Les rencontres d'experts d'Option Droit & Affaires

RGPD : l'heure des contrôles

L'entrée en vigueur du règlement général sur la protection des données le 25 mai 2018 a non seulement augmenté considérablement le montant des sanctions encourues en cas de manquement mais, plus largement, a fait évoluer la philosophie générale de la réglementation et notamment la relation des entreprises concernées avec le régulateur. Après une période de tolérance d'une année de la CNIL pour permettre aux entreprises de se mettre en conformité, qu'en est-il de l'application de cette nouvelle réglementation, en matière de contrôles et de sanctions ? Six experts font part de leur expérience avec l'éclairage du secrétaire général de la CNIL.

es a sonné

De gauche à droite (en haut) :
Christophe Clarenc, associé, DTMV & associés - **Jean Lessi,** secrétaire général, CNIL **Prudence Cadio,** associée, LPA-CGR **Daniel Kadar,** associé, Reed Smith **Florence Samaran,** general counsel continental Europe, Unibail-Rodamco-Westfield, (en bas) **Paul-Olivier Gibert,** président, AFCDP **Isabelle du Châtelier,** DPO, Dassault Systèmes

RGPD : un an après

Jean Lessi, secrétaire général, CNIL : Trois éléments de bilan. Premier élément, le RGPD marque une prise de conscience, chez les professionnels et les particuliers, des obligations, des droits et des enjeux des données personnelles, même si ces derniers préexistaient avec la loi de 1978. Nous l'avons constaté avec l'augmentation du nombre de plaintes et de saisines. Le RGPD a mis un coup de projecteur sur ces sujets.
Deuxième élément : la montée en puissance progressive du respect du cadre juridique. Une transition de deux ans, entre 2016 et 2018, était prévue pour permettre aux organismes de se préparer au RGPD. Force est de constater que la compliance n'est pas encore atteinte et que la transition se poursuit aujourd'hui. Une illustration : 55 000 organismes ont à présent désigné un délégué à la protection des données (DPO), alors qu'on estime qu'il existe entre 80 000 et 100 000 organismes devant désigner un DPO. Autre exemple : les notifications de violations de données. La CNIL en a reçu plus de 2 000 mais nous sommes conscients qu'il y a une forte sous-déclaration.
Enfin, troisième élément, le standard européen en matière de protection des données personnelles s'intègre désormais dans la diplomatie internationale. Non seulement le RGPD est regardé par les pays tiers, mais il devient aussi un objet très opérationnel : soit on veut l'imiter soit on développe un dispositif alternatif, mais dans les deux cas, le RGPD devient un élément structurant de la géopolitique de la donnée.
Voilà en quelques mots les premiers constats après un an d'application.

Florence Samaran, general counsel continental Europe, Unibail-Rodamco-Westfield : Je souscris à vos propos sur la prise de conscience. Notre métier consiste à construire et exploiter des centres commerciaux, qui accueillent des clients et leur proposent des programmes de fidélité ; les données personnelles représentent donc un enjeu important pour notre groupe. C'est un enjeu de différenciation et de confiance de nos clients. Nous avons commencé à anticiper ces sujets en 2016, et j'ai pu constater, à l'occasion de diverses réunions entre professionnels, tout au long de ces années de mise en place, une vraie prise de conscience des professionnels de ces problématiques. La difficulté se situe dans la mise en œuvre pratique, avec des interrogations liées aux zones grises de la réglementation et aux superpositions avec les réglementations européennes locales, sachant que notre groupe opère également aux Etats-Unis…
Nous avons beaucoup investi pour mettre en place le RGPD (temps, ressources humaines avec notamment un recrutement), mais personne ne sera jamais totalement compliant car cette réglementation est un chemin sur lequel nous nous sommes engagés, chemin qui va évoluer au fur et à mesure des nouveaux projets et des nouveaux usages.

Isabelle du Châtelier, DPO, Dassault Systèmes : D'ailleurs, le RGPD ne concerne pas seulement les sociétés européennes. L'une de nos premières actions, lorsque le RGPD a été publié, a été d'informer nos filiales américaines qui s'adressent au marché européen de leurs nouvelles obligations.
Par ailleurs, le RGPD inspire d'autres Etats qui adoptent des lois dans le même esprit. C'est le cas du Brésil dont la loi entrera en application en 2020, et de l'Inde avec un nouveau projet de loi. Travaillant dans un groupe international, il peut m'arriver d'être confrontée à des lois qui se contredisent, avec comme difficulté supplémentaire de gérer les différences de délai de notification d'un pays à un autre, et même d'un Etat à un autre pour les Etats-Unis.

