Le portrait[1] – Icônes des libertés individuelles – Peter Hustinx

«De temps en temps, vous devez taper énergiquement du poing sur la table!»

Jeroen Terstegge et Koen Versmissen

Peter Hustinx est arrivé au terme de son deuxième mandat en tant que contrôleur européen de la protection des données (CEPD) en janvier dernier. Il restera néanmoins en fonction jusqu'au 16 octobre prochain, ce qui doit laisser à la Commission suffisamment de temps pour lui chercher un remplaçant. Le départ à la retraite de Peter étant imminent, le moment apparaît opportun pour passer en revue son impressionnante carrière dans le domaine de la protection des données à caractère personnel.

Comment expliquer que vous ayez déployé vos activités dans le domaine de la politique de protection de la vie privée?

C'est un long récit, mais je peux le résumer en deux épisodes. Il y a d'abord eu une période d'intérêt général pour cette thématique, parmi d'autres sujets, qui a duré une petite vingtaine d'années. Elle a été suivie d'une période d'implication pratique qui a commencé par la Chambre d'enregistrement et a été suivie par le Conseil pour la protection des données à caractère personnel (ces deux institutions étant néerlandaises), puis par la fonction de Contrôleur européen de la protection des données que j'ai assumée à temps plein. Initialement, ce sont les études que j'ai réalisées aux États-Unis qui m'ont amené fortuitement vers cette thématique. C'est là en effet que j'ai assisté aux balbutiements de la réflexion sur la problématique du respect de la vie privée. Alan Westin avait déjà écrit un livre à ce sujet en 1967 (*Privacy and Freedom, réd.)*, mais en 1970-1971, j'ai eu l'occasion d'être l'étudiant du juriste Arthur Miller et d'assister à l'atelier qu'il avait organisé sur son ouvrage *The Assault on Privacy* (1971). J'ai trouvé le sujet terriblement intéressant. Lorsque j'ai décroché un poste auprès du ministère de la justice, en 1971, deux séismes venaient de secouer ce terrain: d'une part, le recensement de la population (1971, *réd.*) et, d'autre part, le tollé soulevé par le numéro CPA (administration centrale des personnes, *réd.)*. Le cabinet Biesheuvel de l'époque (M. Hustinx fait à nouveau référence à la situation néerlandaise) avait repris dans son accord gouvernemental une mention à ce sujet précisant que le gouvernement entendait prendre des mesures dans le domaine de la vie privée et mandatait à cette fin la commission Koopmans, dont je suis devenu secrétaire adjoint par la suite. J'ai de ce fait non seulement touché à un stade précoce aux premières tentatives d'ébauche de la législation sur la protection de la vie privée, mais j'ai ainsi aussi contribué parallèlement à ce qui se produisait sur ce terrain au sein du Conseil de l'Europe (convention no 108, *réd.*).

À la fin des années 1980, lorsque le dossier de la loi sur la protection des données à caractère personnel (Wet Persoonsregistraties) a été clôturé, je me suis essentiellement occupé, au ministère, de droit pénal et de procédure pénale et de

[1] Cet entretien est paru dans «*Privacy & Compliance*», une revue spécialisée destinée aux professionnels, 01/2014, pp. 4-13.

droit administratif. Deux années plus tard cependant, lorsque le premier président de la Chambre d'enregistrement, Klaas de Vries, a démissionné, j'ai été poussé au-devant de la scène. Je me suis alors demandé si, vingt ans plus tard, c'était toujours ce que je désirais, mais entre-temps, il m'était apparu comme une évidence que cette question avait des conséquences profondes et une grande importance et qu'il ne me déplairait pas d'y contribuer. Le fait qu'il s'agirait au début non seulement des principes, pour ne pas dire du contenu du droit, mais aussi très vite de la question des moyens à utiliser pour que cela fonctionne, a encore pesé dans la balance. Cela devait-il se faire via le droit privé, via le droit pénal ou via le droit administratif? Et quelles sont les institutions requises à cette fin? Au sein de la commission d'État Koopmans, on a suggéré d'instaurer une chambre d'information. Faisant suite à la vague de déréglementation qui a eu lieu cette année-là, il m'est apparu intéressant de réfléchir à une chambre qui serait efficace et ne pourrait en outre pas être trop onéreuse. Le champ d'action était, par ailleurs, très vaste, touchant non seulement la justice, mais aussi les soins de santé, les télécommunications, les transports, la sécurité sociale et les registres de population.

Le 1er juillet 1991, c'est-à-dire au moment précis où les Pays-Bas assumaient la présidence du Conseil et à l'époque où le projet de directive 95/46/CE se trouvait sur la table à Bruxelles, j'ai été nommé président de la Chambre d'enregistrement. La Commission européenne avait proposé une directive fortement marquée de l'empreinte allemande, qui établissait une distinction claire entre le secteur privé et le secteur public. Sous la présidence néerlandaise, il a été décidé à l'époque de fondre le tout en un seul régime. J'ai participé de près aux discussions et je me suis ensuite glissé tout à fait naturellement dans le rôle du président du groupe de travail de l'article 29. Par la suite, j'ai occupé la présidence du conseil pour la protection des données à caractère personnel et j'ai enfin été nommé en tant que CEPD.

