Que faire quand la Cnil vient effectuer un contrôle dans votre entreprise ?

Juin 2015

Le Cabinet Mathias publie ce Livre blanc à destination des entreprises et des administrations, des employeurs comme des employés, tous concernés par la protection des données à caractère personnel.

Il nous paraît en effet important de partager notre expérience et notre savoir-faire à travers ce guide pratique afin de vous permettre de gérer au mieux les nombreux enjeux juridiques de ce phénomène.

Le Cabinet Mathias accompagne ses clients dans la réalisation de leurs projets notamment dans le secteur des technologies avancées, de l'Internet, de la propriété intellectuelle et de la protection des données. Nous soutenons nos clients tant en conseil qu'en contentieux.

Garance Mathias
Avocat à la Cour

SOMMAIRE

Résumé

Le contrôle figure parmi les missions dévolues à la Commission Nationale de l'Informatique et des Libertés (Cnil). Récemment renforcé pour une meilleure prise en compte des évolutions numériques, le contrôle permet à la Commission de s'assurer de la bonne application de la réglementation relative à la protection des données à caractère personnel suite à une plainte d'un citoyen, à la demande d'une autorité de protection des données établie dans un autre Etat membre de l'Union européenne ou encore de sa propre initiative.

Les larges pouvoirs de la Cnil et les conséquences qui peuvent en résulter pour l'organisme, notamment en termes d'image, conduisent généralement les responsables de traitements et les Correspondants à la protection des données à caractère personnel à redouter ces contrôles. Face à cette situation, deux stratégies peuvent être adoptées : l'une peut consister à réagir une fois que la Cnil est aux portes de l'entreprise, l'autre peut consister à agir et anticiper le contrôle en élaborant une procédure adaptée à l'organisme. Le Cabinet Mathias accompagne ses clients dans les deux cas, mais ce Livre blanc a pour objectif d'encourager les responsables de traitements à opter pour la seconde solution.

* *
*

Abstract

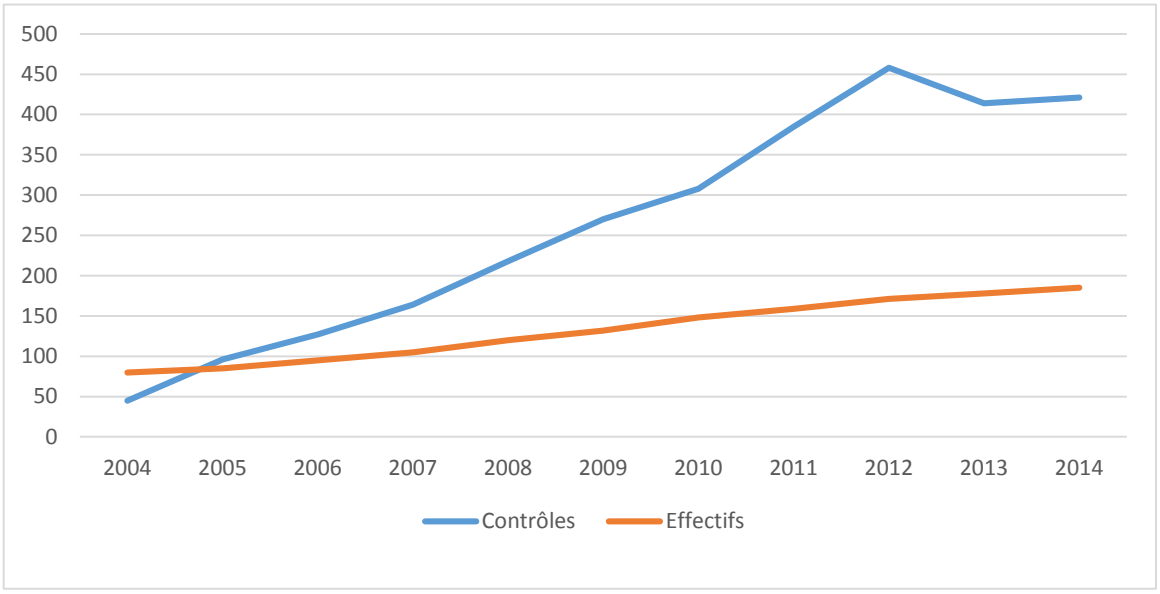
Control is one of the missions conferred by law to the Commission Nationale de l'Informatique et des Libertés (CNIL, National committee for information technology and freedom). This control has recently been made more stringent to take into account the evolutions of digital technologies. It enables the CNIL to monitor the implementation of all regulations relating to the protection of personal data, following a complaint filed by a citizen, a request by a data protection agency from another European member state, or on its own initiative.

CNIL's wide-ranging powers and the possible consequences for the structure being controlled, especially in terms of public relations, usually lead data controllers and data protection officers inside the structure to fear such an eventuality. There are two possible strategies to overcome this fear: a structure can react either when the CNIL is knocking on its door, or earlier through the pro-active elaboration of a suitable procedure for the structure. While our law firm Cabinet Mathias can accompany its clients in both cases, this White paper aims to encourage data controllers to opt for the latter solution.

I. Le contrôle de la Cnil : connaître le contexte

Les visites de contrôle des Commissions Nationales de l'Informatique et des Libertés (Cnils) en Europe sont en pleine expansion et cette tendance va sans nul doute continuer. En 2012, la Cnil française a effectué 458 contrôles, soit une augmentation de 19% par rapport à 2011. A partir de 2004, le nombre des inspections a connu une hausse significative, notamment grâce au renforcement des pouvoirs de la Commission et à la revalorisation de son budget. Toutefois, une légère diminution des contrôles est à noter ces deux dernières années : 414 ont été effectués en 2013 et 421 ont été effectués en 2014.

Evolution des contrôles et des effectifs de la Cnil



Source : Rapports d'activité de la Cnil

Les missions de contrôle sont encadrées par la loi du 6 janvier 1978[1] modifiée le 6 août 2004 et par le décret du 20 octobre 2005[2] modifié par le décret du 25 mars 2007.

Afin de faire face à un audit sur la protection des données, les entreprises se doivent d'être proactives et ne négliger aucune étape dans la gestion de la procédure d'inspection. En effet, outre les éventuelles sanctions financières qui pourraient être ordonnées, tout contrôle emporte des risques en termes d'image de l'entreprise et d'atteinte à sa réputation. A noter que, parfois, la non-conformité est identifiée une fois l'inspection menée. Ainsi, la continuité des activités peut être remise en cause, même pour des sociétés qui semblent, au premier abord, en totale conformité avec la loi Informatique et Libertés.

