Conférence de haut niveau: «Dimensions éthiques de la protection des données et de la vie privée»
Centre pour l'éthique, Université de Tartu / Inspection de la protection des données
Tallinn, Estonie, 9 janvier 2013

Loi européenne relative à la protection des données – situation actuelle et perspectives d'avenir

Peter Hustinx
Contrôleur européen de la protection des données

La protection de la vie privée et des données – plus précisément: le droit au *respect* de la vie privée et le droit à la *protection* des données à caractère personnel – sont deux expressions relativement récentes d'un concept universel à fortes dimensions éthiques: la dignité, l'autonomie et la *valeur unique* de chaque être humain, ce qui implique également le droit de chaque individu de développer sa propre personnalité et d'exercer une influence juste sur les questions qui peuvent avoir une incidence directe sur sa personne.

Domaine spécifique du droit, la protection de la vie privée et des données s'est développée au cours des quatre dernières décennies, notamment dans le cadre du Conseil de l'Europe et de l'Union européenne, en conséquence, notamment, de l'influence grandissante des technologies de l'information et de la communication (TIC). Ces technologies font désormais partie de notre environnement quotidien et permanent, de notre vie tant privée que professionnelle, et il y a fort à parier que ce phénomène s'accentuera encore dans un avenir proche.

Dans ma communication d'aujourd'hui, je souhaiterais examiner l'histoire et l'état actuel du droit, de même que la direction que le droit de la protection de la vie privée et des données pourrait prendre pour garantir une protection plus efficace, conformément à ses origines et à sa vocation éthiques.

Dans cet aperçu, nous en examinerons deux aspects principaux dont le premier est le *renforcement* des droits à la protection de la vie privée et des données en tant que tels, et le second la nécessité de garantir une application *plus cohérente* de ces droits dans l'Union européenne, les deux ayant pour but de promouvoir une protection *plus efficace* dans la pratique et d'éviter une *diversité inutile* dans la façon dont cette protection est assurée dans les divers États membres.

Vie privée

C'est seulement après la Seconde Guerre mondiale que le concept de «droit à la vie privée» a vu le jour dans le droit international. Il est d'abord apparu sous une forme relativement atténuée à l'article 12 de la Déclaration universelle des droits de l'homme (Assemblée générale des Nations unies, Paris, 1948), qui prévoit que nul ne sera l'objet d'immixtions *arbitraires* dans sa vie privée, sa famille, son domicile ou sa correspondance.

Une plus grande protection a ensuite été garantie par l'article 8 de la Convention européenne des droits de l'homme (Conseil de l'Europe, Rome, 1950), qui prévoit que toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance, et qu'il ne peut y avoir d'ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est *prévue* par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est *nécessaire* à certains intérêts importants et légitimes.

La mention du domicile et de la correspondance reposait sur des traditions inhérentes à de nombreux pays du monde et héritées d'une longue évolution, de plusieurs siècles parfois, mais l'accent placé sur la vie privée constituait une nouveauté et une réaction manifeste à ce qu'il s'était passé au cours de la Seconde Guerre mondiale.

La Cour européenne des droits de l'homme de Strasbourg a expliqué la portée et les conséquences de cette protection dans une série de jugements. Dans toutes les affaires concernées, la Cour examine s'il y a une *ingérence* dans le droit à la vie privée et, dans l'affirmative, si cette ingérence est justifiée par une base juridique *appropriée* – c'est-à-dire claire, accessible et prévisible – et si elle est *nécessaire* et proportionnée à l'intérêt légitime en jeu.

Dans la jurisprudence de la Cour, le concept de «vie privée» ne se limite pas aux situations «d'intimité», mais couvre également certains aspects de la vie professionnelle et du comportement en public, appartenant ou non au passé, pour lesquels les personnes concernées peuvent raisonnablement s'attendre à un certain respect de la vie privée, mais cela concerne souvent des situations spéciales, impliquant des informations sensibles ou des enquêtes de la police ou des services secrets.

