L'EFFECTIVITE DE LA TRANSPARENCE DES TRAITEMENTS DE DONNEES PERSONNELLES

169. Dans la sphère numérique, la transparence est le fait de rendre visible l'invisible. C'est tout l'enjeu de la conformité, qui vise à empêcher que les informations communiquées au titre des articles 12, 13, 14, 15 et 22 du RGPD[344], c'est-à-dire du droit à l'information et à l'explicabilité des décisions individuelles automatisées, ne soient erronées, car la personne concernée est *de facto* en situation de vulnérabilité par rapport aux responsables du traitement[345], voire des sous-traitants, à raison notamment d'une asymétrie informationnelle. Le RGPD repose donc sur des pouvoirs traditionnels de conformité par les autorités de contrôle, dont la CNIL au plan national. Ils permettent à la fois d'améliorer la transparence avant que le traitement ne soit mis en œuvre, puis de le contrôler le cas échéant *a posteriori* (Section I).

170. Au-delà de ces considérations, cette réglementation modifie l'approche de la protection sur les données personnelles en ayant fait basculer un régime d'autorisation et de formalités préalables[346] à un régime de responsabilisation des responsables du traitement et de leurs sous-traitants à des fins de simplification. En contrepartie, de nouveaux mécanismes dits de conformité ont été rendus obligatoires. Selon Margot E. Kaminski[347], le RGPD instaure pour certains d'entre-eux une gouvernance collaborative à travers des mécanismes plus novateurs, le plus souvent de droit non contraignant de façon à ce qu'il existe une complémentarité entre la puissance publique, intervenant en tant que régulateur, et les responsables du traitement, leur permettant de prendre part à l'élaboration de la réglementation. Il s'agit donc de la mise en œuvre du principe de responsabilité consistant à ce que les acteurs concernés par les obligations du RGPD démontrent leurs conformités, par eux-mêmes, et qui concourt à l'effectivité de la réglementation, dont celui du principe de transparence en matière de données personnelles, même si celui demeure imparfait (Section 2).

---

[344] S*upra.,* n°80 et s.
[345] Voir en ce sens, DOUVILLE T., HERVOCHON C., NOEL E., PAQUIER Y., « Les vulnérabilités numériques », *Les Cahiers de la Recherche sur les Droit Fondamentaux,* 2020, p. 111.
[346] *Infra*., n° 208 et s.
[347] KAMINSKI M, E., « *Binary Governance : Lessons from the GDPR's Approche to Algorithmic Accountability* », *op. cit*., p. 1609.

SECTION 1 - LES POUVOIRS TRADITIONNELS DES AUTORITES DE CONTROLE

171. La CNIL est la première AAI désignée en tant que telle par le législateur de l'histoire du droit français[348]. Cela démontre que le législateur souhaitait que cette commission soit indépendante du pouvoir politique dans le cadre de sa composition et de son fonctionnement. Compte tenu des nouveaux enjeux, et de l'exacerbation des problématiques relatives au numérique, il n'est pas déraisonnable de penser qu'une telle autorité, avec des compétences élargies, et un budget à la hauteur de ses missions, soit désormais instituée avec un statut qui va au-delà de ce que les autorités administratives indépendantes permettent aujourd'hui. Mais avant d'aborder ce sujet dans la deuxième partie de ces travaux[349], il est nécessaire d'analyser dans leur généralité les prérogatives dont dispose la CNIL pour parvenir à l'effectivité de la transparence des traitements algorithmiques de données à caractère personnel. Il est par ailleurs à noter que la CNIL, depuis l'immixtion du droit de l'Union dans ce domaine, est également sous la supervision du CEPD afin d'uniformiser l'application de ce nouveau droit au sein des Etats membres, mais aussi de la Commission européenne.

172. La CNIL dispose de pouvoirs susceptibles de concourir à la transparence des traitements de données personnelles en amont de leur mise en œuvre. Toutefois, au-delà de la mission préventive de cette institution (Paragraphe 1), qui demeure par ailleurs insuffisante pour les raisons que nous évoquerons, elle jouit d'un important pouvoir coercitif permettant de contrôler les traitements une fois déployés par les responsables du traitement et de leurs sous-traitants (Paragraphe 2).