Les difficultés rencontrées

Prudence Cadio, associée, LPA-CGR : Les difficultés rencontrées sont multiples et majoritairement de deux ordres. La première est liée à la connaissance de cette réglementation par les entreprises ainsi qu'à la mise en place du principe d'accountability. Pour beaucoup d'entreprises, la loi de 1978 était quasiment inconnue : la prise de conscience a pu en être d'autant plus brutale, notamment au regard de son ampleur. La mise en conformité concerne la quasi-totalité de l'activité de l'entreprise. Au stade de l'audit des données, l'entreprise se rend compte qu'une donnée à caractère personnel peut être mise en œuvre par tous les départements, et non uniquement par le service marketing ou les ressources humaines.
Et comme vous le disiez, la mise en conformité est constante. Il y a donc un bloc de gouvernance transverse à mettre en place. En tant que conseil, j'ai également accompagné nos clients sur ces aspects de gouvernance et sur l'élaboration de process liés, entre autres, au principe d'accountability et à la constitution de la documentation probatoire. Il y a une démarche d'accompagnement qui nécessite d'avoir ainsi une perspective de vue plus globale, afin de répondre aux nouvelles exigences structurelles et logiques imposées par le RGPD.
L'autre difficulté porte sur l'appréhension et l'application des nouvelles obligations en particulier pour les prestataires du digital et plus particulièrement les sous-traitants. Ces derniers voient leurs obligations réglementaires renforcées avec en premier lieu la tenue du registre de sous-traitance. Pour les hébergeurs, qui ne connaissent pas les données, il y a un problème de praticité. A ces prescriptions réglementaires s'ajoute le durcissement de leur responsabilité qui doit s'articuler et s'intégrer au cadre contractuel de leurs relations commerciales, soumis au droit civil. Les obligations sont donc complexes et les sanctions potentielles significatives.

Daniel Kadar, associé, Reed Smith : Peut-être une perspective internationale pour compléter. J'interviens notamment pour des sociétés qui n'ont pas leur centre de décision en France. Pour elles, le RGPD constitue un événement juridique novateur qui a généré une croissance des équipes de conformité. Ces groupes ont également dû se poser certaines questions organisationnelles, à commencer par le choix du référentiel du registre de traitement de données. Quand une société a des filiales en Allemagne, en Belgique et en France par exemple, il est difficile de savoir quel registre adopter. Derrière cette question se pose celle de l'autorité chef de file.
Viennent également s'ajouter les problématiques liées au Brexit. Que se passera-t-il pour les entreprises qui ont choisi l'autorité anglaise comme autorité chef de file ? Quels sont les critères pour déterminer, voire modifier, l'autorité chef de file ?
Dans sa décision Google de janvier, la CNIL a déclaré que la principale filiale européenne ne constituait pas le centre de décision, et donc que l'autorité irlandaise n'était pas l'autorité chef de file. Cette décision crée des insécurités : quel sera l'élément de rattachement ? Quels sont les référentiels à utiliser ? Quelles lignes directrices suivre, sachant que certaines autorités sont plus avancées que d'autres ? Des arbitrages doivent être pris, et notre rôle est de les accompagner en essayant de définir un déterminateur commun.
Par ailleurs, il est vrai que le RGPD s'est positionné sur la place internationale comme un élément fondateur dont on s'inspire. Toutefois, malgré l'existence de ce règlement unique européen, force est de constater que l'application est diverse, et que des questions perdurent comme les cookies par exemple. La CNIL travaille actuellement sur ce sujet, tout comme d'autres autorités, avec des approches parfois différentes. Nous faisons donc face encore aujourd'hui à beaucoup d'interrogations.

Jean Lessi : Quelques éléments de réponse sur les différences que vous avez soulignées dans les textes ou les applications entre les pays : il existe effectivement quelques différences entre les réglementations puisque chaque Etat membre dispose d'une marge de manœuvre pour la transcription du règlement européen, disparités auxquelles s'ajoutent des différences de pratiques. Toutefois, il faut d'abord souligner le progrès apporté par l'existence du RGPD qui fournit une base commune, inexistante auparavant.