[1]Articles 11-2°- f et 44 de la loi du 6 janvier 1978 modifiée le 6 août 2004.
[2]Articles 61 à 69 du décret du 20 octobre 2005 modifié par le décret du 25 mars 2007.

Par cet article, nous souhaitons sensibiliser les sociétés sur la manière de gérer les contrôles de la Cnil et sur la manière de s'y préparer.

* *
*

II. Pourquoi une société, une administration ou une association est-elle auditée ?

Bien souvent, les organismes sont sélectionnés pour des audits sur le respect de la protection des données à caractère personnel pour une ou plusieurs des raisons suivantes[3] :

- **Lorsque l'organisme est inscrit dans le programme annuel de la Cnil.** En effet, en France, la Cnil publie tous les ans un programme indiquant les secteurs et les activités de traitement de données pour lesquels un contrôle sera mené l'année suivante. Par exemple, dans le programme de 2012, la Cnil avait planifié 450 contrôles afin de savoir comment les opérateurs de télécommunication et les développeurs d'application utilisaient les données personnelles collectées depuis les Smartphones. (11PVLR709, 21/04/2012).

- **Lorsqu'un particulier a fait un recours auprès de la Cnil.** Les recours de la part des particuliers sont en forte hausse ces dernières années. Cette recrudescence peut être liée à une prise de conscience par le public des droits relatifs à la protection de la vie privée. A ce titre, la Commission européenne et le Conseil National du Numérique travaillent très activement sur l'éducation des citoyens européens sur les questions relevant de la protection des données et du droit au respect de la vie privée.

- **Si une autre autorité publique suspecte ou constate une non-conformité à la réglementation relative à la protection des données personnelles et qu'elle en a alerté la Cnil.** La Commission peut opérer un contrôle notamment à la suite d'informations transmises par la Cnil d'un autre État membre, par une association de protection des consommateurs ou par tout autre autorité publique avec laquelle un partenariat serait mené concernant la protection des données. A titre d'illustration, en vertu d'un protocole de coopération conclu en 2011, la Cnil doit être informée des atteintes au respect de la vie privée révélées lors d'une inspection par la Direction générale de la Concurrence, de la Consommation et de la Fraude (DGCCRF). A noter que cette coopération a été légalement consacrée par la loi relative à la consommation.[4] Pour information, la Cnil était saisie le 24 avril 2013 par une députée européenne sur la pratique de "l'IP tracking" mise en œuvre par certains sites de vente de billetterie et de voyage en ligne.

[3] Le 35ème rapport d'activité dévoilé par la Cnil le 16 avril 2015 précise que pour l'année 2014 :
•28 % des contrôles résultent du programme annuel décidé chaque année par la Commission ;
•24 % des contrôles s'inscrivent dans le cadre de l'instruction de plaintes ;
•40 % des contrôles sont effectués à l'initiative de la CNIL, notamment au vu de l'actualité ;
•6 % des contrôles font suites à un courrier d'observation adressé après un premier contrôle ;
•2 % des contrôles sont réalisés dans le cadre des suites de mises en demeure ou de procédures de sanction.

[4] L'article L.141-1-VI du Code de la consommation dispose que « *VI.-Dans l'exercice de leurs missions, les agents mentionnés au II de l'article L. 450-1 du code de commerce sont habilités à constater les infractions et manquements aux chapitres II, IV et V de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et peuvent communiquer ces constatations à la Commission nationale de l'informatique et des libertés.* ». Pour une analyse de l'impact de la loi relative à la consommation sur l'action de la Cnil voir *Comment la loi relative à la consommation du 17 mars 2014 renforce-t-elle l'action de la Cnil ?*sur le blog du Cabinet Mathias (http://www.avocats-mathias.com/blog)

Cette pratique permettrait de moduler, à la hausse en général, le prix de vente du billet proposé au consommateur à chaque nouvelle visite du site grâce à l'enregistrement de son adresse IP. Sur le fondement du protocole précité, la Cnil et la DGCCRF ont pu diligenter une enquête au terme de laquelle la pratique combinant modulation de tarif et adresse IP n'a pas été constatée.[5]

● **Si l'attention des médias s'est portée sur l'entreprise.** C'est le cas par exemple lorsqu'une importante violation des données a été rendue publique. L'examen de la violation de données personnelles dont l'opérateur télécom historique a été victime en janvier 2014 est en cours d'analyse par les services de la Cnil.[6]

● **Si l'inspection fait suite à une déclaration ou une demande d'autorisation.** Certaines autorités de protection de données procèdent à une enquête après avoir reçu des requêtes d'inscriptions ou d'autorisation qui révèlent des non conformités dans certains domaines.

● Si un contrôle a eu lieu dans une filiale de l'entreprise ou dans une autre société dans le même secteur et a rendu publiques les informations.

* *
*

III. Cadre juridique général et juridictions

Les pouvoirs des Cnils sont actuellement encadrés dans l'Espace Economique Européenne (EEE) par le droit national de chaque État membre, transposant la directive 95/46/CE sur la protection des données. Les lois relatives aux pouvoirs des Cnils diffèrent donc au sein de l'Espace Economique Européen, composé des 28 membres de l'Union Européenne ainsi que de l'Islande, du Liechtenstein et de la Norvège.

Actuellement, la directive dispose[7] que chaque Cnil est compétente sur le territoire de l'État membre duquel elle dépend. Cependant, chaque Cnil peut se voir appelée à exercer ses pouvoirs par la Cnil d'un autre Etat membre. Elles doivent par ailleurs coopérer dans la mesure nécessaire au bon exercice de leurs fonctions.

Par exemple, en 2012, les Cnils estonienne et lettone ont publié conjointement les recommandations qu'elles avaient faites à une société. En effet, les deux Cnils avaient été amenées à coopérer dans le cadre d'un contrôle impliquant les deux Etats membres.

---

[5] *IP Tracking : conclusions de l'enquête conjointe menée par la Cnil et la DGCCRF*, Article de la Cnil du 27 janvier 2014. Pour une analyse de cette affaire voir *L'IP Tracking : enquête de la Cnil en cours* sur le blog du Cabinet Mathias (http://www.avocats-mathias.com/blog)

[6] *Violation de données personnelles : la Cnil réunit les opérateurs de communication électronique*, Article de la Cnil du 5 février 2014

[7] L'article 28§6 de la directive dispose que « *Indépendamment du droit national applicable au traitement en cause, chaque autorité de contrôle a compétence pour exercer, sur le territoire de l'État membre dont elle relève, les pouvoirs dont elle est investie conformément au paragraphe 3. Chaque autorité peut être appelée à exercer ses pouvoirs sur demande d'une autorité d'un autre État membre.* »

Cependant, malgré ces efforts de coopération, les pouvoirs de chaque Cnil ne peuvent pas s'étendre au-delà du territoire de l'Etat membre dont elle dépend et restent donc très limités.