PARAGRAPHE 1 - Les pouvoirs concourant *ex ante* à la transparence des traitements

173. Au-delà des mécanismes de responsabilité des acteurs que nous aborderons ultérieurement, et à laquelle la CNIL participe, les pouvoirs traditionnels de cette autorité, et susceptibles de concourir *ex ante* à la transparence des traitements algorithmiques de données à caractère personnel, reposent davantage sur un droit souple (A) que règlementaire, ce qui aboutit, notamment du fait de la fin du régime d'autorisation de nombreux traitements sous

[348] Art. 6 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[349] *Infra*., n° 717 et s.

l'empire de l'ancienne règlementation, à un affaiblissement de cette dernière en tant que contre-pouvoir technique (B).

A - Un pouvoir de proposition et de droit souple

174. La CNIL dispose d'un rôle en matière d'information auprès des personnes physiques afin de les informer au sujet de leurs droits, mais également auprès des responsables du traitement, qu'ils soient privés ou publics dans le but de les renseigner sur leurs obligations, y compris sur le respect des droits des personnes parmi lesquels la transparence des données personnelles traitées bénéficie d'une place centrale[350]. L'article 8 § 1 1° de la LIL dispose en ce sens qu'« *elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations et peut, à cette fin, apporter une information adaptée aux collectivités territoriales, à leurs groupements et aux petites et moyennes entreprises* ». La commission peut aussi être sollicitée par de nombreux acteurs publics auprès desquels elle exerce une mission de conseil[351]. Elle répond également aux demandes d'avis formulés par les pouvoirs publics[352], y compris des autres autorités administratives indépendantes.

175. Au-delà de l'avis obligatoire au titre des articles 31 et 32 de la LIL[353], elle est consultée pour tout projet de loi ou de décret portant sur le traitement de données personnelles ou sur leur protection au sens large[354]. Nous regrettons sur ce point que cette consultation ne porte que sur les projets, qui certes sont importants afin que les parlementaires puissent le cas échéant bénéficier de son expertise lors des débats, alors qu'il serait en revanche plus constructif qu'elle intervienne tout au long du processus parlementaire ou règlementaire en vue de prodiguer les meilleurs conseils possibles. En effet, les projets ressemblent rarement à la version définitive qui pourtant s'imposera. Elle est également susceptible d'être force de proposition concernant l'évolution des régimes juridiques comme cela est le cas au sujet du projet de règlement européen de la Commission européenne relatif à l'IA[355].

176. Elle effectue par ailleurs des actions de médiation. Il s'agit dans ce cas d'un important volet visant à prévenir les violations à la réglementation. Cette institution joue également un

[350] *Supra.,* n° 80 et s.
[351] Art. 57 1 § 1 c) du RGPD.
[352] Art. 8 § 2 2° e) de la LIL modifiée.
[353] *Infra*., n° 183.
[354] Art. 8 § 2 4° a) de la LIL modifiée.
[355] La CNIL ainsi que ses homologues européens ont formulé un avis conjoint à ce sujet. Voir en ce sens, EDPB-EDPS, *Joint opinion 5/2021, on the proposal for a Regulation of the European Parliament and of the Concil laying down harmonised rules on artificial intelligence,* 18 juin 2021.

rôle de sensibilisation et de recueil de doléances auprès de nombreux publics. Elle a par exemple effectué une concertation citoyenne sur les enjeux de l'IA et des algorithmes ayant abouti à un rapport dans lequel figure d'intéressantes recommandations[356], notamment sur la transparence des algorithmes que nous serons amenés à évoquer dans la seconde partie de ces travaux[357]. Son laboratoire d'innovation numérique (LINC)[358] ambitionne de cerner les enjeux prospectifs, ce qui lui permet de s'émanciper de la mission traditionnelle de régulateur tout en étant force de proposition.

177. En plus des avis qu'elle émet à la demande des pouvoirs publics, la LIL[359] permet de plus aux juridictions de solliciter la CNIL à des fins d'expertise. Sur ce dernier point, il est à noter qu'en matière pénale elle doit saisir le procureur de la République dès lors que sont portés à sa connaissance des faits criminels ou délictueux, et ce conformément à l'article 40 du Code de procédure pénale (CPP) et lui formuler un avis sans délai[360]. S'ajoute à cela la possibilité de « *présenter des observations dans les procédures pénales* »[361], mais également devant toute autre juridiction si le contentieux est relatif à la protection des données à caractère personnel[362]. Ainsi, *« la juridiction d'instruction ou de jugement peut appeler le président de la Commission nationale de l'informatique et des libertés ou son représentant à déposer ses observations ou à les développer oralement à l'audience* »[363]. Lorsque de telles procédures interviennent, le traitement de données est certes déjà mis en œuvre, mais la CNIL est susceptible d'exercer une influence par l'intermédiaire d'interprétation du droit en précisant la portée d'une disposition amenée à se pérenniser dans la jurisprudence pour une meilleure effectivité de la transparence et donc des droit et libertés. Elle participe donc d'une certaine manière à l'action juridictionnelle.