La protection des données

Vers 1970, le Conseil de l'Europe est arrivé à la conclusion que l'article 8 de la CEDH présentait un certain nombre de lacunes au vu des évolutions récentes, en particulier dans le domaine des technologies de l'information: la portée incertaine de la notion de «vie privée», l'accent mis sur la protection contre les autorités publiques et le manque d'approche proactive contre les éventuels abus des informations à caractère personnel de la part des entreprises et des autres organisations du secteur privé.

Après une préparation minutieuse, la Convention pour la protection des données, également connue sous le nom de Convention 108 (Strasbourg 1981), a en conséquence été adoptée, et été à ce jour ratifiée par 44 États membres du Conseil de l'Europe, au nombre desquels tous les États membres de l'UE.

La Convention a pour but de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant («protection des données»). La notion de «données à caractère personnel» y est décrite comme «toute information concernant une personne physique identifiée ou identifiable («personnes concernées»)».

Ceci signifie que «la protection des données» *a une portée plus large* que la «protection de la vie privée», car elle concerne également d'autres droits et libertés fondamentaux et toutes sortes de données *indépendamment* de leur rapport avec la vie privée, et en même temps *une portée plus limitée*, parce qu'elle ne concerne que le traitement des données à caractère personnel et que les autres dimensions de la protection de la vie privée ne sont pas prises en considération.

Tous les types d'activités dans le secteur public ou privé sont actuellement liées d'une façon ou d'une autre à la collecte et au traitement de données à caractère personnel. La protection des individus (citoyens, consommateurs, travailleurs, etc.) contre la collecte, l'enregistrement et l'échange abusifs des détails de leur existence personnelle concerne donc aussi leur participation aux échanges sociaux, que ces échanges aient ou non lieu dans l'espace public, et peut également impliquer la protection de la liberté d'expression, la lutte contre la discrimination et la promotion du «fair play» dans les processus décisionnels.

Garanties structurelles

La Convention énonce un certain nombre de «principes de base pour la protection des données» auxquels chaque Partie doit avoir donné effet dans son droit interne avant l'entrée en vigueur de la convention à son égard. Ces principes continuent de former le noyau de toute législation nationale dans ce domaine. Aux termes de la Convention, les données à caractère personnel doivent être «obtenues et traitées loyalement et licitement» et «enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités». Par ailleurs, les données à caractère personnel doivent être «adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées» et «exactes et si nécessaire mises à jour».

D'autres principes de base de la Convention exigent des «mesures de sécurité appropriées» et «des garanties complémentaires pour la personne concernée», comme le droit d'obtenir la communication des données à caractère personnel la concernant, le droit d'obtenir, le cas échéant, la rectification de ces données ou leur effacement, et le droit de disposer d'un recours si ces droits ne sont pas respectés. Le principe de «contrôle indépendant» ne figurait pas dans la Convention à l'origine, ce qui ne l'a pas empêché d'être appliqué massivement dans la pratique, puis d'être ajouté à la Convention sous la forme d'un protocole.

Soyons bien clairs: l'approche de la Convention n'est *pas* que le traitement des données à caractère personnel doit toujours être considéré comme une *atteinte* à la vie privée, mais que, pour assurer la protection de la vie privée et d'autres droits et libertés fondamentaux, tout traitement de données doit *toujours* respecter certaines conditions légales, comme le principe suivant lequel les données à caractère personnel ne peuvent être traitées qu'à des fins légitimes et spécifiées, si et seulement si ce traitement est bien nécessaire à ces fins, et elles ne peuvent être utilisées d'une manière incompatible avec les fins qui justifient leur traitement.

La substance de l'article 8 de la CEDH, qui est de limiter le droit d'ingérence dans la vie privée aux cas exclusifs où une base juridique le justifie et où une cause légitime le rend nécessaire a donc été appliquée à un contexte *plus large*. En outre, selon les dispositions de la Convention, aucune dérogation à ces principes n'est autorisée, à l'exception de ce qui est déjà applicable au droit à la vie privée lui-même.

Différences de contexte

Précisons que cela ne peut bien fonctionner en pratique que si le système de poids et contrepoids – qui nécessite certaines conditions substantielles, l'existence des droits individuels, des dispositions en vue d'assurer une procédure conforme et une surveillance indépendante – est suffisamment flexible pour tenir compte de la variabilité des contextes et est appliqué avec vision et en tenant compte des intérêts des personnes concernées et des autres parties prenantes. Dans cette perspective, le droit au respect de la vie privée tel qu'il est prévu à l'article 8 de la CEDH continue de jouer un rôle important en toile de fond, pour certaines mesures particulières plus intrusives.