Vous avez aussi participé de près à l'élaboration de la politique européenne.

Dans le contexte européen, c'est surtout le Conseil de l'Europe qui a joué un rôle important en attirant l'attention sur ce sujet sur la base d'un programme relatif aux droits de l'homme. Le Conseil s'intéressait essentiellement à la question sous l'angle de l'élaboration d'une législation, et pas tellement sous l'angle de l'économie ou de la technique. On s'interrogeait certes sur l'influence que la technologie aurait sur les droits de l'homme. On présumait déjà à l'époque que la technologie aurait une influence profonde. Mais on pensait que le problème de la protection des données à caractère personnel se situait quelque part entre la vie privée et la liberté d'information. Rien n'était toutefois couché sur papier à ce sujet. On voulait, par conséquent, savoir quels étaient pour l'heure réellement les principes de l'usage raisonnable des équipements informatiques, ce qui a conduit, préalablement encore à la convention no 108, à la formulation de deux recommandations. La première portait sur le secteur privé. On pouvait clairement lire sur papier quels devaient être ces principes. La deuxième était tournée vers le secteur public, mais contenait des règles spéciales concernant la position particulière des pouvoirs publics tels que la police. Ces deux recommandations ont été à la base de la convention no 108. Celle-ci imposait aux États membres une obligation de transposition en droit national. La Commission européenne s'inquiétait à l'époque de la diversité qui résulterait d'une telle transposition. Les deux premières années des négociations sur la convention, nous les avons consacrées à l'établissement de la structure principale de la

convention. Le reste du temps a été consacré aux règles régissant les transferts de données à caractère personnel (article 12), au droit applicable et à la juridiction nationale. Ces deux derniers points n'ont toutefois pas été retenus dans la convention, étant donné qu'à l'époque ils étaient encore trop complexes. Et ils le sont du reste encore aujourd'hui.

Lorsque la convention fut prête, la question qui s'est posée ensuite a été de déterminer la signification précise de ces principes généraux dans des domaines concrets. Plusieurs corrections ont ainsi été apportées à la convention, par exemple à la notion de «données à caractère personnel». Initialement, le texte faisait référence à une «identification facile», mais il a été reformulé de manière à être plus neutre. Le principe de la finalité y a été repris très tôt. Il s'agissait également d'une conséquence logique de la réflexion contenue dans la convention européenne des droits de l'homme. Toute violation d'un droit fondamental est liée à un objectif, une dimension et une base légale. L'étape franchie par le droit sur la protection des données a été d'imposer que le traitement des données à caractère personnel repose toujours sur une base légale, peu importe que la violation concerne ou non un droit fondamental. Voilà pourquoi j'estime personnellement que la vie privée et la protection des données sont deux choses fondamentalement très différentes bien qu'il y ait des chevauchements. Ce qui est étrange, c'est que la reconnaissance que cela a des conséquences non seulement pour la collecte et la conservation, mais aussi pour l'utilisation – autrement dit, l'idée de l'incompatibilité – n'est arrivée que tardivement. Mais cette reconnaissance a alors fait naître immédiatement le doute: n'est-il pas un peu trop strict de ne vouloir poursuivre qu'un seul et même objectif? Ce terme «incompatible» se retrouvait déjà un peu dans la jurisprudence des droits de l'homme, et les instructions pour la fonction publique (*Aanwijzingen voor de Rijksdienst*), qui étaient une forme d'autoréglementation avant l'adoption de la loi sur la protection des données à caractère personnel, reconnaissaient déjà le principe de l'incompatibilité. On pourrait fort bien comparer le développement des principes de la protection des données à une procédure Wiki; il y avait partout en Europe toute une série de personnes qui collaboraient pour parvenir, au moyen d'un processus itératif, à des formulations.

Les principes de l'OCDE ont relativement bien résisté aux assauts du temps, mais ils sont de plus en plus remis en cause sous l'influence de développements tels que les Big Data.

Je reconnais bien sûr ces défis, mais je suis aussi surpris par la grande continuité. Rien n'est taillé dans le roc et cela serait, du reste, injustifié. Depuis 1980, une évaluation est organisée tous les dix ans environ et chacune d'elles, sans exception, atteste que les principes conservent tout leur sens. Sur le plan du contenu, les principes de l'OCDE sont en outre comparables à ceux du Conseil de l'Europe. Lorsque l'Union européenne a commencé son examen, l'OCDE et le Conseil de l'Europe ont également décidé de revoir leurs lignes directrices, le cas échéant la convention. L'OCDE avait déjà terminé son examen en juin 2013. Mais lorsque l'on y regarde de plus près, on constate qu'il s'agit en réalité d'une confirmation des anciennes lignes directrices. Les seuls changements sont une définition plus précise du devoir de responsabilité et l'insistance sur la collaboration internationale. Ces conclusions reposaient donc manifestement sur une perspective communautaire. Lorsque vous examinez, par exemple, les propos du président Obama concernant le

respect de la vie privée dans le secteur privé, vous constatez qu'il se base essentiellement sur les mêmes principes. Les Américains parlent de principes renouvelés d'information équitable (*Reinvigorated FIPS* [Fair Information Principles, *réd.*]), mais il s'agit au fond des mêmes principes. Je pense que l'analyse des principes de l'OCDE doit toujours se faire dans un contexte donné et c'est précisément ce contexte qui a fortement évolué au cours des dernières années. Dans certaines cultures, notamment en Allemagne et en Autriche, l'accent est placé excessivement sur l'autorisation. À l'autre bout de l'échelle, vous avez aussi des pays qui estiment que l'autorisation est importante, mais qui la mettent en pratique d'une manière relativement simpliste. Cela sape complètement le système.

