FONDATION ROBERT SCHUMAN

POLICY PAPER

Question d'Europe
n°250
3 septembre 2012

Quelle protection européenne pour les données personnelles ?

Isabelle Falque-Pierrotin
Conseiller d'Etat, présidente de la CNIL

Résumé :
La Commission européenne a rendu public, le 25 janvier 2012, un projet de règlement relatif à la protection des données à caractère personnel, qui refond l'ensemble du cadre juridique européen issu de la directive de 1995. Si ce projet comporte de nombreuses avancées, notamment en termes de renforcement des droits du citoyen et de mise en conformité des entreprises, le mécanisme de régulation proposé, fondé sur le critère de « l'établissement principal », n'est pas adapté à l'univers numérique. Il est donc proposé de mettre en place une autre gouvernance, tirant le meilleur des approches juridiques latines et anglo-saxonnes et faisant de la protection des données personnelles un avantage pour les entreprises, un nouvel espace de droit pour le citoyen et une opportunité de renforcer l'intégration européenne.

La protection des données personnelles fait l'objet d'un important débat européen. La Commission européenne a en effet présenté, le 25 janvier dernier, un projet de règlement relatif à la protection des personnes en la matière, ainsi qu'un projet de directive en matière de recherche et poursuite des infractions pénales. Ces deux textes visent à moderniser l'encadrement juridique actuel constitué par la directive 95-46 de 1995 compte tenu, notamment, du développement d'internet et du numérique depuis le début des années 2000.

Tout ceci pourrait paraitre un peu théorique et participer de l'extraordinaire capacité communautaire de produire des normes et standards souvent peu compris des citoyens eux-mêmes. Mais nous parlons d'un enjeu qui concerne chacun d'entre nous, de notre capacité au travail, à la maison, dans nos achats, notre santé, à voir notre vie privée effectivement garantie au sein d'un univers qui a tellement changé depuis dix ans.

En quelques années en effet, le monde numérique s'est installé. Il ne s'agit pas seulement d'internet. Il s'agit de la dématérialisation progressive de toutes les activités humaines qui s'étendent désormais du monde physique au monde virtuel ; l'individu passe de l'un à l'autre souvent sans même sans apercevoir et la donnée est au cœur de ce monde « sans couture ».

L'enjeu est de taille pour l'Europe : précurseur dans les années 90 en la matière, elle doit montrer qu'elle est capable de s'adapter aux nouvelles réalités du numérique - de l'internet aux réseaux sociaux, en passant par la vidéosurveillance ou le *big data*- tout en préservant un haut niveau de protection pour l'individu. Elle doit montrer que sur un sujet qui suscite une mobilisation croissante de ceux-ci, elle est capable d'innover et de construire une gouvernance crédible et légitime des données personnelles.

Car telle est bien la question centrale : quel est l'équilibre entre les attentes des individus, les objectifs de politique publique, notamment de sécurité, et ceux des entreprises qui veulent valoriser le potentiel de l'économie numérique que nous souhaitons voir présider à ce texte ? Quels sont les outils, le dispositif dont nous souhaitons nous doter pour piloter celui-ci ?

A ces deux questions il n'y a pas de réponse univoque. La gouvernance retenue résulte du pacte social qui doit s'établir entre les acteurs publics et privés au terme d'un débat approfondi et celui-ci peut d'ailleurs évoluer avec le temps. L'équilibre recherché est donc intrinsèquement dynamique.

A l'heure de l'économie numérique, dont les données personnelles sont le véritable « carbu-

rant », de l'émergence de nouveaux services comme le *cloud computing*, mais aussi des attentes et des inquiétudes que ces évolutions suscitent, et enfin de l'interdépendance croissante et parfois menaçante entre nos pays en termes de sécurité et d'infrastructures, la renégociation de la directive de 1995 n'est pas un sujet mineur. Il en va de la confiance du citoyen dans la croissance de demain et dans les institutions chargés de protéger ses droits, de la compétitivité économique des entreprises européennes, et de la cohérence et la crédibilité de l'Union.