En effet, les récentes recommandations[8] de la Commission de la protection de la vie privée, Cnil belge, à l'attention de Facebook, des éditeurs de sites utilisant les plug-ins "j'aime" ou "partager" du réseau social et des utilisateurs ne valent que pour le territoire belge alors même que tous les citoyens et éditeurs de site Internet européens sont potentiellement concernés. En l'espèce, la Cnil belge a procédé à un examen du fonctionnement des plug-ins "j'aime" ou "partager" de Facebook. A cette occasion, elle a constaté que le réseau social pouvait suivre les internautes et analyser leurs activités sur l'Internet qu'ils soient ou non utilisateurs du réseau social ou connectés audit réseau.

Les sociétés qui ont exécuté les clauses contractuelles types pour le transfert de données personnelles en dehors de l'EEE, ou celles qui ont adopté des règles d'entreprise contraignantes, doivent également accepter de soumettre leurs opérations au contrôle d'une Cnil européenne. Le *Safe harbor* prévoit d'ailleurs une telle coopération concernant les données « Ressources humaines ». Cependant, lorsqu'elles adhèrent aux principes du *Safe harbor*, les entreprises n'acceptent pas toutes l'engagement de coopération. Pour rappel, le *Safe habor* est un corps de règles relatif à la protection des données personnelles négocié entre la Commission européenne et les autorités américaines. Basé sur le volontariat, il a pour but de permettre aux entreprises qui y adhèrent de recevoir des données personnelles en provenance de l'Union européenne en garantissant qu'elles bénéficieront d'une protection suffisante. A noter que les récentes révélations concernant des programmes américains de collecte de renseignements ont conduit la Commission européenne à définir de nouveaux moyens pour sécuriser les transferts de données outre-Atlantique.[9] En outre, l'Union européenne et les Etats-Unis se sont engagés à renforcer le cadre

[8] http://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_04_2015.pdf
La Cnil belge recommande notamment que :

- le réseau social doit notamment renoncer au placement systématique de cookies d'identification unique de longue durée chez les non-utilisateurs, ainsi qu'à toute collecte et utilisation de données par le biais de cookies et de modules sociaux. Les données des utilisateurs ne doivent pas davantage être collectées sauf consentement là encore.
- les éditeurs de sites l'utilisation d'outils tels que "Social Share Privacy" pour obtenir le consentement de l'utilisateur et ainsi ne permettre la connexion avec des serveurs de tierces parties déclenchant l'envoi des données qu'une fois que l'utilisateur a cliqué sur le module social.
- les utilisateurs désireux de se protéger du traçage réalisé par Facebook d'utiliser des modules complémentaires (add-ons) de navigateur qui bloquent le traçage dont elle donne des exemples, d'avoir recours à la navigation privée disponible via les navigateurs couramment utilisés (Internet Explorer, Firefox, Chrome, Safari par exemple) et de se désinscrire du traçage dans le cadre de publicités ciblées par Facebook via le site Internet d'opt-out de la European Interactive Digital Advertising Alliance (www.youronlinechoices.eu).

[9]La Commission européenne appelle les États-Unis à rétablir la confiance dans les transferts de données entre l'UE et les Etats-Unis, 27 novembre 2013

juridique du *Safe harbor* dans une déclaration conjointe du 26 mars 2014[10]. Le *Safe harbor* fera également l'objet d'une attention particulière des juges de la Cour de Luxembourg[11].

Bien que ces instruments de protection des données soient utilisés, les Cnils n'ont pas les ressources suffisantes pour effectuer les contrôles sur le site des sociétés en dehors de l'EEE. Ainsi, même s'il y a un risque théorique de contrôle, les mises en pratique sont rares.

Il est à prévoir que l'accroissement des pouvoirs des Cnils, comme c'est le cas en France avec l'adoption de la loi Hamon notamment, entraînera une augmentation du nombre des contrôles. Afin d'éviter les sanctions, il est donc conseillé aux sociétés des États membres de l'EEE de ne pas seulement planifier ou notifier les contrôles mais surtout de mettre en place des pratiques, des politiques et des procédures afin de gérer tous les contrôles.

Il faut enfin préciser que les agents de la Cnil ne procèdent aux investigations que sur décision du Président de la Commission après proposition du service des contrôles. Les agents de la Cnil participant aux contrôles sont habilités à cet effet. A noter que la liste de ces agents est publiée sur le site Internet de la Cnil[12]. Ils peuvent être assistés d'experts. Le contrôle peut se dérouler après que le responsable de traitement en ait été informé ou non. Cette décision est prise en opportunité par la Cnil. De plus, le procureur de la République territorialement compétent est informé de la date, de l'heure et de l'objet du contrôle avant que celui-ci ne débute.[13]

Par ailleurs, lorsque le contrôle de la Cnil est effectué à la demande[14] d'une autorité de contrôle d'un Etat membre de l'Union européenne, les contrôleurs sont tenus d'en informer le responsable de traitement. Ils doivent également l'informer de ce que les informations collectées au cours des vérifications pourront être transmises à la Cnil « étrangère ».

[10]Join statement, EU-US Summit, 26 mars 2014

[11]La Cour de Justice de l'Union Européenne (CJUE) devrait se prononcer sur la validité de l'accord « Safe harbor » suite à une question préjudicielle de la Haute Cour de justice irlandaise du 25 juillet 2014 qui examinait une plainte déposée contre Facebook par un citoyen autrichien (Affaire C-362/14)

[12]L'article 52 du règlement intérieur de la Cnil prévoit que « *La commission diffuse sur son site la liste des agents habilités à procéder à des missions de contrôle.* »

[13]L'article 61 du décret n°2005-1309 prévoit que « *Lorsque la commission décide un contrôle sur place, elle en informe préalablement par écrit le procureur de la République dans le ressort territorial duquel doit avoir lieu la visite ou la vérification. Le procureur de la République est informé au plus tard vingt-quatre heures avant la date à laquelle doit avoir lieu le contrôle sur place. Cet avis précise la date, l'heure, le lieu et l'objet du contrôle*. »

[14]L'article 63 du décret n°2005-1309 prévoit que « *Lorsqu'en application de l'article 49 de la loi du 6 janvier 1978 susvisée la commission procède à des vérifications, à la demande d'une autorité exerçant des compétences analogues aux siennes dans un autre Etat membre de la Communauté européenne, elle en informe le responsable du traitement. Elle l'informe également que les informations recueillies ou détenues par la commission sont susceptibles d'être communiquées à cette autorité.* »

Mise à jour Mai 2015

La Cnil dispose, depuis la modification de l'article 44 de la loi « Informatique et Libertés » par la loi « Hamon » relative à la consommation du 17 mars 2014, d'un nouveau moyen de contrôle qui permet de procéder à des constatations en ligne, depuis ses propres locaux, à partir d'un ordinateur connecté à internet, et sans la présence du responsable du traitement.

