Parlement européen

2019 - 2024

Commission des libertés civiles, de la justice et des affaires intérieures

Lundi 25 novembre 2019, de 19 heures à 22 h 30
au Parlement européen
STRASBOURG

Audition du candidat Yann PADOVA

1. Pouvez-vous exposer les raisons pour lesquelles vous vous portez candidat à cette fonction et en quoi vous vous estimez compétent pour la remplir?

Mon parcours professionnel m'a permis d'acquérir **une vision à « 360° » de la protection des données**, matière sur laquelle je travaille **depuis 20 ans**. J'ai d'abord abordé cette matière sous l'angle du Législateur, à l'Assemblée nationale, en travaillant sur la transposition de la Directive 95-46 mais aussi sur différents projets de loi dont celui créant le fichier de suivi des délinquants sexuels. C'est à l'Assemblée nationale, en tant **qu'Administrateur** assujetti à une obligation de **neutralité stricte**, que j'ai appris à travailler avec élus de **tous bords politiques,** ainsi qu'à négocier des solutions de compromis sur des textes de loi. J'ai de nouveau exercé cette mission avec les services de la Commission européenne en travaillant sur les premières versions du RGPD. Et cette **expérience de conseil au Législateur** me semble particulièrement pertinente pour le Contrôleur Européen (CEPD) dans sa fonction auprès du Parlement et du Conseil.

En tant que Secrétaire général de l'autorité de protection des données française (CNIL) ensuite, j'ai mis en place la «nouvelle CNIL» issue de cette transposition, dotée de nouveaux pouvoirs puissants et variés. **L'organisation et les procédures de la CNIL ont été modifiées, l'exercice des pouvoirs coercitifs et de contrôle sécurisé, de nouveaux services et outils aux usagers développés** etc... Pour expliquer ces nouveaux pouvoirs, j'ai engagé une ambitieuse politique de communication, y compris au niveau européen. Compte tenu des nouvelles missions dévolues au CEPD, cette **expérience de conduite du changement**, de **management**, de mise en œuvre de nouveaux pouvoirs, de **gestion budgétaire rigoureuse**, de déploiement d'outils et d'une politique de **communication** forte me semble essentielle pour exercer avec succès la fonction de CEPD.

Comme Commissaire à la Commission de régulation de l'énergie (CRE), j'ai supervisé la rédaction du rapport sur la gestion des données par les opérateurs de réseau d'énergie. Les missions de ces opérateurs de réseaux évoluent rapidement avec le déploiement des « réseaux intelligents » et la collecte massive de données qui en résulte. De nouvelles opportunités se font donc jour mais aussi des risques inédits émergent, comme la cybercriminalité. Là aussi, cette expérience de la construction d'un nouveau cadre régulatoire dans un **secteur industriel**

stratégique, au **service du consommateur final** et de la **confiance numérique**, me servira pour le CEPD.

En tant que conseiller stratégique de **l'ICO** (Information Commissioner's Office - UK), **je travaille aujourd'hui sur le lien entre régulation et innovation**. Mon rôle a été, dès 2016, de proposer la création d'un **« sandbox »** et d'accompagner l'ICO dans cette démarche jusqu'à son déploiement opérationnel. Et ce débat sur l'innovation au service du bien public devra avoir lieu au niveau européen, en particulier au sein du **Parlement,** notamment au vu des ambitions européennes en matière d'IA. La réflexion que j'ai menée sur ce sujet, ainsi que mon activité d'enseignement et mes publications académiques, me serviront utilement pour conseiller le Parlement.

Enfin, j'exerce aujourd'hui la profession d'avocat dans un cabinet international. Je conseille, en matière de données personnelles, des entreprises dans l'élaboration de leurs projets innovants et leur gouvernance. La problématique de la protection des données se transforme pour devenir l'un des leviers de la compétitivité et de la différentiation des entreprises. C'est aussi un facteur de risque plus élevé compte tenu du montant des sanctions prévues par le RGPD. L'exercice de ma mission de conseil en est donc d'autant plus stratégique et multi-juridictionnel aujourd'hui. **Connaître et comprendre les enjeux et le fonctionnement des entreprises de l'intérieur**, les contraintes et objectifs de leur transformation digitale, me semble être une **condition nécessaire** pour exercer avec **pertinence** les missions dont est investi le CEPD**.**