À l'époque, les dispositions de la Convention n'étaient pas destinées à être applicables directement ou intégrées dans le contrôle judiciaire. Depuis 1997, la Cour européenne des droits de l'homme a cependant statué dans une série d'affaires que la protection des données à caractère personnel revêt une «importance fondamentale» pour le droit au respect de la vie privée, tel que garanti par l'article 8 de la CEDH, et elle a également tiré de la Convention des critères lui permettant de déterminer dans quelle mesure ce droit avait été violé. Ceci suggère que la Cour est de plus en plus encline à juger du respect de la Convention - en tout cas pour les «données sensibles» - dans le cadre de l'article 8 de la CEDH.

La Convention a joué un rôle majeur dans l'orientation prise par les législations dans la plupart des États membres du Conseil de l'Europe. Dans ce contexte, la question de la «protection des données» a été considérée dès le départ comme un sujet de grande importance structurelle pour les sociétés modernes, où le traitement des données à caractère personnel a pris une place de plus en plus importante. La Convention est en cours de révision et nous reviendrons sur ce thème dans un contexte plus large.

Harmonisation

Bien que le Conseil de l'Europe ait très bien réussi à mettre la question de la «protection des données» à l'ordre du jour et à définir les principaux éléments d'un cadre juridique, il a moins

bien réussi à assurer une meilleure cohérence dans l'Union européenne. Certains États membres ont tardé à mettre la Convention en œuvre, tandis que d'autres qui l'ont fait sont arrivés à des résultats variables et ont même, dans certains cas, imposé des restrictions sur les flux de données vers les autres États membres.

La Commission européenne a donc craint que ce manque de cohérence n'entrave le développement du marché intérieur dans une série de domaines – impliquant la circulation des personnes et des services – dans lesquels le traitement des données à caractère personnel était appelé à jouer un rôle de plus en plus important. À la fin de l'année 1990, elle a déposé une proposition de directive visant à harmoniser les législations nationales dans le domaine de la protection des données dans le secteur privé et dans la plus grande partie du secteur public.

À l'issue de quatre années de négociations, l'actuelle directive 95/46/CE a été adoptée avec un double objectif. En premier lieu, elle exige de tous les États membres qu'ils assurent, conformément à la directive, la protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel. En deuxième lieu, elle prévoit qu'ils ne peuvent ni restreindre ni interdire la libre circulation des données à caractère personnel entre les États membres pour des raisons relatives à cette protection. Ces deux obligations sont étroitement liées entre elles. Elles visent à créer un haut niveau de protection équivalent dans l'ensemble des États membres en vue d'obtenir un développement équilibré du marché intérieur.

La directive partait des principes de base de la protection des données, tels qu'énoncés dans la Convention 108 du Conseil de l'Europe. En même temps, elle précisait ces principes et les complétait par d'autres préalables et conditions. Cependant, comme la directive recourait à des concepts formulés de manière assez générale et à des normes ouvertes, elle laissait quand même une marge d'appréciation assez large aux États membres pour sa transposition. Il en a résulté que la directive a permis une meilleure cohérence entre les États membres mais certainement pas de parvenir à des solutions identiques ou parfaitement cohérentes.

Plus de substance

La directive actuelle comprend des critères permettant d'évaluer la légalité des traitements de données. Le traitement des données à caractère personnel n'est autorisé que si la personne concernée a *indubitablement* donné son consentement, s'il est *nécessaire* à l'exécution d'un contrat auquel la personne concernée est partie ou au respect d'une obligation légale, à

l'exécution d'une mission d'intérêt public, à la sauvegarde de l'intérêt vital de la personne concernée ou à la protection de l'intérêt légitime poursuivi par le responsable du traitement, à condition que ne prévale pas l'intérêt de la personne concernée. Cela nécessite un examen subtil des différentes phases du traitement des données et implique la nécessité pour les responsables de tenir compte de cette analyse en temps opportun.