La Cnil détient désormais un pouvoir d'investigation adapté au développement numérique, et peut ainsi constater et agir en cas de failles de sécurité sur Internet pouvant affecter les données personnelles.
Ce nouveau pouvoir de contrôle permet à la Cnil de vérifier plus spécifiquement certains aspects de la loi « Informatique et Libertés », notamment :

- la pertinence des données collectées (article 6 de la loi) ;
- les mentions d'information à destination du public (article 32) ;
- la sécurité des données collectées et traitées (article 34) ;
- la réalité des formalités juridiques (articles 22 et suivants).

Ce contrôle en ligne permet également de vérifier la conformité des pratiques des organismes à la recommandation cookies et autres traceurs adoptée par la Cnil le 5 décembre 2013. Ainsi la Cnil vérifiera :

- le nombre et la nature des cookies déposés sur le poste informatique de l'utilisateur ;
- les modalités d'informations à destination du public en matière de cookies ;
- la qualité et la pertinence de l'information ;
- les modalités de recueil du consentement de l'utilisateur.

Ce nouveau pouvoir s'applique aux données librement accessibles ou rendues accessibles en ligne, y compris par imprudence, par négligence ou par le fait d'un tiers ; la Cnil effectue son contrôle au plus près de l'expérience de l'utilisateur.
Il ne donne pas, évidemment, la possibilité à la Cnil de forcer les mesures de sécurité mises en place pour pénétrer dans un système d'information.

En pratique, le contrôle en ligne peut être indépendant ou complémentaire d'un contrôle sur place, sur pièce ou sur audition.
Il se déroule de façon similaire au contrôle sur place : une décision de contrôle est prise par la Présidente, un ordre de mission désigne les personnes chargées de réaliser le contrôle et un procès-verbal de constatation est rédigé.
Cependant, le contrôle et le procès-verbal ne sont pas effectués de manière contradictoire. Le procès-verbal de constatation et les vérifications de l'environnement de contrôle sont adressés dans les 8 jours qui suivent le contrôle au responsable du traitement pour qu'il y apporte ses observations dans le délai imparti.

Au terme de la procédure, la Cnil décide si les constations doivent donner lieu à une mise en demeure (généralement une mise en conformité avec la loi) ou, selon la gravité des faits, à une procédure de sanction.

Avec ces nouveaux pouvoirs, les éditeurs de site internet et d'application mobiles peuvent à tout moment faire l'objet de contrôle à distance par la Cnil.

Le programme des contrôles de la Cnil pour l'année 2014 prévoyait, à ce titre, un objectif de 550 contrôles dont environ 200 contrôles en ligne. Toutefois, le rapport d'activité rendu public le 16 avril 2015 fait état de 421 contrôles effectués dont 58 en ligne réalisés entre octobre et décembre 2014. Ces contrôles portaient sur diverses thématiques dont notamment la conformité des pratiques des acteurs du web à la recommandation cookies et autres traceurs.

IV. Comment préparer et gérer un contrôle ?

L'objectif des contrôles est d'évaluer si une société, une administration ou une association se soumet aux différentes règles de la protection des données telles que :

- les déclarations et les autorisations ;
- la correspondance des traitements mis en œuvre avec les formalités effectuées auprès de la Cnil ou les inscriptions au registre du correspondant à la protection des données à caractère personnel (« Correspondant Informatique et Libertés » ou CIL) ;
- les limitations de la finalité du traitement ;
- le respect des durées de conservation ;
- les mécanismes de transfert en dehors de l'EEE ;
- la gestion des relations clients ;
- les mesures de sécurité adéquate et la mise en œuvre des procédures et politiques des droits du respect à la vie privée ;
- les politiques d'accès et de rectification ;
- les activités de surveillance des salariés ; etc.

La plupart des lois nationales de protection des données contiennent des dispositions générales sur les pouvoirs de contrôle des CNIL, mais certaines Cnils, par exemple, celles d'Irlande et du Royaume-Uni ont publié des guides concernant les procédures, des exemples de questions et des modèles de rapports et de documents.

*

A] Anticiper le contrôle de la Cnil : les prérequis

Les politiques de protection des données personnelles déjà mises en place au sein de l'entreprise sont des facteurs importants dans la gestion les contrôles. Les sociétés qui sont conscientes des risques et qui y sont préparées seront en mesure de gérer efficacement les contrôles.

Effectuer un audit. La première étape pour une entreprise est de se pencher sur la conformité aux lois nationales et mettre en place les changements nécessaires. La conformité minimale prend en compte : l'information des particuliers sur la collecte et le traitement de leurs données personnelles, la mise en place de procédures et de politiques écrites (par exemple sur la sécurité des données, la conservation des données), et si cela est nécessaire, la désignation d'un correspondant à la protection des données à caractère personnel (« Correspondant Informatique et Libertés »).

Les agents de la Cnil procèdent à un contrôle préliminaire de l'entreprise sans visiter les locaux. Par exemple, la Cnil va consulter les rapports d'audits existants, vérifier les registres de la société ou le site internet de l'entreprise pour savoir si des données à caractère personnel sont collectées en ligne. Le récent pouvoir de contrôle en ligne de la Cnil consacré par la loi relative à la consommation facilitera cette dernière vérification.

Un bon niveau de conformité permet de préparer l'entreprise et ses employés aux contrôles. Une formation régulière ainsi qu'une connaissance des obligations générales de l'entreprise et de ses salariés permettra notamment de minimiser les risques de non-conformité.