Cette adaptation du cadre communautaire constitue un objectif d'autant plus délicat que d'autres pays ou régions du monde mènent des réflexions comparables, qu'il s'agisse du « *bill of Rights* » de la protection des données personnelles publié par la Maison blanche en février 2012, ou des travaux de l'APEC sur les transferts internationaux de données. Nos travaux seront donc analysés à l'aune des comparaisons internationales. La difficulté sera bien sûr d'aboutir à un niveau élevé de protection, tout en garantissant l'interopérabilité des différents systèmes entre eux. C'est dans ce contexte que le projet de la Commission européenne s'inscrit.

Ce projet répond-il aux différentes exigences qui viennent d'être rappelées ? En grande partie, oui. Peut-il être amélioré pour être porteur d'une vision pragmatique de la protection des données personnelles, fidèle aux principes fondamentaux applicables en la matière, sans pour autant faire de l'Europe un îlot à côté duquel passerait l'économie numérique ? Tout aussi certainement.

La Commission nationale de l'informatique et des libertés (CNIL) qui a développé une connaissance des acteurs comme des processus depuis plus de 30 ans, entend, selon une démarche constructive et positive, participer à l'amélioration de ce futur cadre juridique commun. La gouvernance qui sera instaurée dans ce domaine sera appelée à servir de modèle, et à constituer une référence de la protection de la vie privée, notamment au sein de l'espace francophone. L'Europe doit en sortir plus forte, plus intégrée, mieux armée pour faire face à la mondialisation des transferts de données, sans renoncer à ses principes et à ses valeurs, dont le citoyen est le centre de gravité.

Le projet de règlement proposé par la Commission européenne le 25 janvier traduit tout d'abord un nouvel équilibre des droits, obligations et sanctions applicables auxquels la CNIL souscrit globalement. Au-delà de ces caractéristiques fondamentales, de nombreux apports méritent d'être soulignés et promus au cours des négociations à venir. En revanche, l'architecture de pilotage de la protection des données personnelles envisagée par la Commission n'est pas adaptée à la réalité de l'univers numérique, le critère de « l'établissement principal » qu'elle promeut étant juridiquement incertain et concrètement impraticable. En fait, l'enjeu est d'apporter une réponse à deux objectifs distincts : faciliter les démarches et le respect de la législation par les entreprises ; et permettre une amélioration des contrôles et des sanctions portées par les autorités de contrôle nationales lorsqu'est en cause un traitement de données intéressant plusieurs pays de l'Union européenne. C'est en particulier sur ces deux questions que la CNIL propose un système cohérent, efficace et protecteur, qui bénéficiera à la construction européenne.

I. LE PROJET DE RÈGLEMENT : UN NOUVEL ÉQUILIBRE DES DROITS, OBLIGATIONS ET SANCTIONS

1. Des avancées réelles

La Commission européenne, et plus particulièrement sa vice-présidente Viviane Reding, ont eu à cœur de porter un message efficace : « un continent = une règle applicable ». La CNIL ne peut que souscrire à cette perspective, même si elle n'adhère pas à toutes les conséquences qu'en tire la Commission.

Il est en effet certain que, à ce titre, la directive de 1995 ne constitue plus un instrument parfaitement adéquat. Alors que la mondialisation progresse et suscite une très forte croissance des échanges de données, que l'Europe a intérêt à constituer un marché unique des données personnelles, la directive a fait l'objet de transpositions nationales variées qui ont facilité des disparités entre Etats membres, compte tenu des réglementations nationales applicables en la matière. A titre d'exemple, la CNIL française dispose depuis 2004 d'un pouvoir de sanction dont elle fait régulièrement usage, alors que de nombreuses autres autorités nationales ne disposent pas des mêmes pouvoirs ou s'en sont vues dotées récemment. Une révision du cadre normatif est donc opportune pour harmoniser le cadre juridique.

L'adoption d'un règlement permettrait indéniablement, dans ce domaine qui touche aux libertés fondamentales des individus, de résorber en partie ces divergences par l'application d'un même texte sur l'ensemble de l'Union. Une telle démarche constitue d'ailleurs à la fois une garantie pour le citoyen, un élément de sécurisation juridique pour les responsables de traitement – au

premier chef les entreprises –, et un moyen d'améliorer la coopération entre les autorités de contrôle.