Il y a de cela quelques années, par exemple, la Cour européenne a rappelé l'Espagne à l'ordre parce qu'elle avait indûment limité l'intérêt légitime en matière de commercialisation. L'approche espagnole avait pour revers qu'elle s'accompagnait sur l'Internet d'un très grand nombre d'autorisations simples, voire d'abus d'autorisations. On prend volontiers l'autorisation comme motif de justification, mais on préfère ne pas réfléchir à ce qui se produit en cas de refus ou de retrait d'autorisation. Mon conseil est donc le suivant: s'il est trop difficile de demander l'autorisation, mieux vaut ne pas la demander. Pensez à l'exécution d'un contrat, au respect d'obligations légales ou à l'intérêt légitime. Dans ce dernier cas, vous devez également beaucoup réfléchir à la question de savoir pourquoi vous estimez que ce que vous faites est légitime. La question qui se pose est la suivante: la position que j'adopte par défaut et que j'impose aux intéressés est-elle réellement la bonne? Il y a donc des raisons d'étayer la base de l'intérêt légitime par une obligation de responsabilité externe.

Dans le cadre de la directive 95/46/CE, il est manifeste que l'autorisation n'est qu'un motif de justification à côté d'autres motifs qui fonctionnent tous à leur façon. Un système équilibré doit laisser une marge pour inclure l'intérêt légitime. On observe le fonctionnement de ces équilibres dans l'avis sur la limitation de la finalité (WP 203 du groupe de travail «Article 29», *réd*.). Il est également question dans cet avis des Big Data et des Open Data. Je serai le dernier à affirmer que l'application des principes du respect de la vie privée à ces développements s'effectue sans problèmes, mais je ne peux partager l'avis des personnes qui affirment que les principes ne sont plus adéquats. Il ne sert à rien de dire que compte tenu du grand volume de données, l'essentiel est l'utilisation que l'on en fait. L'utilisation, c'est le test et c'est précisément là que la protection doit être très forte, mais je pense que vous devez toujours commencer par la perspective de l'acquisition des données. Une bonne gestion des données commence à présent par une réflexion sur la collecte des données. Si vous y renoncez, il est impossible de trouver les solutions appropriées. Pour ma part, les principes restent valables. Moyennant quelques nuances, il est toujours possible de les appliquer. Mais vous devez toujours être attentif aux équilibres qu'ils contiennent. Vu sous cet angle, l'élément central de la discussion est la répartition des responsabilités pour l'application des principes. Pour moi, la révision de la législation européenne en matière de la protection des données est une clarification des principes qui a essentiellement pour but de garantir leur respect dans le contexte concerné.

Comment évaluez-vous votre période d'activité en tant que CEPD?

Faire quelque chose en partant de rien a été, pour moi, réellement enrichissant. Lorsque j'ai pris mes fonctions, il n'existait absolument rien. Pas même un budget! La principale avancée positive est que le CEPD est devenu aujourd'hui une institution et compte plusieurs réalisations à son actif. Le règlement instituant la fonction du CEPD (règlement (CE) n° 45/2001, *réd.*) est un peu le pendant de la loi sur la protection des données à caractère personnel, mais à l'échelle européenne. On y trouvait trois lignes stratégiques: 1) le contrôle, 2) la consultation dans les domaines politique et législatif et 3) la coopération avec les collègues responsables du contrôle. La première tâche principale consiste à veiller au respect du règlement par les institutions européennes. Au début, nous étions confrontés à la même réticence qu'au niveau national (absence de priorité, absence de personnel disponible, etc.). Nous avons eu recours à l'obligation de rendre des comptes comme mécanisme afin de laisser une marge de manœuvre aux responsables tout en leur imposant de se justifier. Nous recourons également à la technique de l'étalonnage des performances pour montrer comment les institutions se profilent les unes par rapport aux autres. Et il apparaît qu'elles ont réellement accompli des progrès.

Des améliorations restent bien entendu toujours possibles, mais globalement, la plupart des institutions obtiennent de bons résultats. Nous utilisons les résultats de l'étalonnage des performances pour mettre en évidence la sous-performance. Nous citons nommément les institutions concernées. Bien sûr, elles ne trouvent pas cela agréable, mais elles font l'objet d'une attention soutenue de notre part. Nous leur rendons visite, nous établissons avec elles une feuille de route afin de leur permettre de s'améliorer et nous leur demandons de rendre compte des progrès réalisés tous les mois. Pour ma part, j'estime que la fonction de contrôle se déroule très bien.