Anticiper et organiser des formations. Il apparaît judicieux de développer une procédure qui énonce comment réagir à la visite de la Cnil. Le plan permet notamment de déterminer qui devrait notifier le contrôle, quels sont les bureaux et les ressources mises à disposition des agents. Les employés devront également être sensibilisés sur le rôle qu'ils pourront avoir à jouer lors de l'inspection. Par exemple :

- Les employés devront être formés sur le rôle et les pouvoirs de la Cnil. La formation devra inclure des sujets comme : la manière de répondre aux questions, la manière de communiquer les documents, les risques d'une obstruction à l'enquête, lorsque des informations fausses ou trompeuses sont communiquées, etc.

- Les réceptionnistes et les gardiens devront également être formés sur la manière dont il faut accueillir les agents et les personnes qu'ils devront informer de leur arrivée. Ainsi devront-ils immédiatement contacter leur avocat conseil spécialisé en la matière ainsi que le Correspondant Informatique et Libertés ou l'agent responsable de la protection des données (même si cela conduit à interrompre une réunion) puis demander aux agents d'attendre dans une salle de réception ou de conférence jusqu'à ce qu'un responsable se présente.

Former une « équipe d'inspection ». Les sociétés peuvent créer une « équipe d'inspection » qui inclut les principaux responsables pour gérer le contrôle. Il peut ainsi s'agir du Correspondant Informatique et Libertés ou de la personne responsable de la protection des données si aucun CIL n'a été désigné, du directeur juridique, du DSI, du RSSI et des responsables des départements les plus importants (comme les DRH ou le directeur marketing par exemple). Il pourrait alors être intéressant de prévoir une procédure incluant la composition de l'équipe, leurs devoirs et responsabilités, la manière d'accueillir et d'accompagner les agents le temps de leur contrôle, la manière de répondre à leurs questions, la coordination avec les autres employés, la présence aux entretiens, etc.

Les membres de l'équipe devront alors être informés directement d'une visite de la Cnil. Ainsi, leurs numéros de téléphones devront-ils être visibles dans les bureaux afin de pouvoir les contacter au plus vite s'ils ne sont pas présents et que l'entreprise fait face à un contrôle imprévu.

Informer les employés. La société devra faire en sorte que ses employés soient au courant d'une probabilité de contrôle sur la question de la vie privée. Il est nécessaire qu'ils sachent à quoi s'attendre lors du contrôle et de son impact éventuel. Si les employés sont préparés, ils seront alors mieux à même de répondre aux questions de la Cnil et d'identifier les documents demandés.

Préparer les documents demandés[15] par la Cnil. Il peut arriver qu'avant de se déplacer sur les lieux de mise en œuvre des traitements, la Cnil demande à un organisme de lui communiquer certains documents. C'est

[15]L'article 54 du règlement intérieur de la Cnil prévoit que « *Lorsque le responsable de traitement est informé que la commission va diligenter un contrôle dans ses locaux, il peut lui être demandé de préparer tous documents de nature à faciliter le déroulement du contrôle.* »

généralement le cas lorsque le contrôle est préalablement notifié au responsable de traitement. Ces documents pourront par exemple permettre à la Cnil de prendre connaissance de la politique de sécurité mise en place.

*

B] Pendant le contrôle

A leur arrivée, les agents notifient au responsable des lieux la décision du Président de la Cnil autorisant le contrôle.

Autorisation. La première chose à faire est de vérifier les accréditations des agents pour la mise en œuvre du contrôle. L'accréditation spécifie la raison et le but du contrôle. Bien souvent, les agents vont produire une note explicative. Les représentants de la société devront alors déterminer la portée du contrôle, notamment afin de savoir si celui-ci se concentre sur un secteur en particulier (le service client, les ressources humaines, etc.) ou bien encore si le contrôle est dû à une visite prévue dans le cadre du programme annuel de la Cnil. Il faudra aussi déterminer quelle est la durée du contrôle.

Droit d'opposition à la visite. En France, avant 2011, les contrôles sur site pouvaient être conduits sans aucun avertissement et sans la possibilité de s'y opposer. L'article 44 de la loi Informatique et Libertés, dans sa version antérieure à la loi du 29 mars 2011, prévoyait simplement qu'en cas d'opposition au contrôle, celui-ci pourrait avoir lieu après l'autorisation du président du tribunal de grande instance.

Toutefois, l'ingérence de la Cnil dans les locaux des responsables de traitement contrôlés est admise pour autant qu'elle soit assortie de « garanties effectives et appropriées » au regard de la finalité du contrôle. Pour le Conseil d'Etat, cette garantie résulte de l'information du responsable des lieux sur sa faculté de s'opposer à la visite de la Cnil sachant qu'elle pourra ensuite être autorisée par un juge. Aussi, depuis la loi du 29 mars 2011[16], la Cnil doit informer[17] la société de sa visite et de son droit à s'y opposer[18]. La notification est souvent envoyée quelques jours avant ou le matin même du contrôle. Si la société s'y oppose, un procès-verbal[19] constate cette opposition et la visite ne peut avoir lieu que si le juge l'autorise. La décision devra alors être rendue dans les 48 heures. Dans le

[16]Loi n°2011-334 du 29 mars 2011 relative au défenseur des droits (art.7-1°)

[17]L'article 62 du décret du 20 octobre 2005 modifié par le décret du 25 mars 2007 dispose que « *Lorsque la commission effectue un contrôle sur place, elle informe au plus tard au début du contrôle le responsable des lieux de l'objet des vérifications qu'elle compte entreprendre, ainsi que de l'identité et de la qualité des personnes chargées du contrôle. […]* »

[18]L'article 44-II de la loi Informatique et Libertés dispose que « *Le responsable de locaux professionnels privés est informé de son droit d'opposition à la visite. Lorsqu'il exerce ce droit, la visite ne peut se dérouler qu'après l'autorisation du juge des libertés et de la détention du tribunal de grande instance dans le ressort duquel sont situés les locaux à visiter, qui statue dans des conditions fixées par décret en Conseil d'Etat. Toutefois, lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie, la visite peut avoir lieu sans que le responsable des locaux en ait été informé, sur autorisation préalable du juge des libertés et de la détention. Dans ce cas, le responsable des lieux ne peut s'opposer à la visite.* »

[19]L'article 56 du règlement intérieur de la Cnil prévoit que « *La décision du responsable des lieux de s'opposer à la tenue du contrôle donne lieu à la rédaction d'un procès-verbal par les agents de la commission. Dans l'hypothèse où le responsable exerce ce droit au cours de la mission, le procès-verbal mentionne les raisons qui ont mené le responsable à prendre cette décision. Le fait, pour le responsable, de s'opposer à certains actes de contrôle après avoir permis aux agents de la commission de pénétrer dans les lieux est regardé comme l'exercice de son droit d'opposition. Dans ce cas, les agents de la commission peuvent décider d'interrompre le contrôle et dresser un procès-verbal faisant état de cette opposition. En cas de refus de signature du procès-verbal, celui-ci est notifié au responsable de traitement par tout moyen postérieurement au contrôle.* »

cas où l'urgence ou la gravité le justifie, ou s'il y a un risque de destruction des preuves, la visite peut avoir lieu sans avertissement et la société ne pourra pas s'y opposer s'il y a déjà eu une autorisation judiciaire en ce sens.