Mais au-delà de la nature du vecteur normatif utilisé, le règlement opère un changement de paradigme dans la régulation des données personnelles, non sur les principes eux-mêmes mais sur les outils de régulation mis à disposition des acteurs et des régulateurs.
Le système actuel est en effet marqué par l'importance des formalités préalables, notamment dans le cadre du régime des « déclarations » de traitements automatisés auprès des autorités de contrôle nationales. Ces formalités portent la quintessence des principes « Informatique et libertés » et sont contrôlés *a priori* par le régulateur. A titre indicatif, la CNIL enregistre ainsi plus de 80 000 déclarations par an. Le dispositif est vécu comme étant très lourd, parfois parcellaire – tous les acteurs concernés n'ayant pas toujours conscience de leurs obligations de déclaration – et, dans certains cas, insuffisamment propice à une mise en conformité évolutive de la part des « responsables de traitements ». Concrètement, une fois les formalités préalables effectuées, le principal moyen de s'assurer de la conformité effective d'un dispositif est le mécanisme de contrôle *a posteriori* susceptible de déboucher sur une mesure coercitive comme une mise en demeure, voire une sanction.

A cette logique forte mais quelque peu binaire, le projet de règlement propose une vision ternaire qui consiste à atténuer considérablement le poids des formalités préalables, à renforcer les pouvoirs de contrôle et de sanction et, entre les deux, à construire une nouvelle couche de responsabilisation des acteurs, l'*accountability*. L'idée est simple : face à l'explosion des données personnelles, il faut que les responsables de traitements intègrent dans leurs pratiques mêmes les principes « informatique et libertés » car la seule politique de sanction ou de formalités préalables ne saurait tout encadrer. La mise en place de politiques internes de conformité mobilisant un certain nombre d'outils prévus par le règlement est donc un nouvel objectif des régulateurs, soucieux d'embrasser de façon effective la réalité dynamique et évolutive de l'univers numérique.
La CNIL souscrit pleinement à cette orientation générale qui s'inscrit dans une démarche de « co-régulation » indispensable dans un univers complexe comme l'univers numérique. Un tel processus est nécessaire tant du point de vue du citoyen que de celui des entreprises. Pour ces dernières, notamment celles dont l'activité est essentiellement numérique, les données personnelles peuvent constituer une valeur commerciale, voire un actif financier. Mais surtout la protection efficace de ces données est désormais une attente majeure et partagée des citoyens, qui sont également, sur le plan économique, des consommateurs. La fiabilité en la matière est donc une exigence commerciale et économique déterminante, parce qu'elle conditionne la confiance individuelle et collective. La protection des données personnelles devient ainsi l'une des composantes de la responsabilité sociale des entreprises et de leur avantage concurrentiel.

Naturellement, les autorités de contrôle seront amenées à accompagner les entreprises dans la définition de règles de conduite internes contraignantes en matière de protection des données, dont la mise en place devra évidemment être prise en compte par ces mêmes autorités, au crédit de l'entreprise, par exemple en cas de faille de sécurité ayant occasionné une violation de confidentialité de données personnelles, ou encore en cas de contrôle postérieur révélant un défaut de conformité. *In fine*, la suppression des déclarations, synonyme de simplification pour les entreprises, sera donc compensée, en termes de protection, par ces mécanismes de mise en conformité. Le projet de règlement est donc profondément novateur et adapté à l'ère numérique en ce qu'il met en place un nouvel équilibre entre formalités préalables, conformité et sanctions.

2. Dont il convient de garantir la pérennité

Les principales avancées du projet de règlement portent sur deux aspects : le renforcement des droits des personnes, et les conditions dans lesquelles les entreprises peuvent traiter et échanger des données à caractère personnel.

S'agissant des droits des personnes, sans en dresser

un inventaire exhaustif, on peut noter le renforcement du consentement des personnes, qui devra désormais être explicite, la reconnaissance d'un droit à l'oubli numérique et d'un droit à la portabilité, lesquels constituent des progrès majeurs.

Le « droit à l'oubli » apparaît particulièrement essentiel, alors que le développement, notamment, des réseaux sociaux se traduit par une exposition croissante de leur vie privée par les individus, en particulier les jeunes, et qu'il est désormais possible de souscrire des assurances destinées à protéger « *l'e-reputation* » de la personne ! Le droit à l'oubli, c'est la volonté de chacun d'entre nous de maitriser ses traces numériques et sa vie privée ou publique en ligne. Le règlement pourrait cependant être plus ambitieux : il est certes prévu que les citoyens n'auront plus à justifier leur demande de suppression de données les concernant sauf à ce que l'entreprise justifie d'un motif légitime à leur conservation, mais le texte ne prévoit aucune obligation de « déréférencement » par les moteurs de recherche, alors que ceux-ci constituent pourtant la principale clé d'entrée pour rechercher des données personnelles sur Internet. Enfin, le projet de texte prévoit une protection spécifique pour les enfants de moins de 13 ans, ce qui est évidemment positif même si l'âge retenu prêtera nécessairement à débat.

