travers du système de "codécision" des autorités nationales.

L'article 65 prévoit qu'en cas de divergence dans une affaire, le CEPD interviendra en tant qu'autorité de règlement des différends. Il

s'agira d'un système de recours ultime. Ainsi, les autorités devront faire preuve d'un esprit de collaboration et devront essayer de trouver un point de compromis avant de faire appel au CEPD. Il faudra donc approfondir la collaboration entre autorités, qu'elles ont déjà développée au travers du G29.

Au sein de la CNIL et du G29, comment voyez-vous la mise en place du guichet unique ?

Florence RAYNAL : Le système de coopération a été pour la CNIL et le G29 un sujet important à suivre, car il concerne directement les autorités et leur capacité à s'organiser afin de créer le système de gouvernance du futur. Si la coopération entre autorités ne fonctionne pas, c'est le règlement dans son entier qui ne peut pas fonctionner.

La première proposition du mécanisme de guichet unique a été critiquée par le gouvernement français et la CNIL dans la mesure où le système proposé était trop favorable aux entreprises leur permettant dans une certaine mesure de choisir l'autorité de contrôle "exclusivement compétente" sur leurs traitements. La CNIL a toujours soutenu la mise en place d'un mécanisme d'interlocuteur unique dans l'Union européenne pour les entreprises, sous réserve que le système ne soit pas défavorable aux individus. Le simple fait qu'un citoyen soit contraint d'exercer ses droits devant un tribunal étranger est une violation de la CEDH et des droits fondamentaux européens. Il faut ainsi trouver un équilibre dans ce système du guichet unique pour chaque acteur.

La version du règlement proposée par le Conseil a rééquilibré les rapports de force entre l'individu et l'entreprise.

Etes-vous sensible à cette convergence entre la Commission et la CNIL ?

Anna POULIOU : Les entreprises sont très enthousiastes à l'idée du guichet unique. Néanmoins, il faut parvenir à un système concret et stable. Le G29 bénéficie d'une expérience croissante et, de fait, le CEPD saura assurer une cohérence entre les autorités nationales.

Florence RAYNAL : Il y aura un niveau national et un niveau européen : une coopération des autorités de contrôle sera donc mise en place conjointement au niveau national et européen. Pour ce faire, des questions subsistent encore. Faudra-t-il habiliter les agents de l'autorité britannique pour faire des contrôles avec la CNIL française, et le cas échéant comment procéder ? Il y aura également des échanges d'information comme le précise l'article 61 qui prévoit une assistance mutuelle. La question de la mise en place d'un tel dispositif demeure entière.

Qu'en est-il du point de vue des droits des individus ?

Anne DEBET : On a pu craindre une forme de *forum shopping* de la part des responsables du traitement situés dans des pays dans lesquels les autorités nationales sont plus "compréhensives", comme dans les pays anglo-saxons. Finalement la définition retenue de l'établissement principal pour la détermination de l'autorité chef de file permet une certaine sécurité. Il est prévu que c'est le lieu de l'administration centrale, à moins que les décisions ne soient prises ailleurs - il s'agit d'un critère plus strict ce qui permet d'apaiser certaines craintes. Ce que l'on peut craindre du point de vue des individus ce sont des délais trop longs et complexes à appréhender.

Florence RAYNAL : S'agissant des recours effectifs pour l'individu, il faut espérer une meilleure application des sanctions, car le montant maximum des sanctions, actuellement insuffisant, pourra demain s'élever à 4 % du chiffre d'affaires mondial de l'entreprise contrevenante et ainsi véritablement produire des effets dissuasifs

QUESTIONS DE LA SALLE

Pourriez-vous apporter un éclairage sur la pertinence de la notion de risque présente dans de nombreux domaines ?

L'approche basée sur le risque s'est accrue au cours des négociations. Il y a là un double objectif :

- avoir des règles moins formalistes qui s'attachent plutôt à la réalité des risques que présentent les traitements ;
- alléger la charge des PME.