Un autre élément de la directive est l'obligation pour le responsable de toujours fournir à la personne concernée, sauf si elle en dispose déjà, des informations sur son identité, les finalités du traitement et les autres informations pertinentes, pour autant que «compte tenu des circonstances particulières dans lesquelles les données sont collectées», ces informations supplémentaires sont «nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données». L'omission de ces informations peut rendre la collecte des données illégale, avec toutes les conséquences qui en résulteront.

La directive prévoit en outre la mise en place d'autorités chargées de surveiller la conformité des législations nationales sur leurs territoires respectifs, autorités qui seront investies d'un certain nombre de missions et de compétences spéciales, qu'elles seront tenues d'exercer «en toute indépendance». Ces autorités collaborent de plus en plus étroitement dans l'exécution de leurs missions, entre autres dans le cadre du groupe de travail Article 29 sur la protection des données ayant un statut consultatif et indépendant au niveau européen.

Portée internationale

La directive s'applique en premier lieu au traitement de données à caractère personnel effectué «dans le cadre des activités d'établissement» d'un responsable sur le territoire de l'un des État membres de l'UE. Le lieu où se produit le traitement n'a à cet égard pas d'importance. Ce critère est également déterminant pour la portée de la législation nationale au sein de l'UE. Si le responsable n'a pas de lieu d'établissement dans l'UE, la loi applicable est celle de l'État membre dans lequel les moyens utilisés aux fins de traitement des données sont situés.

La directive applique également le principe que les données à caractère personnel ne peuvent être transférées que vers des pays tiers qui garantissent un niveau de protection adéquat. À défaut, le transfert n'est autorisé que dans certaines situations.

Ces dispositions s'appliquent à une réalité complexe dans laquelle la question se pose de plus en plus souvent, tant au sein de l'UE que par rapport aux pays tiers, de savoir quel droit est applicable et qui est responsable de son application.

Ceci soulève de nouvelles questions concernant l'internet - au sujet de la position des sites web, des moteurs de recherche, des réseaux sociaux et des techniques modernes de publicité – et aussi concernant les flux de données au sein des entreprises multinationales, la sous-traitance des services et l'informatique en nuage. Dans la pratique, une protection adéquate est de plus en plus souvent assurée par les «règles d'entreprise contraignantes», qui sont autant de codes de conduite définis et promus par les entreprises, qui satisfont à des exigences spécifiques et sont considérés comme suffisamment efficaces par les contrôleurs compétents.

Jurisprudence pertinente

La directive a été transposée par tous les États membres dans leur législation nationale, y compris par les nouveaux États membres pour lesquels cette transposition était une condition d'adhésion. La Commission a déjà lancé plusieurs actions en justice pour mauvaise exécution de la directive. La première action a concerné l'un des États membres ayant la plus longue expérience dans ce domaine: l'Allemagne. En mars 2009, La Cour de justice de l'Union européenne a pourtant arrêté que l'exigence d'une «indépendance complète» signifie qu'une autorité de contrôle doit être exempte de *toute* influence extérieure. Cet arrêt a récemment été confirmé et précisé dans une affaire contre l'Autriche.

D'autres arrêts importants ont déjà été rendus par la Cour de Justice sur le cadre juridique existant pour la protection des données à caractère personnel. Ainsi, la Cour a, dans ses premiers arrêts sur la directive 95/46/CE, affirmé que celle-ci possède un large rayon d'action qui ne dépend pas d'un lien direct avec le marché intérieur. Ceci signifie que la directive s'applique aussi bien à un litige dans le secteur public d'un État membre qu'au site web d'une institution ecclésiastique ou caritative. Dans ce dernier cas, il a été précisé que la directive s'applique en principe à l'internet, même si le simple fait que des données à caractère personnel sont disponibles sur un site web n'implique pas automatiquement que les dispositions sur les flux de données avec les pays tiers s'appliquent.