Quant aux aspects positifs pour les entreprises, l'allègement des formalités préalables et le développement des processus de mise en conformité concilient globalement les exigences de pragmatisme et protection : la désignation obligatoire d'un correspondant à la protection des données – que la France, à l'instar de l'Allemagne ou des Pays-Bas, a instauré dans la loi avec les « correspondants informatique et libertés » – ou l'*accountability* seront de nature à conforter la participation de tous les acteurs concernés à la protection des données, mais aussi à garantir un haut standard de qualité des entreprises européennes vis-à-vis du consommateur. Le texte comporte donc des avancées substantielles en termes de droits et d'obligations ; cependant, le dispositif de mise en œuvre envisagé est, en revanche, très insatisfaisant.

II. MAIS UN DISPOSITIF DE MISE EN ŒUVRE ENVISAGÉ PEU ADAPTÉ À LA RÉALITÉ DE L'UNIVERS NUMÉRIQUE

La protection des données personnelles est un droit à part entière, qui se trouve à la croisée d'autres droits fondamentaux, notamment le droit de propriété, le droit au respect de la vie privée et la liberté d'expression. Elle interagit également avec des principes économiques et commerciaux, en particulier dans le domaine de la protection du consommateur et de règles publicitaires. Elle influe aussi sur l'organisation des entreprises, quelle que soit leur taille. C'est précisément cette situation centrale dans l'exercice des libertés et essentielle en matière économique, notamment pour l'économie numérique, qui est la cause des attentes, mais aussi des inquiétudes profondes des citoyens européens en la matière. Or, de telles inquiétudes ne peuvent être apaisées, ni de tels droits garantis, par une simple consécration juridique.

L'encadrement de l'usage des données personnelles – vitales pour l'individu aussi bien en tant que citoyen que consommateur, donc vitales pour la vie démocratique comme pour les entreprises – implique de mettre en place un dispositif susceptible de susciter la confiance de tous. C'est là que, à notre sens, le bât blesse dans le projet de règlement.

Celui-ci entend procéder intégralement d'une équation en apparence simple et porteuse : « un continent = une règle = une autorité de contrôle compétente lorsque le traitement s'applique à plusieurs pays ». Si nous souscrivons aux deux premiers termes de l'équation, le troisième, tel qu'il est conçu par la Commission, n'est ni de nature à susciter la confiance des citoyens, ni, ce qui est lié, de nature à permettre un contrôle effectif de la protection des données personnelles.

Que dit, sur ce point, le projet de règlement ? L'article 51-2 prévoit que « *Lorsque le traitement des données à caractère personnel a lieu dans le cadre des activités d'un responsable du traitement ou d'un sous-traitant établis dans l'Union, et lorsque le responsable du traitement ou le sous-traitant sont établis dans plusieurs États membres, l'autorité de contrôle de l'État membre*

où se situe l'établissement principal du responsable du traitement ou du sous-traitant est compétente pour contrôler les activités de traitement du responsable du traitement ou du sous-traitant dans tous les États membres, sans préjudice des dispositions du chapitre VII du présent règlement ». En d'autres termes, lorsque des données font l'objet d'un traitement à l'échelle de plusieurs pays de l'Union, l'autorité nationale du pays où est implanté l'établissement principal de l'entreprise en question serait seule compétente pour contrôler celle-ci.

Le critère ainsi posé est d'une part juridiquement flou ; d'autre part, il n'apporte de réponse satisfaisante ni aux autorités, ni aux entreprises ni au citoyen.

Flou juridiquement, car nul n'est, actuellement, en mesure de savoir ce que recouvre la réalité de l'établissement principal. Le projet de règlement définit l'établissement principal comme le lieu où sont prises « les principales décisions quant aux finalités, aux conditions et aux moyens du traitement ». Non seulement il retient une approche traitement par traitement – ce qui signifie que, potentiellement, un même groupe aura autant d'établissements principaux que de traitements – mais il implique également une appréciation de pur fait, sujette à interprétation et à débat, donc synonyme d'insécurité juridique pour le citoyen, l'entreprise et l'autorité de contrôle. A parfois été évoqué une autre définition, faisant état du lieu où se définit la politique de l'entreprise en matière de protection des données. Mais là encore, on reste sur une appréciation de fait et non sur un critère de droit.