Vous avez également interféré énergiquement avec la législation en Europe.

J'ai considéré la consultation dans les domaines de la législation et de la politique comme une tâche stratégiquement très importante et je m'y suis donc consacré avec beaucoup d'énergie. Il fallait agir sans retard et contribuer activement à ce qui passe ici à Bruxelles. Cette attitude est à mettre en relation avec mes antécédents. La consultation est ainsi devenue notre deuxième tâche principale. Nous avons élaboré une méthodologie à cette fin. Chaque année, nous analysons le programme de la Commission. Nous l'évaluons sur le plan de la pertinence et nous indiquons grosso modo ce que nous attendons. Et tant que la Commission en est encore au stade de la réflexion, nous sommes prêts à lui fournir des conseils à sa demande. À partir du moment où la proposition est adoptée, elle doit nous la soumettre et nous formulons un avis destiné au public. Nous avons commencé à travailler avec cette méthode peu après les événements du 11 septembre et à l'époque, la vie privée ne faisait pas encore partie des thèmes de prédilection du troisième pilier (coopération avec la justice et les services de police, *réd.*). Malgré cela, nous sommes parvenus à imposer la méthode d'un bout à l'autre de la procédure d'élaboration de politique et à ma grande satisfaction, pendant toutes ces années, la Commission, le Parlement et le Conseil ont apporté activement leur concours. Il aurait pu en être autrement.

Il vous est arrivé de vous montrer très critique à l'égard de certains dossiers.

De temps en temps, vous devez taper énergiquement du poing sur la table. Pas trop souvent, car autrement on ne vous prend plus au sérieux. Mais effectivement, ces dernières années, nous l'avons fait très énergiquement une douzaine de fois et cela a bien fonctionné! Le règlement m'offre en outre la possibilité de saisir la Cour de justice en cas de litige. Pour les juristes, cette disposition était contestable. En réalité, seules les institutions classiques sont autorisées à le faire. Toutefois, lorsque l'affaire des données relatives aux passagers (PNR) est arrivée devant la Cour, j'ai estimé que le moment était venu d'intervenir. Et la Cour m'a suivi. Elle a en effet estimé que le CEPD avait pour mission de promouvoir le respect de la législation dans toute sa portée. Je n'ai bien sûr pas manqué de le souligner. Depuis lors, la consultation s'est située dans une dynamique différente. Nos avis ont été pris plus au sérieux, précisément parce que nous étions en mesure de nous adresser à la Cour. Cela a été un concours de circonstances incroyable.

Et la troisième fonction?

Il s'agit de la coopération avec les collègues responsables du contrôle. Cette fonction s'est développée progressivement. Au sein du groupe de travail de l'article 29, je suis bien entendu de loin le membre le plus ancien. Lorsque vous faites connaître vos vues de manière sélective, vous parvenez à de bons résultats. Nous avons présenté nos points de vue sur les aspects les plus stratégiques. Pensez par exemple aux principes clés de la protection des données et aux BCR. Je pense que cette façon de faire a progressivement amené la Commission à proposer la participation des services du CEPD aux travaux du comité européen de la protection des données (EDPB).

Êtes-vous satisfait des résultats que vous avez atteints ?

Oui, je suis raisonnablement satisfait de ce que j'ai réalisé en tant que CEPD. Bien sûr, il y a aussi eu quelques sources d'insatisfaction. La rétention des données, par exemple. Sur ce point, j'avais émis un avis négatif, mais je n'ai pas été suivi. En revanche, je suis tout à fait satisfait que dans l'affaire Irlande/Autriche, la Cour nous a invités à venir plaider alors que nous n'étions pas autorisés à intervenir. Reste maintenant à savoir ce que la Cour va faire de notre avis. Un autre point fort a été le moment où la Commission, après que je lui aie indiqué qu'une modification de la directive 95/46/CE était inévitable, a fini par la réaliser et je n'ai pas laissé passer l'occasion par la suite d'apporter une contribution à cette révision.

Quel est le plus grand défi que votre successeur va devoir relever?

Il reste un certain nombre de choses à terminer. La révision du cadre européen de la protection des données, par exemple. Mais il y a également des risques. Plus vous sortez de l'ombre, plus la critique augmente. Nous ne sommes pas une institution politique et pourtant il nous arrive d'intervenir avec fermeté! Dans ces cas-là, mieux vaut ne pas se trouver au mauvais endroit au mauvais moment. Cela peut avoir de fâcheuses conséquences! La fonction de CEPD réclame beaucoup de doigté.

Compte tenu de vos réussites en tant que CEPD, la recherche d'un bon successeur risque d'être une tâche ardue.

Malheureusement, cela ne me réjouit pas. La question est à présent sur la table du Conseil et du Parlement. Ce sont eux qui décident de poursuivre la procédure ou d'y mettre un terme. Mais ils parviendront à trouver quelqu'un qui pourra prendre le relais!

Chaque institution européenne doit avoir au minimum un DPD. Collaborez-vous avec ces DPD?