Lorsque la directive s'applique dans un domaine du champ d'application de l'article 8 de la CEDH, elle doit être interprétée en tenant compte de cette disposition. Dans cette perspective, la Cour a opéré une distinction entre les traitements de données susceptibles de porter ou non

atteinte à l'article 8 de la CEDH. Les premiers s'appliquaient à une réglementation qui obligeait les employeurs à fournir à un organisme public certaines données concernant leurs salaires. Le traitement de ces données par l'employeur lui-même ne posait en principe pas de problème, tant que les règles de la protection des données étaient respectées. Cette approche cadre avec la distinction entre «la vie privée» et «la protection des données à caractère personnel» dans l'évolution juridique, comme cela a été mentionné précédemment.

Une réforme nécessaire

La directive 95/46/CE constitue toujours l'élément principal du cadre juridique européen pour la protection des données, mais elle fait désormais l'objet de réformes considérables. Il y a près d'un an, le 25 janvier 2012, la Commission européenne a présenté un ensemble de mesures visant à actualiser et à moderniser le cadre juridique européen actuel. Entre-temps, des discussions sur les éléments de cet ensemble de mesures ont eu lieu au Parlement européen et au Conseil.

Pourquoi cette révision? Pour trois grandes raisons. La première est effectivement la nécessité évidente de mettre à jour le cadre actuel, et en particulier la directive 95/46/CE, qui en constitue la pierre angulaire. En l'occurrence, «mettre à jour» revient à faire en sorte que cette directive demeure *efficace* dans la pratique.

Lorsque la directive a été adoptée, l'internet en était encore à ses balbutiements. Aujourd'hui, dans un monde de plus en plus numérisé, nous avons également besoin de garanties plus solides permettant une protection plus efficace. Les défis que constituent les nouvelles technologies et la mondialisation nous incitent immanquablement à faire preuve d'imagination pour proposer des innovations en vue d'une protection plus efficace.

La deuxième raison, c'est que le cadre actuel a abouti à la *diversité* et la *complexité*, ne fût-ce que parce qu'une directive doit, par nature, être transposée en droit national. Nous en sommes donc arrivés à 27 versions différentes de principes fondamentaux identiques. C'est tout simplement excessif, sans oublier les coûts et la perte d'efficacité que cela engendre.

En d'autres termes, nous devons accélérer l'harmonisation en renforçant le système et en le rendant plus efficace dans la pratique, mais aussi plus *cohérent*. Ainsi, nous pourrons réduire cette diversité et cette complexité *qui ne mènent à rien*.

La troisième raison concerne le nouveau cadre institutionnel de l'UE. Entré en vigueur il y a quelques années, en décembre 2009, le traité de Lisbonne place instamment l'accent sur les droits fondamentaux. L'article 8 de la Charte des droits fondamentaux prévoit un droit séparé à la protection des données à caractère personnel, tandis que l'article 16 TFUE propose une nouvelle base juridique horizontale en matière de protection des données garantissant une protection complète dans tous les domaines d'action de l'UE, que ce soit le marché intérieur, l'application des lois ou pratiquement tous les autres composants du secteur public.

La révision du cadre vise donc à mettre en place une protection des données à caractère personnel renforcée, plus efficace, plus cohérente et plus *exhaustive*.

Un pas de géant en avant

Nous disposons maintenant d'un ensemble comprenant au moins deux propositions principales: une directive destinée – pour dire les choses succinctement – au domaine d'application des lois, et un règlement directement applicable pour ce qui relève encore de la directive 95/46 concernant les domaines commerciaux et le secteur public, autre que l'application des lois.

J'ai applaudi à cette proposition de règlement sur la protection des données en la qualifiant de «pas de géant en avant» vers une protection des données à caractère personnel plus efficace et plus cohérente dans l'UE, mais j'ai également demandé que plusieurs aspects importants en soient clarifiés et améliorés. Les personnes intéressées peuvent retrouver l'avis de fond du CEPD du 7 mars 2012 sur notre site, ainsi que tous les documents relatifs à la question.

Toutefois, l'architecture même de ce train de propositions – une directive et un règlement – met en évidence leur manque d'exhaustivité. Et à y regarder de plus près, c'est effectivement là que le bât blesse: le niveau de protection est sensiblement plus faible dans la proposition de directive que dans la proposition de règlement.

Il est possible d'analyser la situation au cas par cas, mais l'échange de données entre des entités publiques et privées, par exemple les autorités chargées de l'application de la loi et les banques, la téléphonie, les voyages, etc. est en pleine expansion, et un déséquilibre aura des conséquences concrètes à une échelle plus large.