Durée et moment de l'inspection. La durée du contrôle peut aller de plusieurs jours à plusieurs semaines. A noter que même des visites de routine peuvent conduire à des contrôles de plusieurs semaines ou plus.

En règle générale, c'est l'ordre du jour de l'agent qui déterminera le programme de la visite. Les agents indiqueront ainsi ce qu'ils souhaitent faire et quand. Il est important de discuter de l'ordre du jour à l'avance puisque cela permet à la société de mieux organiser les ressources nécessaires pour rassembler les informations et pour planifier les entretiens des employés. De plus, planifier à l'avance le déroulement du contrôle permettra de limiter les perturbations dans les activités de l'entreprise tout en permettant aux employés interrogés de revoir leurs calendriers.

Les agents se rendront bien souvent dans les locaux de l'entreprise pendant les horaires normaux de travail. A noter que les agents de la Cnil peuvent entrer dans les locaux de l'entreprise entre 6h00 et 21h00.

La logistique. Une fois que les agents sont arrivés, ils doivent être accompagnés dans une salle où ils pourront travailler mais ils ne doivent pas être perdus de vue. La pièce qui leur est attribuée doit pouvoir réunir les agents ainsi qu'une équipe de taille similaire de la société. Une table pour les documents à consulter doit également se trouver dans la salle, tout comme un téléphone, des papiers et des crayons. Par ailleurs, en plus de cette pièce de contrôle, un lieu pour leur permettre de faire des photocopies et d'estampiller les documents doit leur être attribué.

Il est par ailleurs important de faire savoir aux agents que le personnel (qui aura été formé à de tels contrôles) est à leur disposition et qu'ils peuvent leur demander l'assistance dont ils ont besoin. Il peut également être intéressant de rappeler aux employés qu'ils ne doivent pas écrire de mail, de mémos ou tout autre document sur le contrôle. Exception faite si leurs managers, l'équipe juridique ou « l'équipe d'inspection » le demande.

Les pouvoirs de l'agent. La mission de contrôle vise prioritairement à obtenir copie du maximum d'informations, techniques et juridiques, pour apprécier les conditions dans lesquelles sont mis en œuvre des traitements informatiques. Pour y parvenir, les agents des Cnils disposent d'un large pouvoir dans la manière de mener leurs visites. Ils doivent notamment pouvoir compter sur la pleine collaboration du responsable de traitement contrôlé tenu, en vertu de l'article 21[20] de la loi, de « *prendre toutes mesures utiles afin de faciliter [la] tâche* » de l'autorité de contrôle.

[20] Dans l'exercice de leurs attributions, les membres de la commission ne reçoivent d'instruction d'aucune autorité. Les ministres, autorités publiques, dirigeants d'entreprises publiques ou privées, responsables de groupements divers et plus généralement les détenteurs ou utilisateurs de traitements ou de fichiers de données à caractère personnel ne peuvent s'opposer à l'action de la commission ou de ses membres et doivent au contraire prendre toutes mesures utiles afin de faciliter sa tâche.
Sauf dans les cas où elles sont astreintes au secret professionnel, les personnes interrogées dans le cadre des vérifications faites par la commission en application du f du 2° de l'article 11 sont tenues de fournir les renseignements demandés par celle-ci pour l'exercice de ses missions.

Généralement, les lois disposent que les agents peuvent accéder à tout endroit, locaux, équipements ou bâtiments qui sont utilisés dans le cadre du traitement des données personnelles à des fins professionnelles[21]. Les agents sont par ailleurs autorisés à regarder et à demander des copies de documents, à s'entretenir avec le personnel, à examiner et imprimer les données stockées de façon électronique. Ils peuvent également effectuer des contrôles sur tout outils, support de données ou système informatique utilisé pour le traitement des données mais aussi demander des explications écrites ou orales. La Cnil a déjà prononcé un avertissement public[22] pour défaut de coopération notamment contre une société qui avait ignoré une trentaine de courriers qu'elle avait envoyés et deux convocations suite à l'impossibilité à procéder un contrôle sur place.

Demandes de documents. Les documents demandés peuvent être nombreux.

Les demandes suivantes sont bien souvent celles qui posent problème :

- Les documents fournis aux agents doivent répondre à leur demande mais ne doivent pas aller au-delà. Bien souvent, à moins qu'il y ait une demande expresse ou qu'une réponse soit incomplète sans un document, les questions peuvent être rendues sans communiquer de document.

- « L'équipe d'inspection » doit identifier tout problème de logistique quand elle répond à la requête des agents. Cela peut être, par exemple, la récupération de documents à partir d'endroits éloignés/distants (par exemple lorsque les documents sont détenus par des filiales). L'agent ne comprend pas toujours l'organisation de la société et le procédé de gestion des documents. Cependant, les représentants de la société devront s'abstenir de questionner sur la pertinence du document demandé. Ils devront plutôt expliquer aux agents leurs difficultés et demander ainsi un laps de temps approprié à la remise des documents.

- Malgré leur large autorité, les agents peuvent demander des documents qui vont au-delà de leur étendue de pouvoir. C'est par exemple le cas lorsque leurs demandes portent sur des informations concernant les finances, les secrets commerciaux, la performance des employés ou leurs fichiers médicaux. La décision de communiquer ou de garder ces documents doit être prise par les représentants en consultation avec les avocats. Il est nécessaire d'avoir une note décrivant toutes les différences d'opinion entre la société et les agents en ce qui concerne les documents considérés hors de leurs domaines d'application. De manière alternative, la société peut proposer que les documents soient examinés mais pas photocopiés. Dans tous les cas, les documents sensibles devront être marqués comme étant « confidentiels » avant toute copie.

- « L'équipe d'inspection » devra garder une liste des documents qui auront été communiqués aux agents, en faisant, par exemple, référence à la date ou à la version du document. Il lui faudra également garder les copies de tous les documents ou extraits de documents emmenés par les agents. Il ne faudra pas oublier non plus de dresser la liste des éléments demandés par les agents mais qui ne leur ont pas été délivrés.