Par ailleurs, le mécanisme imaginé est difficilement praticable sur le plan institutionnel : il implique tout d'abord que les autorités de contrôle déterminent l'établissement principal, ce que l'entreprise pourra contester, au risque éventuellement de faire tomber tardivement la procédure. Mais surtout, il fait des autorités des pays des citoyens lésés de simples « boîtes aux lettres » pour ces derniers, dénuées de toute compétence puisque le règlement prévoit une compétence exclusive de l'autorité du pays où est implanté le fameux « établissement principal ». Pour corriger les effets néfastes d'un tel mécanisme, le projet de règlement imagine un système dans lequel les autorités de contrôle pourraient, à la demande de leurs ressortissants respectifs, contester les décisions les unes des autres. Mais un tel mécanisme, animé d'une volonté de simplification louable, aboutit à l'effet contraire de celui recherché : une moindre intégration européenne, une concurrence entre autorités et, *in fine*, une moindre protection du citoyen.

Car le principal danger est ici : le mécanisme proposé fragilise la protection du citoyen. En amont, il favorisera des stratégies de contournement de la part d'acteurs peu scrupuleux, selon, notamment, les moyens dont seront dotées les autorités de contrôle des Etats membres. Il s'agit, en quelque sorte, d'un risque de « *data dumping* » en fonction des capacités effectives des autorités de contrôle, mais aussi des autres législations avec lesquelles la protection des données doit être articulée (droit social, droit du travail, etc.). En aval, en cas de plaintes ou de contrôles, l'autorité compétente sera celle de l'auteur potentiel de l'infraction, et non celle du citoyen-victime. Ce système, caractérisé par une territorialité du contrôle administratif et juridictionnel favorable à l'auteur potentiel de l'infraction, est évidemment très défavorable pour le citoyen. Au-delà, on peut s'interroger sur l'effectivité du droit au recours ouvert à ce dernier, sur laquelle les considérants du règlement insistent pourtant, et, plus généralement, sur le respect des droits de la défense. Comment ne pas imaginer le sentiment d'impuissance, l'inquiétude, voire la défiance, d'un citoyen qui ne saura pas à qui s'adresser, qui ne verra dans l'autorité la plus proche de lui qu'une simple boîte aux lettres, et qui devra engager des recours devant des juridictions d'autres Etats membres, avec tout ce que cela suppose en termes de coûts, de traduction et de méconnaissance des systèmes juridiques des autres Etats ?

Enfin, une telle défiance se doublera d'une difficile mise en œuvre pour les entreprises elles-mêmes. A aucun moment, le règlement ne définit les responsabilités respectives de « l'établissement principal » et des autres entités (notamment la maison mère ou les filiales). Le système imaginé est en fait conçu pour un certain type d'entreprises, à savoir les grands acteurs de l'Internet et de la vente en ligne. Or, la plupart des

entreprises du secteur industriel ou du secteur tertiaire ne sont pas organisées de manière centralisée, mais au contraire de manière déconcentrée, conformément d'ailleurs au principe d'indépendance des filiales. Le système envisagé est donc peu lisible pour le citoyen et peu effectif en termes de droit au recours ; il est peu adapté à la diversité organisationnelle des entreprises et difficilement praticable entre des autorités de régulation appelées par ailleurs à coopérer pour assurer l'application uniforme de la réglementation communautaire. En un mot, le dispositif n'est pas opérationnel.

III. VERS UNE AUTRE GOUVERNANCE

1. Pour un dispositif européen de régulation efficace en matière de protection des données personnelles.

Le système actuel, issu de la directive de 1995, soulève deux difficultés majeures. La première, au stade des formalités préalables, est que la « territorialisation » de ces démarches impose aux entreprises qui souhaitent mettre en œuvre des traitements automatisés dans plusieurs pays de multiplier les démarches administratives. Ces démarches répétitives ont certes un coût financier – la Commission européenne avance le montant de 2,4 milliards € par an, à rapporter toutefois au nombre total d'entreprises dans l'Union. Mais elles sont surtout source d'interrogations voire d'insécurité juridique pour les entreprises, notamment du fait de la diversité des procédures et délais applicables. La seconde difficulté réside, au stade de l'examen des plaintes et des contrôles, dans l'impossibilité pour les autorités de contrôle de prendre une décision commune de sanction lorsqu'un traitement commun à plusieurs pays de l'Union est en cause.