Continuité et changement

En ce qui concerne le règlement, il importe que vous gardiez à l'esprit quelques messages essentiels.

Tout d'abord, en dépit de son caractère novateur, le règlement se caractérise par une forte continuité. Tous les concepts et principes fondamentaux actuels sont maintenus, malgré certaines clarifications et innovations. Par exemple, le texte insiste à présent davantage sur la minimisation des données, en somme sur la nécessité de ne pas traiter plus de données que nécessaire. De même, le respect de la vie privée dès la conception («privacy by design») est désormais reconnu comme un principe général. En outre, le texte apporte des précisions relatives au consentement: *lorsque* le consentement est nécessaire, il doit être réel et explicite.

L'innovation majeure consiste en «une protection des données plus efficace dans la pratique». Comme nous le verrons, il s'agit d'insister fortement sur la mise en œuvre des principes et sur l'exécution des droits et des obligations, pour veiller à ce que la protection soit assurée dans la pratique.

En même temps, le règlement prévoit la simplification et la réduction des coûts. Un exemple typique est la suppression de la notification préalable des opérations de traitement. Elle reste nécessaire dans les seules situations qui présentent un risque spécifique. Le règlement instaure également un guichet unique pour les entreprises disposant de sièges dans différents États membres, ce qui suppose l'instauration d'une autorité de contrôle centrale, agissant en étroite coopération avec les autres autorités compétentes.

Un règlement directement contraignant offrira évidemment également une harmonisation nettement plus large - en *principe*: une seule règle applicable dans tous les États membres – et une plus grande cohérence. En soi, il permet également aux entreprises actives dans différents États membres de simplifier leurs obligations et de réduire considérablement leurs coûts.

Portée générale

Permettez-moi d'insister sur le fait que la proposition de règlement a une portée générale: elle s'appliquera au secteur privé comme au secteur public. Ceci est tout à fait en phase avec ce qui est prévu par la directive actuelle (directive 95/46/CE). La possibilité d'opérer une distinction systématique entre secteur public et secteur privé dans cette directive avait été explicitement examinée et rejetée.

Cette approche globale de la directive actuelle a été rendue possible par le fait que certaines dispositions (en matière de missions publiques) concernent davantage les pouvoirs publics, tandis que d'autres (en matière de contrats ou d'intérêts légitimes) concernent davantage les acteurs privés.

La CJUE a clairement expliqué que la directive actuelle s'applique également au secteur public d'un État membre. Elle a toutefois souligné que le droit national ne peut constituer un motif légitime justifiant le traitement que s'il respecte les droits fondamentaux.

Cette position est renforcée par l'article 8 de la Charte des droits fondamentaux, qui prévoit désormais la reconnaissance explicite du droit à la protection des données à caractère personnel, et par l'article 16 TFUE, qui offre une base juridique horizontale explicite pour l'adoption de règles sur la protection des données à caractère personnel, au niveau européen comme dans les États membres, lorsque ceux-ci agissent dans le champ d'application du droit de l'UE.

Parallèlement, j'ai encouragé une analyse plus pointue de la relation entre le droit de l'Union européenne et le droit national sur la base de la proposition de règlement. Croire que le règlement remplacera purement et simplement la législation nationale en la matière est une erreur. Le droit national et le droit européen coexisteront et interagiront d'au moins quatre manières différentes. Pensons notamment au fait que le règlement complétera le droit national qui respecte entièrement les droits fondamentaux.

À cet égard, nous devons également examiner très minutieusement si, et le cas échéant où et comment le règlement doit accorder une plus grande place à la spécification de ses dispositions dans le droit national. En tout état de cause, j'estime qu'il n'est pas utile d'envisager une transformation du règlement en deux instruments juridiques différents, l'un pour le secteur public, l'autre pour le secteur privé ou commercial. Bien au contraire, un tel changement aurait des conséquences *désastreuses*, à la fois pour l'efficacité et pour la cohérence du nouveau cadre, en particulier pour les services frontaliers et inter-frontaliers.