Paul-Olivier Gibert, président, AFCDP : Sachant que le texte contient une clause de revoyure. Le texte pourra donc encore évoluer.

Jean Lessi : C'est une conformité dynamique.

Paul-Olivier Gibert : A la fois dans la mise en œuvre et dans la conception du texte.

Jean Lessi : Nous sommes en tout cas conscients des différences de pratique. Vous prenez l'exemple des cookies, sujet qui concerne à la fois le RGPD et la directive Privacy de 2002, modifiée en 2009, pour laquelle tous nos homologues ne sont pas compétents. Sur ce sujet, notre objectif est évidemment de ne pas avancer seuls. S'il n'est pas possible, à court terme, d'avancer à 28, nous souhaitons travailler en lien avec d'autres

autorités afin d'apporter une sécurité juridique sur ce sujet. Nous avons toujours à l'esprit cet arbitrage que nous devons opérer entre l'agilité de la réponse et la couverture européenne de cette dernière. Une réponse européenne nécessite forcément du temps. Au cas par cas, nous essayons de distinguer les sujets qui doivent être portés au niveau européen rapidement, et ceux, peut-être un peu moins systémiques ou plus «franco-centrés», pour lesquels la CNIL avance de manière plus autonome.
La question de l'établissement principal est importante car elle va conduire à désigner l'autorité de référence. Pour revenir sur la décision Google, la CNIL s'est rapprochée de ses homologues avant d'affirmer sa compétence, et a suivi les lignes directrices du G29 reprises par le CEPD (Comité européen de la protection des données). Il existe un critère : celui de la localisation du pouvoir de décision sur le traitement des données. Autrement dit, si une filiale emploie beaucoup de salariés mais que ces derniers ne sont pas décisionnaires sur le traitement des données, elle ne sera pas considérée comme l'établissement principal. En l'occurrence, la CNIL a estimé que ce pouvoir de décision, sur les traitements en cause, ne se trouvait pas au siège irlandais.

Daniel Kadar : Dans cette phase de trajectoire de conformité, il est important de voir quelles sont les réflexions que peut avoir un groupe européen afin d'essayer d'avancer de manière coordonnée. Pour ce groupe, il est assez logique de suivre le raisonnement suivant : mes plus grosses opérations se situent dans tel pays, c'est donc l'autorité de ce dernier qui est mon autorité chef de file. Le fait qu'ensuite l'analyse se fasse plus dans le détail, notamment pour des entreprises du numérique, va susciter des questions, d'autant plus que les organisations sont de plus en plus matricielles. Des questions d'arbitrage vont se poser.

Jean Lessi : Vous avez parfaitement raison. Définir un critère c'est une chose, l'appliquer en est une autre. Nous en sommes conscients.

Daniel Kadar : Des projets, par exemple, qui sont menés avec des personnes travaillant à distance, aux quatre coins du monde, posent question, et dans de tels cas, la détermination du lieu de prise de décision constitue un vrai enjeu.

Jean Lessi : Il y a effectivement un enjeu de clarification.

Isabelle du Châtelier : Il me semble en outre que ce critère de centre de décision doit s'analyser selon la finalité. Par exemple, il est possible que le centre de décision pour des sujets RH soit situé dans un pays, alors que le centre de décision marketing est établi dans un autre.

Prudence Cadio : La question de la pertinence et de la cohérence de la mise en œuvre du plan de conformité pour les groupes se pose. Nous avons d'un côté cette phase de mise en conformité globale et des procédures harmonisées, et de l'autre une appréciation spécifique par traitement qui requiert une analyse fine de la loi applicable. Cette distorsion peut être porteuse d'insécurité juridique et reste difficile à gérer pour les entreprises.

Prudence Cadio, associée, LPA-CGR

«La première difficulté est liée à la mise en place du prinicipe d'accountability.»