La Commission européenne a cru devoir apporter une réponse unique à ce double problème. La CNIL propose au contraire de distinguer les deux et de créer ainsi un système lisible pour le citoyen, aisé à mettre en œuvre pour l'entreprise, et contrôlable plus efficacement par les autorités de contrôle nationales. La protection des données implique, à notre sens, de satisfaire à deux exigences : placer le citoyen au centre du système ; créer un système de contrôle qui soit à la fois décentralisé et intégré.

Le point de départ est celui du critère de détermination de la compétence générale « de droit commun » des autorités nationales. Nous proposons de retenir le lieu de résidence du citoyen et, à titre subsidiaire, celui de l'établissement du responsable de traitement. En d'autres termes, lorsque les données personnelles d'un citoyen font l'objet d'un traitement, l'autorité de son pays de résidence doit se voir, par principe, reconnaître une compétence pour s'assurer de la conformité du traitement à la réglementation. A partir de là, il convient de distinguer les deux aspects précédemment évoqués :

a) Sur le premier point – la mise en conformité des entreprises en « amont » -, nous proposons d'ouvrir aux entreprises disposant de plusieurs établissements dans l'Union européenne, la possibilité de désigner en leur sein l'entité en charge de la protection des données et de solliciter, à ce titre, un interlocuteur unique. Puisque les entreprises ont besoin à la fois d'une certaine souplesse organisationnelle et, pour certaines, d'un « point d'entrée » unique pour leurs démarches, il est ainsi proposé de leur offrir cette faculté de désigner une « entité de référence », juridiquement responsable des traitements communs à plusieurs pays de l'Union, à charge pour les autorités des pays dont les résidents sont concernés de se rapprocher dans le cadre du mécanisme de coopération.

Une telle solution présente l'avantage d'épouser les structures des entreprises. Celles-ci n'ont pas besoin de se voir imposer une forme d'organisation interne déterminée. Elles ont besoin au contraire, en fonction du secteur d'activité concerné et de leurs priorités stratégiques, de retenir l'organisation de leur choix, ce qui implique que les autorités publiques puissent contrôler le respect d'exigences de fond, en interférant le moins possible avec leur organisation interne. En la matière, offrir aux entreprises une faculté de désigner une entité de référence pour conduire la politique de mise en conformité et effectuer les formalités préalables, et leur donner pour cela un interlocuteur unique, permet de tenir compte des différents modèles économiques,

du groupe industriel classique à l'opérateur de l'économie numérique. Un tel mécanisme est enfin synonyme de sécurité juridique, puisque l'entité de référence constitue alors le responsable de traitements pour les traitements communs à plusieurs pays de l'Union.

Concrètement, les critères proposés (lieu du traitement, siège social, lieu de définition de la politique vie privée) pourraient alors être utilisés comme faisceau d'indices pour aider les entreprises à faire leur choix « d'entité de référence », comme c'est le cas en droit de la concurrence. Elles pourront ainsi, en fonction de leur réalité économique, retenir l'entité la plus pertinente.

Quant aux autorités de contrôle, alors que le projet de règlement actuel conduit à retenir un critère de fait, applicable traitement par traitement, ce qui conduira les autorités à s'immiscer dans la réalité et l'organisation de l'entreprise pour identifier, d'elles-mêmes, l'établissement principal, notre proposition, qui fait de l'entité de référence le responsable principal de traitement, retient au contraire, du point de vue de l'autorité « pilote » en matière d'accountability, un critère de droit : celui, si l'entreprise le souhaite, du responsable principal de traitement. Si l'entreprise ne le souhaite pas, c'est alors la situation actuelle qui s'appliquera – autant d'interlocuteurs que de pays concernés – mais dans un cadre juridique marqué par la très nette diminution des formalités préalables. Concrètement, les autorités de contrôle seront donc amenées à coopérer autour de l'autorité pilote – interlocuteur unique.