S'agissant de la substance du règlement, celui-ci renforce le rôle des partenaires-clés, à savoir les personnes concernées, l'organisation responsable et les autorités de contrôle.

Contrôle des utilisateurs

La première perspective peut également être perçue comme un renforcement du contrôle des utilisateurs. Les droits actuels des personnes concernées ont été préservés mais surtout consolidés et étendus.

L'exigence relative au consentement a été clarifiée et le droit d'objection a été renforcé. Les moyens mis en œuvre pour veiller au respect de ces droits dans la pratique sont également renforcés et la transparence mise en exergue. Par ailleurs, une disposition introduit non pas un recours collectif à l'américaine, mais une action en nom collectif, à savoir que des organisations pourront intervenir au nom de leurs membres ou de leurs parties prenantes.

Vous avez certainement entendu parler à maintes reprises du «droit à l'oubli», qui consiste principalement à effacer les données lorsqu'il n'existe pas de raison suffisante de les conserver. De même, le droit à la portabilité des données est fondamentalement une spécification du droit actuel de demander une copie de toute donnée à caractère personnel.

Responsabilité

L'accent est principalement placé sur la responsabilité réelle des organisations chargées de la gestion des données. La responsabilité n'est pas une notion qui n'intervient qu'*à la fin*, en cas de problème. Il s'agit au contraire d'une obligation de développer une *gestion correcte des données* dans la pratique. Cette responsabilité est traduite dans des expressions telles que «prendre toutes les mesures qui s'imposent afin de veiller à la mise en œuvre» et «vérifier et démontrer» que ces mesures «sont toujours efficaces».

Il s'agit là de l'une des principales évolutions. Cela implique aussi que la *charge de la preuve* incombe dans la plupart des cas à l'organisation responsable qui doit, en d'autres termes, prouver l'existence d'une base juridique adéquate, la réalité du consentement et l'efficacité continue des mesures.

Le règlement prévoit également un certain nombre d'exigences spécifiques telles que la nécessité d'une analyse d'impact relative à la vie privée, l'établissement de documentation et la désignation d'un délégué à la protection des données. Certaines de ces dispositions, notamment celles qui concernent la documentation, sont à mon sens trop détaillées et doivent être modifiées pour être plus appropriées. Quelques exceptions figurant dans ces mêmes

dispositions ne se justifient peut-être pas tout à fait. Un meilleur équilibre de cette partie de la proposition pourrait sans doute résoudre ces deux problèmes.

Une disposition générale sur la notification des violations de la sécurité est également prévue. Le droit de l'Union européenne limite désormais cette notification aux seuls fournisseurs de télécommunications.

Surveillance et contrôle de l'application

Un troisième point majeur du règlement concerne la nécessité de renforcer la surveillance et le contrôle de l'application. Les garanties prévues pour l'indépendance complète des autorités de contrôle ont été renforcées, conformément à l'arrêt de la CJUE dans l'affaire contre l'Allemagne.

En outre, le règlement confère aux autorités de contrôle des pouvoirs d'exécution renforcés dans tous les États membres. Les amendes administratives s'élevant à des millions d'euros, et s'inspirant de la concurrence, attirent beaucoup l'attention, mais le message est le suivant: aux grands maux les grands remèdes. De cette manière, la protection des données figurera à un rang plus élevé parmi les priorités à l'ordre du jour des conseils d'administration des entreprises, pareille évolution mérite d'être saluée.

En réalité, nous constatons déjà une forte tendance de plus en plus de mesures afin de veiller à une application plus stricte des lois: sanctions correctives, amendes administratives et responsabilités renforcées. Cette tendance se poursuivra certainement au cours des années à venir.

La coopération internationale entre les autorités de contrôle est vivement encouragée et facilitée. L'instauration d'une autorité principale pour les entreprises possédant plusieurs sites est accueillie positivement, même si, là encore, ladite autorité n'agira pas seule mais au sein d'un réseau, en étroite collaboration avec d'autres autorités compétentes.

Un autre changement très important est l'instauration d'un mécanisme de contrôle de la cohérence dans le cadre du comité européen de la protection des données, qui doit s'inspirer de l'actuel groupe de travail «Article 29». Ce mécanisme garantira la cohérence des résultats de la surveillance et du contrôle de l'application dans tous les États membres.