[356] CNIL, Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle, *www.cnil.fr* [en ligne]. Décembre 2017. [Consulté le 2 décembre 2020]. Disponible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf
[357] *Infra.*, n° XXX.
[358] Site du Laboratoire d'Innovation Numérique de la CNIL [en ligne]. [Consulté le 2 juillet 2021]. Disponible à l'adresse : https://linc.cnil.fr
[359] Art. 8 § 1 4°e) de la LIL modifiée.
[360] Art. 8 § 1 4°f) de la LIL modifiée.
[361] *Ibid*.
[362] Art. 8 § 1 5° de la LIL modifiée.
[363] Art. 41 de la LIL modifiée.

178. La CNIL recourt notamment aux lignes directrices[364] et aux recommandations afin de venir préciser, voire interpréter la réglementation applicable[365]. En tant qu'autorité de contrôle indépendante, elle siège également au sein du CEPD, ce qui lui offre la possibilité de participer à l'interprétation des dispositions au niveau européen. A ce titre, elle a concouru à l'élaboration des lignes directrices sur la transparence[366]. Toutefois, ces actes de droit souple ne peuvent être de portée générale et absolue[367]. Il convient donc d'en déduire que la CNIL ne pourrait pas aboutir à une interprétation particulièrement large des obligations des responsables du traitement en matière de transparence. Ce droit souple est par ailleurs susceptible de recours s'il fait grief, ce qui correspond parfaitement à la nature de ces recommandations qui font droit[368]. Elle peut donc établir des règles en matière de transparence, mais certaines lignes directrices laissent à penser que les droits des personnes concernées font l'objet de régression par rapport à la réglementation afin de favoriser les acteurs économiques dans leurs transitions. En ce sens, le 17 septembre 2020, elle avait encore décidé de repousser de six mois la mise en conformité des acteurs en matière de « cookies et autres traceurs » dans de nouvelles lignes directrices[369], alors pourtant que la règlementation générale et sectorielle relative aux données à caractère personnel est en application et connue depuis de nombreuses années[370].

B - L'affaiblissement du pouvoir de décision de la CNIL

179. Afin notamment de favoriser la circulation des données dans le cadre du libre marché européen, le régime d'autorisation préalable avant la mise en œuvre de nombreux traitements, s'est en grande partie substitué à une logique de responsabilité des acteurs[371]. Nous notons à

[364] Le Comité consultatif de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel élabore également des lignes directrices. A titre d'exemple, il a récemment proposé par cette intermédiaire un régime juridique sur la reconnaissance faciale. Voir en ce sens, Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, lignes directrices sur la reconnaissance faciale, 28 janvier 2021.
[365] Art. 8 § 2 2° b) de la LIL modifiée.
[366] G29, lignes directrices relatives à la transparence au sens du RGPD du 11 avril 2018.
[367] CE, n° 434684, 19 juin 2020.
[368] *« Les documents de portée générale émanant d'autorités publiques, matérialisés ou non, tels que les circulaires, instructions, recommandations, notes, présentations ou interprétations du droit positif peuvent être déférés au juge de l'excès de pouvoir lorsqu'ils sont susceptibles d'avoir des effets notables sur les droits ou la situation d'autres personnes que les agents chargés, le cas échéant, de les mettre en œuvre. Ont notamment de tels effets ceux de ces documents qui ont un caractère impératif ou présentent le caractère de lignes directrices »*, CE, n° 418142, 12 juin 2020.
[369] CNIL, délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019.
[370] En ce sens, le RGPD est en application depuis le 25 mai 2018, tandis que la transposition de la directive 2002/58/CE du 12 juillet 2002, dite « *eprivacy* » modifiée en 2009, a été effectuée par l'ordonnance n° 2018-1125 du 12 décembre 2018.
[371] *Infra.*, n° 208 et s.

regret une tendance à l'affaiblissement des pouvoirs contraignants de la CNIL ayant pourtant participer à la transparence des traitements de données personnelles.

180. Au-delà de son pouvoir règlementaire portant sur l'édiction de son règlement intérieur, la CNIL dispose également d'un tel pouvoir afin d'adopter des règlements types contraignants. Ils ne sont cependant possibles qu'« *en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel et de régir les traitements de données biométriques, génétiques et de santé* »[372]. A titre d'exemple, la CNIL a édicté un règlement *« relatif à l'accès par authentification biométrique sur les lieux de travail* ». Il précise la mise en œuvre de l'article 12 et suivants du RGPD dans ce domaine, concourant par cet intermédiaire à la transparence[373].