La sécurité des traitements de données

Christophe Clarenc, DTMV & Associés : Le bilan est également intéressant sur la sécurité des traitements de données personnelles, avec les manquements constatés et les sanctions prononcées en 2018, les notifications de violations de données personnelles depuis l'entrée en vigueur du RGPD et la récente décision Sergic de juin 2019. Comme en 2017, les manquements à la sécurité et à la confidentialité des données représentent en 2018 la majorité et les montants les plus élevés des sanctions prononcées, pour des manquements aux précautions et mesures élémentaires de sécurité et causals dans les violations

de données constatées. Le principe et les règles de sécurité sont renforcés dans le RGPD qui par ailleurs élève sensiblement le niveau des sanctions et institue une obligation de notification des violations de données. La CNIL indique qu'elle a reçu plus de 1000 notifications entre la fin mai et la fin décembre 2018. Outre les éventuels défauts de notification, il sera donc instructif de voir comment la CNIL traite ce stock et le flux au regard des éventuels manquements qu'il comporte, de l'ensemble des conditions conformité prévues dans le RGPD, de l'opportunité des poursuites, des possibles cas de manquements multiples et de la combinaison des mesures correctrices, et enfin de l'évolution des montants de sanction et de la décomposant des montants en cas de manquements multiples. La décision Sergic rendue sur le fondement du RGPD soulève des questions à tous ces égards par l'économie de ses indications et de ses motifs. Par ailleurs, tant au plan de la conformité qu'au plan des moyens opérationnels, la sécurité des traitements de données personnelles doit être replacée dans la problématique et la responsabilité fondamentales de la sécurité des systèmes d'information critiques et de la protection du patrimoine et des échanges informationnels des entreprises. Certaines entreprises cumulent d'ailleurs différents régimes sectoriels et référentiels de sécurité. Dans l'univers de l'économie hyper numérisée et connectée, la bonne gouvernance de la sécurité des systèmes d'information critiques dont les systèmes de traitements de données personnelles est une responsabilité élémentaire.

La fin des réponses individuelles de la CNIL

Paul-Olivier Gibert : L'AFCDP regroupe environ 1 600 entreprises et organisations de toutes tailles et 5 000 professionnels de la protection de la vie privée qui sont préoccupés par le fait que la CNIL sera moins en mesure de les accompagner dans les démarches de mise en conformité et dans le cadre de leur obligation d'accountability.

Florence Samaran : La CNIL sera en effet amenée à prononcer des sanctions en cas de défaut de mise en conformité.

Paul-Olivier Gibert : Au-delà de cette question, le problème tient dans le fait que les professionnels concernés ne sont plus en mesure de disposer d'une prise de position de la CNIL sur laquelle ils peuvent se reposer et qu'ils étaient amenés à diffuser au sein de l'entreprise.
Un certain nombre d'acteurs constatent une certaine prise de distance de la CNIL, qui s'illustre notamment par les changements de forme des ateliers de la CNIL. Dans d'autres domaines, nous sommes, certes, parfois confrontés à des flous juridiques, mais dans le cas du RGPD nous sommes exposés à un risque important de sanction. Nous devons faire preuve d'une grande vigilance et œuvrer avec honnêteté selon des interprétations effectuées de bonne foi, qui peuvent se trouver contredites par une décision de l'autorité de contrôle. Ces questions s'accompagnent de problèmes d'organisation qui sont relativement sensibles.

Christophe Clarenc, DTMV & associés

«Les obligations en matière de sécurité des données posent divers problèmes d'organisation.»

Christophe Clarenc : Le principe de responsabilité institué dans le RGPD réclame non seulement de respecter mais de démontrer le respect de ses exigences. Or nombre de ses exigences sont des exigences de moyens organisationnels et techniques appropriés. Il peut donc y avoir des flottements et des hésitations sur ce qui est approprié pour démontrer la conformité. La certification répond dans ce sens, mais elle a un coût, outre les possibles coûts de mise à niveau pour son obtention. Les petites et moyennes entreprises sont évidemment plus démunies et exposées que les grandes à cet égard. Mais l'assurance de conformité, en particulier en matière de sécurité, tend à devenir une condition de commercialité dans les relations avec les clients, les fournisseurs, les prestataires, les prêteurs et les acquéreurs.

Paul-Olivier Gibert : Cela implique de pouvoir obtenir des réponses précises de la part du régulateur, et les années qui viennent seront très importantes pour l'évolution de cette situation.

L'accompagnement par la CNIL des opérateurs

Jean Lessi : Sur la question de l'accompagnement et de cette forme de «distance» accrue évoquée par Paul-Olivier Gibert de la part de la CNIL à l'égard de ceux qui travaillent au quotidien sur les traitements de données, il ne s'agit pas d'une volonté de la CNIL ou d'un plan. Cela traduit notamment des moyens manifestement insuffisants, et la CNIL doit se fixer des priorités dans ses actions. Je souhaiterais que nous disposions de plus de moyens pour répondre à toutes les demandes d'accompagnement, mais les choix budgétaires ne nous le permettent pas.