[21]Par exemple, l'article 44-I de la loi Informatique et Libertés dispose que « *Les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de l'article 19 ont accès, de 6 heures à 21 heures, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé.* »

[22]Délibération de la formation restreinte n°2012-156 du 1er juin 2012 portant avertissement à l'encontre de la société YATEDO FRANCE

Entretiens avec les employés. Les agents demandent toujours des entretiens avec le personnel de la société et il peut leur arriver de demander à voir une personne en particulier. Normalement, il faut répondre positivement à cette demande. A noter que parfois, les contrôleurs peuvent s'entretenir avec une autre personne suggérée par « l'équipe d'inspection ». Il faut cependant garder à l'esprit que la non-présentation de l'employé convoqué pour un entretien peut être interprétée comme une entrave à l'inspection.

Sous réserve de l'accord exprès du supérieur hiérarchique, de l'équipe juridique ou de « l'équipe d'inspection », les personnes entendues par les agents peuvent tenir un journal de suivi de l'entretien qui pourra éventuellement être utilisé pour enrichir le procès-verbal établi en fin de contrôle.

Lorsque l'organisme est prévenu du contrôle avant le jour de son déroulement, « l'équipe d'inspection » doit s'interroger sur les personnes qui seront probablement appelées à s'entretenir avec les agents. Des réunions devront donc être planifiées avec le personnel identifié afin de discuter des domaines possibles de contrôle, pour déterminer quels documents peuvent être demandés et les préparer à toute question probable. A noter que l'équipe d'inspection de la société devra être présente pendant l'entretien.

Les réunions. Si les agents sont d'accord, il serait bon de commencer et de finir chaque journée par une réunion entre l'équipe d'inspection et les agents.

Procès-verbal. Un procès-verbal de fin de mission est établi contradictoirement à l'issue du contrôle dont le contenu est prévu par le décret d'application de la loi[23] Il est important de garder une trace écrite des étapes du contrôle et de toutes les communications avec les agents. Le procès-verbal doit inclure toutes les questions ou demandes de la Cnil, toutes les réponses à celles-ci, le nom de la personne qui y a répondu puis enfin, la satisfaction ou non de l'agent. Les procès-verbaux permettent de conserver une trace du contrôle qui pourra servir à contredire les conclusions des agents mais aussi à préparer au mieux les prochains contrôles. Il est important de noter que lorsque le contrôle de la Cnil est effectué en ligne, le procès-verbal de la Cnil n'est pas contradictoire.

S'opposer au contrôle. Dans certains domaines, la société a le droit de s'opposer ou de ne pas procéder à la rédaction d'informations confidentielles. Cependant, s'opposer aux demandes des agents, lui refuser le droit d'accéder aux locaux ou à des documents ou tout autre refus pourra être perçu comme une entrave au contrôle et peut donc naturellement conduire à une mauvaise vision de la société et/ou ses représentants. Empêcher les agents de mener à bien leurs tâches est punissable d'une peine d'un an d'emprisonnement et d'une amende de 15 000€ d'amende. Conformément à l'article 51[24] de la loi Informatique et Libertés, le délit d'entrave à l'action de la Cnil est constitué par :

---

[23] L'article 63 du décret n°2005-1309 prévoit que « *Les missions de contrôle sur place font l'objet d'un procès-verbal.*
Le procès-verbal énonce la nature, le jour, l'heure et le lieu des vérifications ou des contrôles effectués. Il indique également l'objet de la mission, les membres de celle-ci présents, les personnes rencontrées, le cas échéant, leurs déclarations, les demandes formulées par les membres de la mission ainsi que les éventuelles difficultés rencontrées. L'inventaire des pièces et documents dont les personnes chargées du contrôle ont pris copie est annexé au procès-verbal.
Lorsque la visite n'a pu se dérouler, le procès-verbal mentionne les motifs qui ont empêché ou entravé son déroulement, ainsi que, le cas échéant, les motifs de l'opposition du responsable des lieux ou de son représentant.
Le procès-verbal est signé par les personnes chargées du contrôle qui y ont procédé et par le responsable des lieux ou par son représentant. En cas de refus ou d'absence de signature, mention en est portée au procès-verbal.
Le procès-verbal est notifié au responsable des lieux et au responsable des traitements par lettre recommandée avec demande d'avis de réception. »

[24] « *Est puni d'un an d'emprisonnement et de 15 000 euros d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés :*

- l'opposition à l'exercice des missions confiées aux agents de la Cnil lorsque la visite a été autorisée par le juge ;
- le refus de communiquer aux agents de la Cnil les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les détruisant ;
- la communication d'informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible.

Lorsqu'elle constate un délit d'entrave, la Cnil peut dénoncer les faits au Procureur de la République. Le Tribunal de grande instance de Paris a, par exemple, prononcé une amende de 5 000€ dont 4 000€ avec sursis sur le fondement de l'article 51 de la loi Informatique et Libertés suite au refus du Directeur général de l'entreprise contrôlée de permettre aux agents de la Cnil de poursuivre leur investigations alors que le Président directeur général, désigné responsable des lieux, ne s'était pas opposé au contrôle.[25]

*

C] Après le contrôle

A la suite du contrôle, les membres de « l'équipe d'inspection » de la société devront notamment :

- savoir si les documents communiqués et les explications donnés étaient suffisants ;
- chercher à savoir si tout facteur pertinent au contrôle a été mis en avant ;
- se demander s'il est nécessaire de corriger une mauvaise impression sur la société de la part des agents.

Selon le résultat du contrôle (notamment si des sanctions sont à prévoir), « l'équipe d'inspection » va devoir déterminer quelles actions doivent être prises afin de remédier aux violations constatées.

Rapport. A la suite du contrôle, les agents vont présenter un rapport final incluant les dossiers et les résultats du contrôle opéré.

Le résultat du contrôle. A la fin du contrôle, la Cnil envoie une copie du rapport à la société. Tout non-respect identifié doit être traité dans le laps de temps prévu par la Cnil. A noter qu'il est nécessaire que les actions correctrices envisagées soient documentées.