Ce parcours diversifié est le gage d'une expertise pluridisciplinaire, d'une vision stratégique des enjeux, d'ouverture internationale mais aussi de pragmatisme. Mon parcours démontre **ma capacité à construire des « ponts »** : **entre des disciplines** juridiques différentes, **entre le droit et la technologie,** entre le **droit et l'économie,** entre des **systèmes juridiques de pays différents,** entre des **institutions et des acteurs, y compris politiques, aux intérêts parfois divergents,** entre **des cultures**. Ce parcours illustre aussi mon **attachement à la conception européenne de la protection des données**, ma capacité à la défendre et à **la promouvoir** au niveau international. Cet attachement découle aussi de **mes origines personnelles**, étant moitié suédois par ma mère, originaire des territoires orientaux polonais par mon père et portant le nom d'une ville italienne où mes ancêtres trouvèrent alors refuge.

Enfin, j'ajouterai que **l'indépendance est au cœur de ma vie professionnelle**. Elle l'a été lorsque j'ai décidé de rejoindre la CNIL et la CRE, autorités indépendantes. Elle l'est aujourd'hui dans mon métier d'avocat comme obligation déontologique. Mais au-delà des statuts, l'indépendance se mesure aux actes : **mes articles** académiques sur le droit à l'oubli qui vont dans le même sens que la décision de la CJUE (C-507/17), ou encore ma récente **plaidoirie devant la CJUE** en matière de surveillance étatique (C-511/18) en témoignent. L'indépendance est une discipline exigeante. Elle doit inclure le **dialogue avec toutes les parties prenantes,** sans quoi elle se transforme en une inaccessible autarcie. C'est d'une telle conception de l'indépendance, exigeante mais **constructive, ouverte mais ferme**, dont le CEPD aura besoin et que je souhaite mettre à son service et **à votre service**.

2. Pouvez-vous décrire comment vous imaginez l'avenir de l'autorité que vous seriez amené à diriger en tant que CEPD, y compris les éventuelles difficultés auxquelles vous vous attendez et les priorités que vous définiriez pour cette autorité indépendante?

Avec les développements rapides de **l'intelligence artificielle** (IA), de l'autoapprentissage des algorithmes et de l'internet des objets, l'Europe est confrontée à **des défis éthiques sans précédent.** Alors que le volume des données produit double tous les 24 mois, comment réguler des algorithmes qui se modifient par eux-mêmes et qui semblent parfois échapper à leurs créateurs ? Comment assurer la transparence et l'intelligibilité de ces outils qui envahissent notre quotidien ? Comment garantir leur objectivité et mesurer leurs biais ? Comment les corriger lorsqu'ils sont discriminatoires ? Ces défis sont d'autant plus importants que **l'Europe est prise en tenaille entre deux modèles de régulation :** celui des États-Unis, où il n'existe pas de législation fédérale transversale sur les données et où c'est le juge, voire le régulateur sectoriel, qui interviennent *a-posteriori,* et celui de la Chine, caractérisé par une hypercentralisation étatique de l'accès aux données.

Dans cette **géopolitique de la donnée**, dans ce monde digital en construction, **l'Europe doit s'affirmer** comme le nouvel acteur majeur. La Commission a annoncé son intention de présenter une proposition sur l'IA dans les 100 jours. Et l'Europe **a les moyens de ses ambitions** car elle possède déjà un cadre juridique robuste sur lequel **construire** cette nouvelle régulation : **le RGPD**. Ce texte prévoit des principes pertinents, tels que «l'accountability», la transparence, le droit pour les personnes à ne pas faire l'objet d'une décision prise sur le seul fondement d'un traitement automatisé. En s'appuyant sur le RGPD, l'Europe peut et doit **parvenir à un usage éthique de l'IA, responsable, bénéfique aux personnes et à la société dans son ensemble**. Et dans la **construction** de cette **voie Européenne et humaniste de l'IA**, **le CEPD** a toute sa place à jouer en tant que **conseil**, apporteur de **propositions** pragmatiques et innovantes au **Parlement qui est le lieu privilégié** où pourra se construire **démocratiquement** cette voie européenne. Sur le fond, il pourrait être envisagé l'introduction : d'une approche par les risques qui pourrait s'adosser sur un droit à l'expérimentation, de mécanismes de certification, de correction et de transparence renforcés, voire d'une traçabilité des données et des algorithmes utilisés (vers « un passeport » des données ?). C'est un premier défi de taille qu'il faudra aussi **porter au niveau international. Et le CEPD** devra être **le porte-parole de cette voie européenne**.