Oui, nous collaborons beaucoup avec les DPD. Trois fois par an, nous nous réunissons avec tous les DPD. En dehors de cela, nous travaillons également avec eux sur une base mensuelle, hebdomadaire ou même quotidienne, notamment par courriels ou entretiens téléphoniques. Nous informons les DPD dans toutes les affaires en leur adressant nos courriels en copie. À un stade précoce, nous avons également positionné les DPD en tant que partenaires stratégiques pour les responsables. Les DPD sont informés bien à l'avance de nos activités. Nous organisons ainsi d'avance l'implication du DPD dans les affaires qui le concernent. La Commission, par exemple, compte deux DPD, mais ceux-ci sont entourés de toute une série de coordinateurs de la protection des données. 35 pour être précis, soit un par DG! Ces 30 à 40 personnes, dont certaines travaillent à temps partiel, constituent la clé de voûte de la mise en pratique de l'obligation de rendre des comptes. Nous avons maintenu avec les DPD une distance suffisante pour leur permettre de fonctionner de la façon qu'ils jugent appropriée, mais nous entretenons avec eux des liens suffisamment étroits pour leur apporter notre appui lorsque cela s'avère nécessaire.

Le règlement exige diverses mesures de la part des organisations, par exemple l'engagement d'un DPD. Pour d'autres aspects du respect des règles, de telles exigences ne s'appliquent généralement pas, ce qui donne parfois lieu à une certaine résistance au sein des organisations. Que fait un DPD pour être pris au sérieux?

Cela est manifeste. Telle est la raison pour laquelle nous avons rédigé une note sur le positionnement des DPD et y avons abordé des aspects tels que l'indépendance du DPD, la fonction à temps partiel de DPD et la position hiérarchique du DPD (niveau dans l'organisation?). Outre cette note, les DPD ont élaboré, avec mon soutien, un code de déontologie qui précise ce qu'un DPD doit faire lorsqu'il vient d'être nommé, quelles doivent être ses priorités, etc. Un DPD doit organiser le *buy-in*. Il doit établir un programme et obtenir un appui pour celui-ci. Ce programme doit être en adéquation avec le mandat de l'organisation. Quant à l'organisation, elle doit pouvoir comprendre les possibilités d'amélioration que cela comporte pour elle. Bien entendu, il y a des obligations, mais une bonne politique en matière de protection de la vie privée peut aussi être porteuse de possibilités. Un DPD ne doit donc jamais rester attentiste. Les DPD qui réussissent sont ceux qui relèvent ce défi. Je pense, du reste, qu'il n'est pas exact d'affirmer que des prescriptions précises font défaut pour d'autres aspects. Pensez, par exemple, à la comptabilité et à l'obligation de rendre des comptes pour lesquelles il existe des règles de longue date. Mais des règles comparables existent également dans les domaines plus récents. Je pense

par exemple à la comptabilité des substances chimiques et des émissions. Des prescriptions précises s'appliquent également dans le domaine des conditions de travail. En principe, la révision de la directive s'appuie sur la même réflexion.

Le fait est que c'est dans la pratique que le respect des règles (*compliance*) prend sa forme. La responsabilité n'est pas une définition, mais bien une action. Ceci nous amène à l'obligation de rendre des comptes (*accountability*). Le terme proprement dit n'apparaît pas dans le règlement, mais ces dernières années, les entreprises en ont approfondi tous les éléments et l'on arrivé aux mêmes conclusions: le tout est une question de gestion des données (*data management*). Je suis satisfait, mais en partie seulement, de la façon dont tout cela est prévu dans le règlement. Certains points ont été formulés de façon trop désuète par la Commission, par exemple la détermination de la preuve (obligation de documentation visée à l'article 28, *réd.*). Il est évident que l'on a besoin de preuves, mais il n'est pas indispensable que les organisations fournissent, à tout moment de la journée, une description précise de leurs opérations. Cela se trouvait déjà dans l'obligation de notification. J'ai conseillé de suggérer la prescription d'une méthode pour gérer les opérations. Cette méthode pourra ensuite être standardisée, puis précisée par secteur. Nous œuvrons actuellement à la mise au point d'une approche basée sur le risque, afin que ce type d'obligation puisse fonctionner correctement.

Dans le règlement, les obligations de contrôle désuètes ont, à juste titre, été supprimées. L'obligation de notification des opérations en est un exemple. D'autres obligations ont été introduites en lieu et place, mais l'échelle appliquée n'est pas toujours adéquate. Il aurait été préférable que la Commission décrive les éléments constituants caractéristiques de la responsabilité tels que la prise de mesures, la vérification de leur efficacité et la mise à disposition de preuves pour les étayer. On aurait alors pu décrire les mesures minimales à prendre. Telles qu'elles figurent dans le règlement, les dispositions peuvent se justifier dans un milieu culturel unique, mais il est évident que dans 28 cultures différentes, leur développement risque d'être tout à fait différent. Le défi consiste donc à parvenir à des règles uniformes qui ne seront ensuite pas trop contraignantes, mais qui pourront s'adapter partout. Je crois que sur ce point, nous, c'est-à-dire les membres du Conseil, nous rapprochons sensiblement du but.