A la suite du contrôle, l'autorité de contrôle peut demander à la société des informations additionnelles. La Cnil statuera ensuite sur la conformité ou non du responsable de traitement à la loi. Si c'est le cas, la procédure de contrôle sera clôturée par une lettre du Président de la Cnil dans laquelle il peut formuler des recommandations si

---

1° Soit en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 lorsque la visite a été autorisée par le juge ;
2° Soit en refusant de communiquer à ses membres ou aux agents habilités en application du dernier alinéa de l'article 19 les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;
3° Soit en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible. »

[25]Délibération n° 2009-201 du 16 avril 2009 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société JEAN MARC PHILIPPE

nécessaire. En revanche, lorsque les violations constatées appellent des sanctions, il appartient à la formation contentieuse de se prononcer. A noter que le Conseil d'État[26] reconnait à la formation restreinte de la Cnil la qualité de tribunal, au sens de l'article 6§1[27] de la CESDH relatif au droit au procès équitable, dans l'exercice de son pouvoir de sanction. Par conséquent, les responsables de traitement mis en cause peuvent être assistés d'un avocat, accéder à leur dossier et être entendus lors de la formation contentieuse. Les mesures suivantes peuvent être imposées ou ordonnées conformément à l'article 45 de la loi[28] :

- **Avertissements.** L'autorité de contrôle peut adresser un avertissement à une société qui n'est pas en conformité avec la loi.

- **Mise en demeure.** La formation contentieuse de la Cnil peut prononcer une mise en demeure afin que le responsable de traitement mette un terme au manquement constaté.

La Commission fixe un délai pour que l'organisme se mette en conformité.

[26]CE référé, 19 février 2008, n° 311974, Société Profil France

[27]L'article 6§1 de la CESDH dispose que « *Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle. Le jugement doit être rendu publiquement, mais l'accès de la salle d'audience peut être interdit à la presse et au public pendant la totalité ou une partie du procès dans l'intérêt de la moralité, de l'ordre public ou de la sécurité nationale dans une société démocratique, lorsque les intérêts des mineurs ou la protection de la vie privée des parties au procès l'exigent, ou dans la mesure jugée strictement nécessaire par le tribunal, lorsque dans des circonstances spéciales la publicité serait de nature à porter atteinte aux intérêts de la justice.* »

[28]L'article 45 de la loi Informatique et Libertés dispose : « *I. - La formation restreinte de la Commission nationale de l'informatique et des libertés peut prononcer, après une procédure contradictoire, un avertissement à l'égard du responsable d'un traitement qui ne respecte pas les obligations découlant de la présente loi. Cet avertissement a le caractère d'une sanction.*
Le président de la commission peut également mettre en demeure ce responsable de faire cesser le manquement constaté dans un délai qu'il fixe. En cas d'urgence, ce délai peut être ramené à cinq jours.
Si le responsable du traitement se conforme à la mise en demeure qui lui est adressée, le président de la commission prononce la clôture de la procédure.
Dans le cas contraire, la formation restreinte peut prononcer à son encontre, après une procédure contradictoire, les sanctions suivantes :
1° Une sanction pécuniaire, dans les conditions prévues par l'article 47, à l'exception des cas où le traitement est mis en œuvre par l'Etat ;
2° Une injonction de cesser le traitement, lorsque celui-ci relève des dispositions de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25.
II. - Lorsque la mise en œuvre d'un traitement ou l'exploitation des données traitées entraîne une violation des droits et libertés mentionnés à l'article 1er, la formation restreinte peut, après une procédure contradictoire, engager une procédure d'urgence, définie par décret en Conseil d'Etat, pour :
1° Décider l'interruption de la mise en œuvre du traitement, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés aux I et II de l'article 26 ou de ceux mentionnés à l'article 27 mis en œuvre par l'Etat;
2° Prononcer un avertissement visé au premier alinéa du I ;
3° Décider le verrouillage de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés aux I et II de l'article 26 ;
4° Informer le Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui sont mentionnés aux mêmes I et II de l'article 26 ; le Premier ministre fait alors connaître à la formation restreinte les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.
III. - En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés. »

● **Ordre et actions correctives**. L'autorité peut notamment :

- suspendre le transfert des données vers des Etats non membres de l'UE ;
- exiger l'effacement des données personnelles qui ont été collectées contrairement aux principes de la loi ;
- ordonner l'interruption du traitement pour une durée qu'elle détermine. A la suite d'un contrôle sur place, la Cnil a ainsi ordonné la suspension d'un traitement de vidéosurveillance jugé injustifié et disproportionné qui filmait les salariés de manière constante ;
- retirer l'autorisation accordée pour la mise en œuvre du traitement.

● **Sanctions financières.** La première sanction financière ne peut pas excéder 150 000€.

Dans le cas d'une deuxième violation, une deuxième amende peut être imposée et celle-ci ne peut pas excéder 300 000 euros pour un particulier et 1,5 million pour les personnes morales.

● **Publicité des sanctions.** La Cnil peut procéder à la publicité des sanctions qu'elle prononce. Elle peut également ordonner leur insertion dans des publications, journaux et supports qu'elle désigne aux frais des personnes sanctionnées. Depuis la loi du 29 mars 2011 relative au défenseur des droits, la formation restreinte de la Cnil peut rendre publiques les sanctions financières qu'elle prononce.

● **Actions pénales.** Les sanctions prononcées par la Cnil ne l'empêchent pas de dénoncer les faits constatés au Procureur de la république. En outre, en cas d'atteinte grave et immédiate aux droits des personnes, le Président de la Cnil peut demander, par référé, à la juridiction compétente d'ordonner toute mesure de sécurité nécessaire à la protection desdits droits. Cela fonctionne comme une dissuasion pour les sociétés et peut être une sanction indirecte si le résultat est négatif. Cela peut en effet conduire à une perte de confiance de la part des clients, influencer le prix des actions etc.

Recours. Le responsable de traitement peut contester les conclusions de la procédure de contrôle et les sanctions ou mesures imposées par la Cnil. Lorsque des sanctions pénales ont été prononcées contre le responsable de traitement, une demande de révision devant la juridiction compétente pourra également être envisagée.

Les suites. Les sociétés qui ont été contrôlées peuvent s'attendre à être contactées par la Cnil pour faire savoir quelles actions ont été prises pour mettre en œuvre les recommandations énoncées dans le rapport final. Ces demandes post-contrôle sont souvent écrites et conduisent à la fourniture de documents additionnels. Le but est en effet de limiter le risque d'une autre procédure de contrôle.

Si vous souhaitez de plus amples informations au sujet du droit des données à caractère personnel, n'hésitez pas à poser vos questions à l'adresse suivante :

contact@avocats-mathias.com

Mathias
Avocats

Ce Livre blanc est purement indicatif et non exhaustif. Il ne constitue aucunement un conseil juridique.