Le deuxième défi stratégique du CEPD découle de **la valeur croissante des données, de la complexité et de l'évolutivité de l'économie de la donnée**. Comprendre la chaine de valeur, **identifier les tendances** émergentes, les nouveaux acteurs, devient un prérequis pour dispenser un conseil pertinent, **agile** et **proactif**, et non plus seulement réactif. Pour cela le CEPD **va devoir accroitre** les mécanismes de **coopération** opérationnels avec les autorités européennes en charge de la **concurrence**, avec les **autorités de protection des données nationales**, développer des partenariats avec des centres de recherche en **économie**, en **cybersécurité,** en **sociologie** des usages des technologies. Mais surtout, le CEPD devra augmenter sa propre capacité d'analyse **prospective technologique** et d'intervention **en diversifiant le profil de ses agents, ce qui confortera son indépendance**.

Je possède cette **expérience de construction d'une capacité d'analyse technologique prospective** puisque j'ai créé, à la CNIL, le **laboratoire d'expertise**, l'un des premiers en Europe, tout en faisant passer la part des ingénieurs de 3 % à 10 % des effectifs en 6 ans. Car la protection des données ne peut plus fonctionner en **silos.** Pour être un conseiller **pertinent, proactif et pluridisciplinaire au bénéfice du Parlement, du Conseil et de la Commission, le CEPD doit s'ouvrir** davantage et **fédérer** autour d'un **nouveau projet stratégique.** Et je m'engage à le **co-construire** en consultant les **parties prenantes** dans les 6 mois suivants ma prise de fonction, car **l'indépendance** n'est **pas l'autarcie**.

Le troisième défi concerne la question du partage et des transferts de données entre États, y compris tiers, pour des motifs de lutte contre la criminalité. La **CJUE et le Parlement ont pris des positions fortes** sur lesquelles le CEPD pourra s'appuyer tant dans sa mission de conseil que de contrôle (voir Q 3).

Le dernier défi auquel sera confronté le CEPD découle de sa **mission de superviseur** des institutions européennes. Le CEDP doit être un contrôleur **prévisible, juste et crédible**. A cette fin, il doit poursuivre l'accompagnement dans la conformité des institutions européennes, les **soutenir dans leur montée en maturité,** par exemple en leur proposant des **outils nouveaux** «d'accountability», tels que des modèle de contrat de sous-traitance, ou encore des outils d'auto-évaluation, des **guides pratiques** thématiques, des formations approfondies en cybersécurité. Le CEPD devra également monter en compétence dans **sa propre capacité de contrôle** sur place et sur pièces qui exige des **compétences spécifiques.** Je le sais pour avoir **mis en place le service de contrôles de la CNIL**. Enfin, le CEPD devra **publier son programme annuel de contrôles et rendre compte de son exécution,** notamment **devant le Parlement**. Il en va aussi de sa **crédibilité,** au sein de l'Union comme à l'extérieur.

Pour faire face à ces défis, **le CEPD aura besoin** de **tout le soutien du Parlement** pour obtenir une augmentation de ses moyens qui demeurent insuffisants au vu de ses missions et de ses défis.

3. Comment comptez-vous remplir la mission qui vous serait officiellement confiée en tant que CEPD en matière de contrôle des agences chargées de la justice et des affaires intérieures et que pensez-vous des transferts de données à caractère personnel depuis et vers les agences dans ces domaines, en particulier dans le cadre du contrôle des transferts de données à caractère personnel vers des pays tiers?

Pour contrôler effectivement les traitements de données des agences européennes judiciaires et policières, il est préférable de **connaitre le fonctionnement de la chaine pénale**, des institutions judiciaires et des services en charge de la lutte contre la criminalité. A cet égard, mon expérience à la Commission des Lois de l'Assemblée nationale et à la CNIL (autorité de protection française) me semblent particulièrement pertinentes.

A la Commission des lois, j'étais en charge du droit pénal, du suivi du budget de l'administration pénitentiaire et du droit des données personnelles. Dans ce cadre, j'ai été amené à travailler sur tous les textes pénaux pendant 7 ans, et notamment sur la création d'une base de donnée et de dispositifs de suivi des délinquants sexuels graves (fichier « FIJAIS »).