Protection globale de la vie privée

Enfin, un dernier élément doit être relevé: la dimension internationale du règlement dans un sens plus large. Le champ d'application du règlement a été clarifié et étendu. Les dispositions s'appliqueront non seulement à tous les traitements relatifs à un site établi dans l'Union européenne, mais aussi aux livraisons de biens et prestations de services sur le marché européen à partir d'un pays tiers ou aux modalités de contrôle du comportement des personnes concernées au sein de l'Union.

Comme vous le constaterez, il s'agit d'une réalité de plus en plus présente dans le monde actuel de l'internet. Mais cette approche est également réaliste et s'appuie sur une réflexion commune en matière de protection des données dans de nombreux pays concernés aux quatre coins du globe.

Toujours en ce qui concerne les aspects internationaux, les dispositions relatives aux transferts de données vers les pays tiers ont été étendues, mais aussi rationalisées et simplifiées à certains égards. Une disposition spécifique relative aux règles d'entreprise contraignantes a été introduite et prévoit également plusieurs simplifications.

Permettez-moi également d'ajouter que les autorités de contrôle mettent en œuvre une coopération internationale à plus grande échelle – par exemple, entre la Commission fédérale du commerce (*Federal Trade Commission*) aux États-Unis et les autorités de contrôle dans l'UE – au sein d'un réseau mondial (GPEN). Grâce à ce réseau, il sera davantage possible de s'occuper des acteurs mondiaux sur l'internet. Ce phénomène s'explique aussi par une convergence croissante des principes et des pratiques de protection des données dans le monde.

Conclusions

En somme, cette proposition mérite, à mon sens, d'être accueillie favorablement, pour autant que certains éléments essentiels soient quelque peu améliorés.

Outre le déséquilibre actuel entre le règlement et la directive en matière d'application des lois, j'ai évoqué la nécessité d'accorder plus de place à l'interaction entre le droit européen et le droit national ainsi que la nécessité de reconsidérer certaines des exceptions en l'espèce, notamment concernant les petites et moyennes entreprises. Il est *essentiel*, selon moi, que les

dispositions générales soient *évolutives* par nature. Des spécifications inadéquates n'entraînent que des exceptions inutiles.

Mais, permettez-moi d'ajouter que, dans une perspective plus large, ces évolutions représentent également une chance immense. Bien qu'il soit nécessaire de réexaminer les dimensions éthiques de la protection des données et de la vie privée, il ne faut pas oublier de relier la nécessité d'une protection plus efficace et plus cohérente de la vie privée et des données à caractère personnel à d'autres sujets importants, comme la relance économique, sur laquelle l'Agenda numérique pour l'Europe et la stratégie Europe 2020 auront probablement une forte incidence.

En tout état de cause, je suis fermement convaincu qu'une «Europe intelligente, durable et inclusive», telle que l'ambitionnent ces programmes politiques, n'est pas possible sans garanties appropriées des droits fondamentaux, en ce compris la protection des données et de la vie privée. C'est la raison pour laquelle cette conférence de haut niveau est si opportune et c'est pourquoi l'endroit où elle se déroule est si bien choisi.

Comme je l'ai déjà évoqué brièvement, l'UE n'est pas la seule à s'efforcer de réformer la protection des données. Le Conseil de l'Europe et l'OCDE (que je n'avais pas encore évoquée) examinent également leurs cadres respectifs. Ces efforts ont jusqu'ici fait l'objet d'une remarquable synergie, ce qui est important pour garantir un bon niveau de cohérence et d'interopérabilité partout dans le monde.

Pour finir, où en sommes-nous à Bruxelles? Des discussions sont en cours au Parlement: un projet de rapport est actuellement sur la table au sein de la commission LIBE. Le Conseil devrait remettre ses conclusions sous la présidence irlandaise d'ici le milieu de cette année. La Commission comme le Parlement chercheront certainement à parvenir à des résultats finaux avant la fin de leurs mandats actuels en 2014.

Même si l'avenir est toujours incertain, je m'attends à ce que le règlement proposé aboutisse, avec certaines améliorations, cela va de soi, et je ferai tout mon possible pour y contribuer.

Je vous remercie.