Selon moi, les coûts des mesures sont, par ailleurs, fortement exagérés. On ne tient compte ni des bénéfices ni des coûts des frictions. De même, on ne tient pas compte du non-respect actuel des règles. La Commission a secoué les esprits en menaçant d'infliger des sanctions se chiffrant en millions d'euros. Celles-ci sont bien entendu échelonnables, mais elles constituent quand même un moyen extraordinairement efficace pour attirer l'attention dans la salle du conseil. Vous avez alors besoin de contrôleurs capables d'intervenir raisonnablement à ce niveau. Autrement dit, ils doivent récompenser les bonnes pratiques et sévir lorsqu'une faute est commise. Les contrôleurs doivent donc disposer de la compétence non seulement de fractionner les amendes, mais aussi d'exiger une ébauche d'approche et des rapports sur l'avancement des travaux et lier cette exigence à des sanctions afin de suivre les organisations. Il n'est pas possible de le faire pour tous les secteurs économiques. Un contrôleur doit donc pouvoir expliquer pourquoi il intervient dans une affaire concrète.

L’économie numérique est très internationale aujourd’hui. Comment pouvons-nous imposer au monde nos valeurs européennes dans le domaine de la vie privée sans risquer de nous mettre nous-mêmes hors jeu?

Il existe une grande unanimité dans le monde sur les principes applicables dans ce domaine. Prenez, par exemple, les nouveaux principes de l’OCDE. Ceux-ci ont été approuvés par un plus grand nombre de pays que les précédents alors que, de façon surprenante, le résultat final est le même. Je dresse ce même constat lors de conférences internationales. Il existe certes des différences entre la CEAP et l’UE, mais il y a aussi des points communs. En ce qui concerne l’exécution pratique, je pense que nous pouvons parcourir un bon bout de chemin ensemble. Cela est vrai aussi pour l’Amérique, même si on a tendance là-bas à freiner des quatre fers. Ne sous-estimez toutefois pas l’influence que l’Europe a eue — et aura encore — dans ce domaine.

Dès lors, si nous parvenons à bien tirer profit du moment, cela conduira *de facto* à une norme mondiale qui aura une influence énorme. Il existe de nombreux moyens pour pouvoir rendre une telle norme interopérable entre les différents pays. L’un d’eux consiste à partir du principe que les entreprises aspirent à se conformer à une norme, mais ne sont disposées à la mettre en œuvre qu’une seule fois et au coût le plus bas possible. Cette possibilité existe aujourd’hui. Par ailleurs, il existe la formidable puissance de marché de l’Europe. La Federal Trade Commission, aux États-Unis, est devenue, elle aussi, nettement plus active sur le terrain de la protection de la vie privée. Aux États-Unis, à la différence de l’Europe, le non-respect de la politique de vie privée est perçu comme une pratique commerciale déraisonnable, mais ce principe est poussé très loin. Dans plusieurs affaires, la FTC s’est déjà montrée disposée à sanctionner, via le groupe américain, des promesses qui ont été faites en Europe et qui n’ont pas été tenues. Ce n’est pas par hasard qu’ils l’ont fait.

Il existe donc une volonté croissante de collaborer avec l’Europe. À la lumière du marché transatlantique, il s’agit d’une contribution formidable à l’interopérabilité. L’occasion m’a été donnée à plusieurs reprises de présenter le système européen de l’*adequacy* comme une contribution à l’interopérabilité. Nous sommes à la veille d’un nombre de développements substantiels. Pensez, par exemple, à Google qui est mise en examen aujourd’hui dans plusieurs pays. Cela va sans doute déboucher sur une jurisprudence, ce qui est indispensable, car notre monde est de plus en plus intégré.

Comment un responsable de la conformité doit-il se comporter dans les litiges mondiaux?

Le DPD peut veiller à ce que soit élaboré dans le cadre de son organisation un programme qui reprend systématiquement ce genre d’aspects. Il doit faire en sorte que les exigences (mondiales) soient prises en compte dans les produits et services de son entreprise. De petites différences entre les pays et les marchés pourront bien entendu subsister, selon les besoins, mais une approche intégrée doit exister. Lorsque vous travaillez dans une organisation qui accorde une grande importance au respect des données à caractère personnel et qui ne souhaite pas courir le risque de

subir une publicité négative en raison d'une fuite de données ou d'un manque de contrôle, vous devez investir dans une telle approche. Lorsque les activités d'application augmentent, cette approche intégrée n'en devient que plus importante et il s'agirait d'une évolution saine.

Et comment un contrôleur doit-il se comporter face à une telle complexité?

Il incombe au responsable de respecter des règles et il appartient à l'intéressé de faire valoir ses droits. Pour le contrôleur, il est important que le système fonctionne globalement bien. Si les rouages sont grippés, c'est à vous, en tant que contrôleur, qu'incombe la responsabilité d'y remédier. Cela s'applique aussi lorsque les parties se comportent de manière inadéquate d'un point de vue structurel. Le contrôleur ne doit donc pas trop s'arrêter sur les détails, mais ceux-ci doivent quand même être pris en considération. Il doit exister un guichet à cette fin, éventuellement dans un autre cadre.