D'une part, il n'y a, en effet, plus de prise de position préalable systématique de la CNIL sur des pratiques de traitement de données. Mais il faut se souvenir que le système antérieur a montré toutes ses limites, et il s'agit du choix du législateur européen. La prise de position préalable, dans le système antérieur, contribuait à «endormir» l'opérateur, qui pouvait associer une demande d'autorisation préalable à un feu vert ferme et définitif. L'objectif de la nouvelle réglementation est de s'inscrire dans une démarche vertueuse de responsabilisation de l'opérateur.

Dans ce contexte, la CNIL poursuit deux objectifs. D'abord, toute prise de position préalable de la CNIL ne disparaît pas. Dans un souci de «gain» d'échelle, nous développons la rédaction de codes de conduite, dont les premiers ont été présentés il y a quelques semaines, et qui ont vocation à se multiplier dans tous les secteurs et à destination de tous les tissus professionnels. Nous travaillons également sur des formes de réponses collectives, notamment via des certifications, des lignes directrices, des recommandations et des référentiels.

D'autre part, nous comptons sur la montée en compétence de tous les acteurs. Le système antérieur reposait beaucoup sur le face-à-face opérateur/régulateur, au détriment de l'apprentissage collectif des opérateurs, des fédérations, des secteurs ou des territoires. Nous croyons vraiment que tout notre écosystème peut profiter d'une dynamique vertueuse dans un secteur, par le biais d'échanges de bonnes pratiques ou de mutualisations de ressources et d'expertises. La CNIL aura alors vocation à intervenir plus spécifiquement sur les questions que le tissu ne parviendra pas à résoudre lui-même ou sur les questions où le besoin de sécurité juridique est majeur. Le but n'est donc pas de nous placer en retrait mais de stimuler cette montée en compétence des opérateurs. Avec les moyens dont nous disposons, le but est de veiller à ce que chaque opérateur puisse, à défaut d'obtenir systématiquement une réponse individuelle de la CNIL, trouver une réponse au sein de cet écosystème. Et cela devra sans doute prendre encore quelques années.

Le rôle répressif de la CNIL

Christophe Clarenc : La société Sergic a récemment été condamnée à une sanction pécuniaire de 400 000 euros, soit environ 1% de son chiffre d'affaires, pour deux manquements graves dont l'un à la sécurité. La décision motive peu et ne décompose pas le montant de la sanction entre les deux manquements et ne permet donc pas de mesurer l'éventuelle évolution de la politique répressive dans le cadre du RGPD. Elle ne donne pas non plus d'indication sur les conditions de l'opportunité des poursuites, même si on comprend les poursuites dans le cas d'espèce.

Jean Lessi, secrétaire général, CNIL

«Il faut d'abord souligner le progrès apporté par l'existence du RGPD qui fournit une base commune, inexistante auparavant.»

Jean Lessi : C'est un point qui était débattu. C'est pourquoi nous avons affirmé ce principe d'opportunité des poursuites.

Christophe Clarenc : Les orientations et degrés de l'opportunité des poursuites et la possibilité de décisions combinant les mesures correctrices seront des facteurs décisifs en particulier dans les affaires de sécurité compte tenu à la fois du stock des notifications de violations et des ressources de l'autorité.

Jean Lessi : Concernant la «politique répressive» : je remercie Christophe Clarenc pour son analyse de la décision rendue à l'encontre de la société Sergic et pour son approche concernant l'imbrication du traitement des données et de la sécurité de systèmes d'information, à laquelle j'adhère entièrement.
Nous avons reçu plus de 11 000 plaintes l'an dernier. Dans ce contexte, l'objectif de la CNIL est, avant tout, la conformité. Notre objectif n'est pas de prononcer une sanction à tout prix, c'est de faire respecter les textes, et que cette démarche soit vertueuse. Nous avons donc recours à de simples rappels à la loi, ou à de simples observations à la clôture de la procédure, qui sont la plupart du temps largement suffisants. Dans d'autres cas, lorsque nous sommes confrontés à des opérateurs de mauvaise foi, très peu coopératifs, ou à des faits très graves, une suite répressive s'avère nécessaire. Une récente loi a instauré le droit à l'erreur, notamment en matière fiscale ; mais la CNIL, de longue date, applique un droit à l'erreur auprès des opérateurs. Preuve en est le fait que, sur les 400 contrôles que nous avons effectués, nous avons prononcé 10 à 15 sanctions et une centaine de mises en demeure, qui correspondent à des cas trop graves ou à des opérateurs ayant montré une volonté de ne pas respecter la législation, en dépit parfois des signaux d'alertes envoyés.Concernant la pratique décisionnelle, il est vrai que le RGPD nous confronte à de nouveaux enjeux de lisibilité de la pratique répressive, en particulier sur les questions de cohérences européennes, sur le niveau et les montants des sanctions et les enjeux d'articulation en cas de manquements multiples. Cela devrait prendre un peu de temps, alors que nous n'en sommes qu'à trois décisions rendues post-RGPD.
Pour revenir sur la décision Sergic : tout d'abord, je rappelle que la CNIL a été la seule autorité de régulation en Europe à assumer une politique de tolérance dans les premiers mois suivant le 25 mai 2018, concernant les obligations nouvelles.
En l'occurrence, dans cette affaire, la formation restreinte a été saisie par la présidente de CNIL, qui a l'opportunité des poursuites.