b) Sur le second point – la compétence en matière de contrôles et de sanctions -, nous proposons, dans le prolongement de l'avis du G29, d'instaurer un mécanisme d'autorité pilote. Toute autorité nationale, saisie d'une plainte d'un de ses résidents ou après auto-saisine, serait compétente pour instruire la plainte et opérer les contrôles relatifs aux traitements mis en œuvre sur son territoire. Le principal critère de compétence est ainsi un critère de « ciblage » sur le lieu de résidence du citoyen concerné – comme par exemple en droit de la consommation – quel que soit, par ailleurs, le lieu d'établissement du responsable de traitement. Lorsque plusieurs pays européens seraient concernés, les différentes autorités compétentes devraient désigner une autorité « chef de file » pour piloter en leur nom l'enquête commune aux plaintes susceptibles d'aboutir. Cette autorité chef de file pourrait recourir à l'expertise et aux moyens d'instruction des autres autorités. La décision de sanction serait alors prononcée, soit conjointement par les autorités concernées (codécision), soit après une procédure d'avis pouvant donner lieu à la publication « d'opinion dissidente ».

Concrètement, l'autorité chef de file pourra être désignée en fonction de critères tels que, par ordre de priorité, l'antériorité ou le nombre des plaintes ; le pays d'établissement de « l'entité de référence » - ce sera alors la même autorité pilote que celle en charge du pilotage de l'*accountability* – ; le pays dans lequel le traitement est mis en œuvre. Pour le citoyen, il s'agit d'un système lisible : c'est bien l'autorité de son pays qui est compétente, dès lors qu'il a été concerné par un traitement de données à caractère personnel, à charge pour cette autorité de s'organiser avec ses homologues s'il y a lieu. Ses droits au recours sont totalement protégés, puisqu'il y a alors une cohérence totale entre le lieu du contrôle administratif et le pays de l'éventuel litige juridictionnel. Enfin, la cohérence est absolue pour le citoyen quelle que soit la situation de l'entreprise : que l'opérateur ait ou non un établissement au sein de l'Union, le critère de compétence de l'autorité de contrôle reste le même : le lieu de résidence du citoyen. Pour les entreprises, le système est également synonyme de sécurité juridique et de lisibilité institutionnelle : elles peuvent être contrôlées partout où leurs traitements sont mis en œuvre, mais selon des critères communs et dans le cadre d'une procédure qui leur garantit l'unicité du contrôle et de la sanction administrative. Pour les autorités nationales, enfin, ce mécanisme permet de préserver une compétence proche du terrain et de la réalité des entreprises.

La CNIL propose donc une solution alternative à celle du critère de l'établissement principal, en recourant à des notions juridiques connues, et au service des objectifs qui ont guidé le travail de la Commission européenne. L'enjeu est de permettre une coopération renforcée, voire une prise de décision intégrée, entre des autorités nationales souveraines, conformément au principe communautaire de subsidiarité. Lisibilité,

sécurité juridique, simplicité, efficacité : tels sont les maîtres mots de cette proposition, qui a pour objectif de préserver la confiance des citoyens. Cette proposition a par ailleurs pour corollaire la définition précise du contenu de l'*accountability*.

2. Donner un contenu effectif à l'accountability

Il faut d'abord savoir de quoi on parle : à la mode, le concept d'accountability n'en reste pas moins flou. Or, compte tenu de la place centrale que tient cette notion dans le projet de texte, il nécessite d'être défini rigoureusement. Nous proposons, dès lors, de désigner sous ce vocable *le processus permanent et dynamique de mise en conformité d'une entreprise aux principes informatique et libertés grâce à un ensemble de règles contraignantes et de bonnes pratiques correspondantes*, l'entreprise étant accompagnée dans cette démarche par l'autorité de régulation.

Le projet de règlement prévoit notamment que les responsables de traitement et les sous-traitants devront mettre en place des règles internes et des politiques transparentes en la matière et, en particulier, effectuer une analyse d'impact pour les traitements présentant des risques pour les données personnelles, avertir la personne concernée en cas de violation de ses données personnelles, désigner un délégué à la protection des données et mettre en œuvre des mesures techniques et opérationnelles afin d'assurer la sécurité des données. Le projet répond ainsi à certaines des exigences qu'a toujours portées la CNIL dans son accompagnement des entreprises en matière de protection des données personnelles : protection et information de la personne ; prise en compte dès la conception d'une politique ou d'un choix stratégique de l'aspect « protection des données personnelles » ; et sécurité logique et physique des données.