La difficulté pour le contrôleur est qu'il doit continuer à axer son attention sur le tableau général et intervenir à temps. En tant que contrôleur, vous ne pouvez pas vous laisser piéger dans un tunnel parce que vous êtes trop occupé par les tâches journalières telles que les plaintes, les notifications, etc. Au contraire, vous devez sans cesse vous remettre en question et vous demander si vos préoccupations sont les bonnes et si vous gérez efficacement les rares ressources.

Les contrôleurs plaident pour un renforcement de l'obligation de rendre des comptes, mais dans la pratique, ils s'arrêtent souvent sur des détails insignifiants et n'accordent aucun crédit à ce qui se passe au sein des organisations dans le domaine de la gestion de la vie privée. Les contrôleurs vont-ils réussir à franchir cette étape?

Je l'espère. Plusieurs le font déjà. Et un organisme tel que le comité européen de la protection des données a un rôle à jouer à ce niveau. La situation va devenir de plus en plus cohérente, mais il s'agit d'un processus en croissance. En tant que CEPD, nous travaillons déjà de cette manière. Nous examinons avec le responsable où se situent les risques primordiaux, par exemple le contenu de l'information et son utilisation, où la situation est globalement satisfaisante et où nous devons intervenir parce que les risques sont trop importants.

L'idée du guichet unique et le principe de la proximité sont aujourd'hui d'importants obstacles à l'avancement du règlement. Mais il n'est pas superflu qu'une bonne solution intervienne à ce niveau-là aussi, y compris du point de vue du DPD qui doit conseiller l'organisation sur les règles et les risques. Qu'en pensez-vous?

L'idée du guichet unique et le principe de la proximité sont en effet contradictoires. C'est le sujet autour duquel tournent toutes les discussions aujourd'hui et la réussite ou l'échec du projet de révision en dépend à ce stade. En octobre, nous étions, selon moi, plus près de la solution qu'en décembre. Ces points ne doivent pas être examinés indépendamment l'un de l'autre. Le guichet unique est un excellent concept, mais vous devez faire en sorte qu'il existe un guichet unique pour les entreprises et un guichet unique pour les intéressés. Et comme ceux-ci sont

différents dans des situations transfrontalières, vous devez accepter qu'il n'y ait jamais un seul guichet. L'autorité chef de file n'a pas de compétence exclusive. Vous devez donc envisager celle-ci comme une forme de répartition des tâches. Si vous percevez l'autorité chef de file comme le dirigeant d'une équipe, vous vous rapprochez bien plus de la solution. Et l'inverse est vrai également. Il existe donc selon moi certainement une solution au problème.

En fin de compte, ne s'agit-il pas tout simplement que d'une question de moyens financiers? Vous ne voulez pas que chaque pays puisse imposer distinctement une amende, mais vous désapprouvez lorsque l'amende va en totalité dans les caisses d'un seul pays.

À ce niveau-là aussi, il devrait être possible de faire quelque chose. Si vous êtes logique dans votre plaidoyer en faveur d'une coopération, vous devriez pouvoir déterminer en toute autonomie qu'une amende de 100 millions d'euros, par exemple, soit répartie entre les pays concernés. Cet aspect n'est pas encore fixé dans le règlement, mais si vous voulez résoudre le problème, c'est la voie à suivre. Il est toutefois plus important de se demander ce qu'est en réalité le guichet unique. D'une part, un contrôleur a une mission dans le cadre du guichet unique; d'autre part, il a des compétences déterminées qui ne lui permettent pas de l'exercer. Aujourd'hui, le contrôleur français n'a pas le droit d'effectuer une enquête sur place en Allemagne. Il doit demander la collaboration de son collègue allemand. Dans ce cas, il y a donc coopération sur le terrain de l'enquête et cette coopération peut s'étendre à l'imposition d'obligations. Sous le guichet unique, le règlement génère donc en fin de compte une forme de collaboration. Et il s'agit aussi de la solution pour la proximité. La confiance joue aussi un rôle entre les juges entre eux et les contrôleurs entre eux. Le responsable ne doit pas toujours attendre longtemps avant d'obtenir une décision.

Au sein de l'EDPB, nous pouvons tenter d'accélérer un aspect. L'EDPB pourrait, par exemple, essayer de parvenir à ce qu'une position à laquelle toutes les parties se tiendront soit adoptée dans les six mois. Je comprends qu'à l'ère de l'Internet, six mois puissent paraître une éternité, mais l'enjeu est si important qu'un tel délai se justifie. La proposition avait ceci d'intéressant qu'elle contenait les éléments déclencheurs de procédure qui assuraient qu'une bonne décision soit prise à la base. Un contrôleur qui s'écarte du point de vue de l'EDPB doit justifier son choix, mais un juge n'acceptera pas forcément cette justification d'emblée. Parallèlement, notre proposition apportait également une solution à un autre problème, notamment au rôle trop important que s'était octroyé la Commission, ce que d'aucuns avaient désapprouvé. La solution se trouvait sur la table en octobre de l'année dernière. Ensuite, il y a eu trop de divergences d'opinions, de sorte qu'il est apparu impossible en décembre de parvenir à un accord. Ce problème peut être résolu de diverses manières sans qu'il soit nécessaire de créer un nouvel organe (un contrôleur paneuropéen, *réd*.), ce que personne ne souhaite en réalité. Le paradoxe peut donc être résolu.