L'équilibre peut être délicat à trouver entre une approche basée sur le risque et une approche fondée sur la sécurité juridique. En outre,

s'agissant de l'obligation de tenir une documentation, il y a également eu une évolution du texte en ce qui concerne les petites entreprises. La Commission était partie d'un critère relatif à la taille des entreprises et cela permettait de reconnaitre le rôle particulier des PME. Néanmoins, ce critère a été critiqué comme étant trop formaliste. Ainsi, désormais l'approche est basée sur le risque.

L'article 80 ne parle pas à proprement parler d'action de groupe. En revanche, le projet de loi pour une République numérique actuellement en examen contient des dispositions sur ce principe. Quelle est votre position ?

Ce projet de loi contient des dispositions concernant un champ relativement large. Néanmoins, lorsqu'un règlement est mis en place, il se substitue au droit national. Ce règlement sera en effet d'application immédiate en droit français dans deux ans. Il ne faudra pas contredire le texte du règlement.

S'agissant de l'action de groupe, il y a de grandes divergences entre les Etats membres. L'article 80 reconnaît la possibilité d'une action de groupe. Le règlement vient ainsi favoriser le mécanisme tout en laissant une certaine liberté aux droits nationaux d'en faire usage ou non.

Vous dites que le règlement est adopté de manière définitive politiquement alors même que l'Autriche a publié un communiqué dans lequel elle considère que le règlement ne va pas assez loin et qu'elle ne souhaite pas le signer en l'état.

Cela ne remet pas en cause l'accord politique ni même le contenu du règlement tel que conclu entre les colégislateurs. Le règlement s'adopte à la majorité qualifiée des Etats membres ainsi, en dépit de ce refus de l'Autriche, le règlement sera adopté dans la mesure où une majorité des membres du Conseil (ainsi que du Parlement) a adopté cet acte, qui s'impose désormais à l'ensemble de l'Union, y compris aux Etats membres qui s'y opposent.

Le règlement laisse la possibilité aux Etats membres de mettre en place des lois de transpositions en matière de santé. Cela ne complique-t-il pas les choses ?

En effet, pour les données de santé, il y a eu une certaine résistance de certains états membres par rapport à l'objectif initial qui prônait une forte harmonisation. Toutefois le règlement pose des paramètres communs que les réglementations nationales doivent respecter.

Quelle sera l'articulation entre les sanctions pénales et civiles ?

Il y a très peu de jurisprudence en matière de sanctions pénales. Ces sanctions étaient trop importantes ce qui expliquait leur rareté.

Il est prévu au considérant 119 du règlement que les sanctions pénales devront être appliquées dans le respect du principe *non bis in idem*[1]. La question est donc de savoir si ce principe n'entrainait pas une impossibilité de cumul avec des sanctions administratives. Néanmoins, la CJUE en 2013 a considéré que non.

Le faible développement du contentieux au civil est-il la conséquence du fait qu'il est difficile de déterminer le préjudice ? Quelle perspective pourrait permettre aux individus de mieux agir ?

Les enjeux pour les individus sont très importants notamment en termes de traitement de données bancaires ou de santé. L'obtention d'une indemnisation devrait être possible.

Le recours contentieux n'est pas forcément la solution la plus simple, les individus préférant souvent se tourner vers la CNIL. L'arrêt *Schrems* en est une parfaite illustration : les autorités de protection des données et la CJUE protègent mieux les droits des citoyens.

L'injonction de cessation des traitements ou des transferts est une sanction qui semble encore plus théorique que les sanctions pénales ou administratives. Quelle est votre opinion ?

Il s'agit d'une sanction très peu appliquée. Les difficultés portent sur le point de savoir si cela sera toujours le cas avec le règlement. Cette sanction vise les cas extrêmes pour lesquels le responsable du traitement ne veut manifestement pas se mettre en conformité avec les obligations qui lui incombent au regard de la loi. ■

[1] *Non bis in idem* : principe fondamental de la procédure pénale selon lequel nul ne peut être poursuivi ou puni pénalement à raison de mêmes faits déjà sanctionnés