Daniel Kadar, associé, Reed Smith

«Quand une société a des filiales en Allemagne, en Belgique et en France par exemple, il est difficile de savoir quel registre adopter. Derrière cette question se pose celle de l'autorité chef de file.»

Prudence Cadio : En effet, et c'est la démonstration d'une grande fermeté, au-delà de la sanction pécuniaire de 400 000 euros, deux contrôles ont été opérés en moins de deux semaines, sans mise en demeure ou notifications, et la formation restreinte a été saisie. En termes de mise en œuvre, il semble qu'il s'agisse de votre première décision appliquant une telle verticalité.

Jean Lessi : La formation restreinte est saisie sans mise en demeure préalable, comme cela a pu être mis en œuvre par le passé. Dans le régime en vigueur précédemment, cela ne pouvait être appliqué que pour des manquements ponctuels. En résumé, la loi ancienne nous imposait de passer par une mise en demeure préalable pour des manquements continus. Désormais, et c'est une question nouvelle, outre le choix de la sanction, se pose la question du choix de l'aiguillage entre la saisine de la formation restreinte et de la mise en demeure. Cette question ne se posait pratiquement pas précédemment car nous étions tenus par les textes à un certain déroulement.
Le plafond de la sanction a également changé. Il ne serait pas pertinent de comparer avec le régime antérieur, dans la mesure où les plafonds des sanctions ont été très largement augmentés.

Daniel Kadar : Il s'agit d'un signal fort envoyé aux acteurs. Il y a une absence de mise en demeure préalable qui aurait

Florence Samaran, general counsel continental Europe, Unibail-Rodamco-Westfield

«J'ai été surprise par la longueur du délai séparant la date du contrôle et la clôture de la procédure.»

pu permettre une amorce de dialogue avant le prononcé de la sanction. La CNIL semble désormais s'engager vers des sanctions très fortes. Et l'acteur en question est un administrateur de biens immobiliers.

Christophe Clarenc : Vous semblez faire une analyse extrêmement dure de cette décision, au contraire celle-ci me semble très mesurée.

Florence Samaran : Le Conseil d'Etat a vocation à intervenir et à réguler ces sujets.

Jean Lessi : En effet, toutes ces procédures restent sous le contrôle du juge.

Christophe Clarenc : On a parfois du mal à mesurer la politique de sévérité ou au contraire de modération de certaines décisions de sanction, comme la décision Sergic.

Isabelle du Châtelier : Cette décision m'a également paru relativement clémente, même si nous ne connaissons pas tous les détails de l'affaire.

Jean Lessi : Je vous laisse apprécier l'opportunité de cette décision de la formation restreinte, dont je vous précise que je ne suis pas membre. Je souhaiterais revenir sur le sujet de l'obligation de sécurité, qui n'est pas une obligation nouvelle. D'une manière générale, la période de tolérance consentie par la CNIL portait sur les obligations nouvelles issues du RGPD. Cette obligation de sécurité étant très ancienne, il n'y avait pas lieu de faire preuve de tolérance. C'est une précision que je souhaitais apporter, et je vous laisse apprécier le quantum de la sanction prononcée.