La vraie question est, finalement, celle du contenu qu'il convient de donner à cette orientation. Deux visions se confrontent en la matière : pour les uns, il s'agit, finalement, d'une liste de prescriptions « passives », à l'instar de cases, qu'il suffirait à l'entreprise de cocher pour être en règle ; l'*accountability* jouerait ici plutôt un rôle de clause exonératoire de responsabilité ! Pour les autres, dont fait partie la CNIL, il s'agit, bien au-delà de ceci, d'une mise en conformité réelle et vertueuse, c'est-à-dire susceptible à la fois de renforcer la confiance des consommateurs et de générer de la création de valeur pour l'entreprise en l'inscrivant dans un processus durable de responsabilité. C'est d'ailleurs par ce qu'elle touche à la substance que cette *accountability* pourrait être prise en compte par les régulateurs dans leurs politiques de sanction.

A cet égard, la CNIL ne peut être que réservée sur des dispositions qui ouvrent la possibilité aux entreprises d'encadrer les transferts de données personnelles vers des pays « tiers » ne disposant pas d'un même niveau de protection, grâce à des instruments juridiques non contraignants résultant d'une auto-évaluation des risques impliqués par le transfert. Il ne s'agit pas en effet pour l'entreprise de s'auto-évaluer, mais de s'inscrire dans une démarche de responsabilité sociale qui inclut la protection des données personnelles, en liaison avec les autorités de contrôle compétentes. C'est précisément cette relation qui garantira la protection optimale des données personnelles.

3. Rendre effectif les nouveaux droits des individus

Les individus craignent le nouveau monde numérique tout en profitant largement de ses services. Ils craignent de ne pas maitriser leurs traces numériques, ils craignent la mise en place d'une société de surveillance et de contrôle, ils craignent finalement de voir cette modernité se retourner contre eux.

Le règlement est donc fortement attendu sur ce point. A cet égard, le renforcement des droits des citoyens passe, à nos yeux, par l'introduction d'un véritable « droit au déréférencement », qui est le corollaire du droit à l'oubli à l'ère du numérique. Comment, en effet, peut-on concevoir un droit à l'oubli qui ne serait qu'un simple droit à l'effacement des données, si celles-ci peuvent être rapidement et durablement répliquées à grande échelle, sans considération de temps ou de frontières ? Seul un droit effectif au déréférencement, dûment encadré bien sûr, permettra de rendre effectif le droit à l'oubli de demain, comme l'Union européenne

a su rendre effectif le droit à l'effacement hier.

CONCLUSION

Le projet de la Commission est entré dans la phase de débat parlementaire. L'Europe – comme le reste du monde – est confrontée au défi majeur d'assurer une juste protection des données personnelles de ses citoyens, sans enrayer le formidable développement du numérique, notamment dans la sphère économique. Fondamentalement, la question est dorénavant celle de la mise en place d'une régulation, par définition territoriale, d'un phénomène partiellement déterritorialisé. Dans ce contexte, la protection des données personnelles repose sur un triptyque : les citoyens ; les responsables de traitement, notamment les entreprises et leurs sous-traitants ; et les autorités de contrôle. Pour les premiers, il s'agit d'une liberté fondamentale ; pour les deuxièmes, il doit s'agir désormais, à part entière, d'une composante de leur responsabilité sociale ; pour les dernières, la protection implique une forte coopération, voire un véritable mécanisme de codécision dans certains cas.

C'est dans ce sens que vont les propositions de la CNIL. Au service du citoyen, au bénéfice des entreprises, et à l'appui de l'Union chargée de les protéger.

Isabelle Falque-Pierrotin

conseiller d'Etat, est présidente de la Commission nationale de l'informatique et des libertés (CNIL) depuis le 21 septembre 2011. Ancienne présidente de la Commission interministérielle relative à internet en 1996, elle a été présidente du Conseil d'orientation et déléguée générale du Forum des droits sur l'internet de 2001 à décembre 2010. Elle est membre de la CNIL depuis janvier 2004.

Retrouvez l'ensemble de nos publications sur notre site :
www.robert-schuman.eu

Directeur de la publication : Pascale JOANNIN