Six mois peuvent apparaître acceptables pour une enquête ou une plainte, mais le mécanisme de la cohérence va également s'appliquer à la consultation du contrôleur pour des projets du responsable pour lesquels une analyse de l'incidence sur la vie privée existe déjà. Et six mois, c'est très long.

Pour de tels projets, il est clair que les délais doivent être réalistes. Une entreprise ne peut pas se dire qu'elle a une bonne idée et tenter, au dernier moment, d'obtenir une autorisation. Il est important qu'il existe de bons conseillers pouvant donner l'alarme en temps utile. Il est, par ailleurs, probable que les choses qui apparaissent évidentes et entrent en ligne de compte seront les premières à être soumises au mécanisme de la cohérence *(consistency)* pendant la période transitoire du règlement. À partir du moment où le règlement entre en vigueur, des directives et une politique contrôlée existeront déjà pour les sujets les plus fréquents. Par conséquent, si une entreprise pose une question sensée, une réponse pourra être donnée dans un délai raisonnablement court. Sur ce point-là aussi, il y aura de la progressivité. Mais lorsque les choses se produisent au niveau européen, vous devez le faire dans des proportions adéquates.

Le règlement risque donc d'être appliqué différemment d'un État à l'autre?

La commissaire Reding considère que le règlement est «une loi d'application universelle». Personnellement, je préférerais parler d'une «loi-cadre d'application universelle». Le règlement qui a vu le jour laisse un grand nombre de possibilités d'interprétation sur des aspects importants. Et cela est nécessaire, car le règlement doit permettre la cohabitation des législations de 28 États membres, ce qui est impossible dans une approche dogmatique. Selon le droit européen, un règlement est largement prédominant, mais tout dépend du contenu de ce règlement. Si ce règlement est conçu de manière à permettre cette coexistence, aucun problème ne se pose. Le Conseil y travaille pour l'instant. Le règlement contient des «obligations légales», mais il ne précise pas les obligations concernées. Pensez par exemple à la législation fiscale ou à la législation dans le domaine de la santé et de la sécurité au travail. Celles-ci renferment une foule d'obligations légales concernant le traitement des données à caractère personnel. Si ces obligations sont compatibles avec les droits fondamentaux, elles seront alors considérées comme des obligations légales au sens du règlement. Elles pourront donc coexister. Mais les États membres doivent anticiper le règlement. Dans le cas contraire, la législation locale risque, juridiquement parlant, de devenir inopérante suite à l'entrée en vigueur du règlement, ce que personne ne souhaite. Il faut bien y réfléchir et je pense que la Commission a légèrement sous-estimé la situation.

Dans une optique globale, quel message aimeriez-vous encore adresser à nos lecteurs?

Je commencerai par dire que les professionnels de la protection des données sont un fonds de croissance et qu'ils vont jouer un rôle très stratégique dans le système. Nous allons avoir besoin de tels professionnels à tous les niveaux; pas seulement des juristes, mais aussi de personnes qui disposent d'un bagage technique ou de compétences en gestion.

Deuxièmement, vous ne devez pas rester là à attendre, les bras croisés. Le risque est que chacun tente de son côté de faire émerger un iceberg. Cela ne peut bien sûr pas réussir. Il conviendra donc de réfléchir à un plan qui permettra d'induire progressivement un changement. Vous devrez faire preuve de patience et d'une certaine dose d'imagination. Dites-vous pour vous consoler que partir de rien, c'est précisément ce que j'ai dû faire lorsque j'ai accepté le poste de CEPD. Les succès

que nous avons engrangés jusqu'ici montrent que tout est possible. Et avec un peu de chance et une équipe très enthousiaste, vous pouvez réussir.

Troisièmement, je dirais que ce renouvellement du cadre européen est inévitable. La date à laquelle vous atteindrez la ligne d'arrivée n'est pas encore connue. Soyons honnêtes, nous n'y parviendrons pas avant les élections européennes. Le produit fini ne sera pas non plus tel qu'il aura été introduit, mais il s'en approchera et sera même meilleur. Nous nous consacrons actuellement à plus d'une question, mais c'est d'autant mieux. Nombreux sont ceux et celles qui ne se rendent pas compte de la sensibilité du problème et des grandes problématiques normatives qui l'entourent.

Enfin, en tant que contrôleurs, nous sommes occupés pour le moment à jeter des ponts entre les professionnels conventionnels de la protection des données et toutes ces personnes qui s'occupent du développement de l'Internet, de logiciels, de matériel et de normes. Ces personnes ont subi un choc suite à l'affaire NSA. Nous allons impliquer un nombre de personnes qui sont actives dans le monde du «*privacy-aware internet development*» afin de tenter de parvenir à un effet multiplicateur. Et cela montre que les contrôleurs doivent aussi être créatifs.