Le déroulement des contrôles

Florence Samaran : J'ai été confrontée à deux contrôles, avant l'entrée en vigueur du RGPD, et ceux-ci se sont très bien déroulés. Si je peux faire une observation, j'ai été surprise par la longueur du délai séparant la date du contrôle et la clôture de la procédure. Même si le contrôle se passe bien, les entreprises préfèrent connaître rapidement les suites qui sont données, a fortiori s'il est nécessaire par la suite de procéder à des aménagements, à des modifications ou à la mise en place de process.

Paul-Olivier Gibert : C'est un sujet qui remonte fréquemment de nos adhérents, qui peuvent constater un long délai entre le contrôle et ses conclusions. Un délai de trois mois pourrait par exemple être institué comme bonne pratique pour connaître les conclusions d'un contrôle.

Isabelle du Châtelier : C'est en effet un ressenti partagé par de nombreux DPO. Réduire ce délai pourrait constituer une bonne pratique à mettre en œuvre, notamment afin de mettre en application rapidement les observations mentionnées dans les conclusions d'un contrôle.

Jean Lessi : Le délai d'instruction à la suite du contrôle est hélas en partie imprévisible à la date du début du contrôle. Tout dépend de ce que l'exploitation des procès-verbaux va révéler.

Isabelle du Châtelier : Il pourrait être utile que la CNIL revienne vers le contrôlé pour lui donner une indication du délai de réponse à la suite du contrôle.

Jean Lessi : C'est, en effet une suggestion intéressante, dont je prends note.

Florence Samaran : Une règle similaire pourrait être appliquée pour les pilotes soumis à la CNIL. Nous évoluons dans un environnement où nous devons aller vite et où les technologies sont assez évolutives.

Jean Lessi : Le temps de réponse est conditionné par trois éléments. En premier lieu, par les ressources dont vous disposez pour répondre. En deuxième lieu, par le degré de crédibilité de la réponse que nous nous devons d'apporter. La réponse du régulateur va être interprétée comme l'état du droit. Chacun des agents de la CNIL peut rapidement établir sa première impression sur un dossier, mais la réponse donnée par le régulateur doit être mûrie, au terme de procédures internes rigoureuses, parfois même en lien avec nos homologues européens. En troisième lieu, comme je l'évoquais, le RGPD nous conduit à davantage de coopération au niveau européen, ce qui nécessite un certain temps.

Isabelle du Châtelier : Dans le cas d'une procédure de consultation, nous, DPO, sommes soumis aux questions de nos collaborateurs qui souhaitent savoir dans quelle mesure ils peuvent avancer dans leur projet dans l'attente de la réponse de la CNIL. Ces délais de réponse peuvent être handicapants, compte tenu des impératifs métiers auxquels nous devons faire face…

Les contrôles en ligne

Prudence Cadio : Pour revenir sur le déroulement des contrôles, je souhaiterais également évoquer le cas des contrôles en ligne, dans lesquels l'opérateur n'est pas informé qu'il est soumis à un tel contrôle. Cette pratique qui consiste à auditer les données en libre accès est de plus en plus courante et va prendre une place grandissante, ce que l'opérateur va découvrir a posteriori, au moment de la notification.
En termes de sécurité, le contrôlé peut bénéficier d'une assistance au cours d'un contrôle sur place, mais dans le cadre d'un contrôle en ligne, il ne bénéficie pas des mêmes garanties.

Jean Lessi : En effet, il n'y a pas d'accompagnement dans l'immédiat, mais une fois que le PV est notifié. Néanmoins, si nous constatons une faille de sécurité, celle-ci est immédiatement signalée, parfois sans attendre l'établissement du PV de contrôle.
Dans tous les cas, même dans le cas d'un contrôle sur place, il s'agit d'un contrôle inopiné.

Christophe Clarenc : La CNIL est une autorité de police, et son intervention en matière de manquement à la sécurité des traitements de données, comme police de marché, est essentielle, d'où l'importance du référencement des entreprises qui interviennent sur ces questions de sécurité.
On a constaté néanmoins dernièrement certaines différences de traitement entre les grosses entreprises et de plus petites organisations. Je pense par exemple à une association qui s'est vu infliger une amende de 75 000 euros, alors que le montant infligé à une grande entreprise n'a été que de 50 000 euros.

Florence Samaran : Il existe également des enjeux d'image liés à ces questions.

Isabelle du Châtelier, DPO, Dassault Systèmes

«L'une de nos premières actions, lorsque le RGPD a été publié, a été d'informer nos filiales américaines qui s'adressent au marché européen de leurs nouvelles obligations.»