Quant à la CNIL, elle a longtemps été l'une des seules autorités de protection des données en Europe à posséder une compétence de contrôle *a priori* et *a posteriori* sur les fichiers de police et judiciaire. C'est pourquoi, en tant que Secrétaire général, j'ai organisé, en 2008 et 2009, **le premier contrôle général du fichier de police judiciaire** (le « STIC »), placé sous le contrôle des procureurs de la République compétents. À l'époque de ce contrôle, le STIC comprenait des données sur 36 millions de personnes. Ce contrôle a duré plus d'un an, a conduit à 19 inspections sur place, l'envoi de questionnaires à 34 tribunaux représentant 50 % de l'activité pénale en France ainsi que des requêtes techniques sur les mesures de sécurité et de traçabilité des connexions. En outre, le droit d'accès des personnes aux traitements de police s'exerçait alors exclusivement de façon dite « indirecte », à savoir que la CNIL exerçait ce droit au nom de la personne l'ayant demandé, comme cela est d'ailleurs possible pour le CEPD en application

de l'article 84 du Règlement 2018/1725. Cette **expérience unique de contrôle et de pratique du droit d'accès indirect** (près de 4 000 demandes par an à la CNIL) me sera particulièrement utile pour le CEPD.

En effet, le CEPD intervient dans un **cadre juridique complexe** et qui sera amené à évoluer au cours de son prochain mandat. En dépit de l'adoption du Règlement 2018/1725 et de son chapitre IX, les pouvoirs du CEPD demeurent variables car fondés sur plusieurs instruments juridiques spéciaux. Tel est le cas des traitements de données opérationnels mis en œuvre par Europol, Eurojust ou par le Parquet européen. Les pouvoirs du CEPD diffèrent puisqu'il ne peut pas prononcer d'amende administrative ou encore ordonner la suspension des flux internationaux de données ni adresser d'avertissement au Parquet européen. Il ne peut pas non plus prononcer d'interdiction de traitement à Eurojust et au Parquet européen, à la différence d'Europol.

Les régimes juridiques désormais en vigueur permettent toutefois au **CEPD d'exercer un contrôle exigeant sur ces agences, contrôle absolument indispensable compte tenu des risques inhérents aux traitements** de telles données **et au vu de la perspective d'interopérabilité** de certains systèmes d'information. C'est pour les transferts de données, en particulier vers des États tiers, que les risques sont les plus élevés et que le contrôle doit s'exercer avec la plus grande rigueur. En l'absence de décision d'adéquation adoptée par la Commission en application de la Directive 2016/680, le rôle du CEPD sera crucial.

Ce contrôle existe déjà s'agissant des accords conclus entre l'Union et des États tiers pour les transferts de données par Europol. Il devra se poursuivre avec un niveau d'exigence sans cesse réaffirmé. S'agissant d'Eurojust et du Parquet européen, le contrôleur devra se saisir des pouvoirs de contrôle qui lui sont conférés pour s'assurer précisément que les **transferts de données s'effectuent dans le respect des règles définies par les règlements applicables et en conformité avec les exigences de la CJUE**. Le risque que les données transmises soient utilisées pour d'autres finalités dans les États tiers est réel et un contrôle strict devra s'opérer à cet égard.

Afin **d'éviter la fragmentation** des régimes de contrôle et donc l'affaiblissement du niveau de protection des données des personnes dans cette matière éminemment sensible, l'article 98 du Règlement 2018/1725 prévoit une « clause de rendez-vous » (au plus tard le 30 avril 2022). Cette clause invite la Commission à examiner les textes spéciaux, s'assurer de leur compatibilité avec la Directive 2016/680 et recenser les éventuelles divergences ayant conduit à une telle fragmentation. Le rôle du CEPD sera déterminant ici pour partager son retour d'expérience et conseiller la Commission, le Conseil et le Parlement.

À cette fin, il me semble **essentiel que le CEPD**: (ii) monte en **compétence** et en moyens disponibles sur ses missions de contrôle sur place; (iii) développe la **coordination** approfondie avec les **autorités de protection des données nationales** compte tenu de la nature «mixte» des données traitées par ces agences; (iv) **rende compte** de façon plus explicite et distincte de sa mission de supervision et (v) développe des **outils d'accompagnement** et de mise en conformité dédiés en collaboration avec les équipes de ces agences.