Le choix de la procédure

Christophe Clarenc : Outre et avant la question de l'opportunité des poursuites, on peut distinguer les contrôles effectués à la suite d'un signalement ou d'une plainte, des contrôles qui s'inscrivent dans le cadre des programmes de contrôle général et de suivi de la CNIL.

Jean Lessi : Il existe à la CNIL quatre types de contrôles. Ceux qui s'inscrivent dans les priorités fixées annuellement par la commission, ceux qui sont issus de plaintes, ceux qui font suite à un signalement, parfois médiatique, et enfin ceux qui font suite à la vérification du respect d'une précédente

mesure correctrice. Nous allons par ailleurs publier un «guide du contrôlé» dans les prochaines semaines qui reviendra sur les différentes situations de contrôle et les droits et devoirs qui en découlent.

Daniel Kadar : La question de ces droits et devoirs est un élément fondamental car nous nous orientons vers une judiciarisation des relations des différents acteurs avec la CNIL.
La difficulté qu'a évoquée Paul-Olivier Gibert, qui est de s'assurer de la bonne interprétation de la règle et du respect de ses obligations, s'accentue lorsque l'on souhaite confronter cette interprétation face à celle de la CNIL, qui n'est pas en mesure d'apporter une réponse individuelle en renvoyant à des référentiels généraux. De ce fait, le débat est déplacé de la recherche d'une solution, qui est l'essence de l'accountability, vers une recherche plus administrative de la démonstration des démarches que l'opérateur a effectuées pour justifier ses décisions a posteriori en cas de contrôle.
En tant qu'avocat faisant du contentieux réglementaire, j'anticipe un certain nombre de questions de procédure qui vont se poser dans les contentieux à venir, qui concernent les conditions du contrôle (vous avez, M. Lessi, mentionné un guide à cet égard qui est attendu), les éléments de preuve, la compétence de l'autorité chef de file dans les procédures internationales, avant que l'on traite de l'essence même du débat. Ensuite, on pourra s'interroger sur la manière dont vont se dérouler les recours devant le Conseil d'Etat. Il existe tout de même un principe de séparation des pouvoirs entre l'autorité qui édicte la norme et celle qui juge ; nous sommes donc, en matière de conformité, dans une dimension qui mérite d'être décantée.

Paul-Olivier Gibert : Je souhaiterais simplement ajouter deux interrogations que nous devons garder à l'esprit. La question de la finalité du traitement doit-elle découler des fondements juridiques qui justifient le traitement ou l'inverse ? Les bénéfices que la personne physique retire des traitements dont elle fait l'objet sont-ils équilibrés par rapport à ceux tirés par l'opérateur du traitement ?

Jean Lessi : Parmi tous ces éléments intéressants, je répondrai simplement qu'en matière d'interrogation préalable, ou dans le cadre d'un contrôle, la CNIL va se demander si le choix opéré est bon, mais surtout s'il y a eu une véritable réflexion qui a mené à ce choix. Si le choix de la base légale est manifestement mauvais, nous le préciserons. Si deux bases légales étaient envisageables, et que le choix est justifié, dans le cadre de cette logique de responsabilité, quand bien même nous aurions peut-être suivi un raisonnement différent, nous serons amenés à valider les choix qui nous sont présentés ou, en tout état de cause, à ne pas sanctionner en principe.
Nous avons d'ailleurs, nous-mêmes, été confrontés à ces questions quand nous avons établi notre propre registre. Et nous avons eu des débats très intéressants au sein de la CNIL sur les bases légales de certains des traitements. Nous avons pratiqué à nous-mêmes ce que nous appliquerons aux autres, notamment cet exercice de justification.

Isabelle du Châtelier : Ma préoccupation en tant que DPO est en effet de m'assurer d'une part que les traitements mis en place au sein du groupe sont documentés et reposent sur des bases légales, et d'autre part que l'approche retenue est justifiée au titre du principe d'accountability. Dans ce cadre, je considère que je bénéficie d'une marge d'interprétation pour apprécier si ces justifications et les informations communiquées notamment en termes de sécurité me paraissent suffisantes et sont conformes à la loi et au regard du droit des individus.■

Propos recueillis par Coralie Bach
et Gilles Lambert

Paul-Olivier Gibert, président, AFCDP

«Les professionnels concernés ne sont plus en mesure de disposer de prise de position individuelle de la CNIL sur laquelle ils peuvent se reposer.»