181. Autrefois obligatoires, le RGPD a mis fin aux autorisations préalables qui portaient sur certaines catégories de données, ce qui à notre sens est regrettable dans la mesure où ce mécanisme permettait indiscutablement de contrôler un traitement avant sa mise en œuvre, et le cas échéant de ne pas l'autoriser si les garanties, notamment de transparence n'étaient pas respectées. Cela explique pourquoi les dispositifs biométriques ne sont désormais plus soumis à une telle autorisation. Toutefois, la CNIL est toujours susceptible de se prononcer sur certains traitements, ne serait-ce que parce que le législateur national[374] les a maintenus pour quelques rares exception dans la LIL. Tel est encore le cas pour certains traitements de données de santé[375]. Mais contrairement à la directive 95/46/CE, le RGPD en a simplifié la tenue.

182. Comme l'indique Christina Koumpli dans sa thèse à propos des formalités préalables à effectuer par le responsable du traitement,

> « *(…) il est important de relever que les processus de simplification ont contribué de manière notable à une moindre transparence. Comme la doctrine l'a noté, « la disparition progressive des formalités pose (...) une difficulté puisqu'elle diminue la capacité de contrôle des personnes concernées sur les traitements ». Or, ce*

[372] Art. 8 § 1 2° c) de la LIL de 1978 modifiée.
[373] Le droit à l'information dans ce domaine, au titre du règlement type de la CNIL, « *doit figurer dans une notice écrite remise par le responsable de traitement à chaque personne concernée préalablement à l'enrôlement des données biométriques de ce dernier* ». Voir en ce sens, délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail, art. 9.
[374] Conformément à l'art. 9 § 4 du RGPD.
[375] Lire en ce sens, CLUZEL-METAYER L., FRANCOIS A., « La protection des données personnelles à l'épreuve de la télémédecine », *RDSS*, 2020, p. 51-59.

contrôle est la manifestation même du droit fondamental à la protection des données personnelles selon certains auteurs »[376].

183. De plus, certains « *traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat* »[377], ne pouvaient être mis en service qu'après un avis motivé de la CNIL[378]. Mais il ne s'agit plus d'un avis conforme depuis 2004[379], ce qui affaiblit la mission préventive de protection des libertés et de contre-pouvoir technique de cette institution. Cet avis conforme était pourtant qualifié par certains auteurs, dont Christina Koumpli, de pouvoir règlementaire attribué à la Commission par le législateur originel de la LIL de 1978[380]. Dans le contexte particulier de la Covid-19, les parlementaires avaient adopté, dans une disposition du projet de loi prorogeant l'urgence sanitaire[381], la réintroduction de l'avis conforme de la CNIL au sujet des décrets mettant en œuvre les systèmes d'information en matière de santé. A défaut de l'aval de la CNIL, les traitements de données déployés dans le cadre de l'urgence sanitaire n'auraient pas pu être déployés. Toutefois, le Conseil constitutionnel a déclaré cette disposition inconstitutionnelle dans la mesure où le législateur ne peut « *subordonner à l'avis conforme d'une autre autorité de l'État l'exercice, par le Premier ministre, de son pouvoir réglementaire* »[382].

---

[376] KOUMPLI C., *Les données personnelles sensibles : contribution à l'évolution du droit fondamental à la protection des données à caractère personnel : étude comparée : Union européenne, Allemagne, France, Grèce, Royaume-Uni*, Thèse de doctorat, soutenue à l'Université Paris 1 Panthéon-Sorbonne le 18 janvier 2019, spec. p. 455.

[377] Il s'agit des traitements de données à caractère personnel visés par les article 31 et 32 de la LIL tels que « *1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ; 2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté. » mais également ceux pris dans le cadre de « l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.* ».

[378] Art. 8 § 1 2° a) de la LIL modifiée.

[379] Avant la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, si la CNIL rendait un avis défavorable pour un traitement de cette nature, seulement un décret pris sur avis conforme du Conseil d'Etat permettait la mise en œuvre de ce dernier (art 15 de la LIL de 1978).

[380] KOUMPLI C., *Les données personnelles sensibles : contribution à l'évolution du droit fondamental à la protection des données à caractère personnel : étude comparée : Union européenne, Allemagne, France, Grèce, Royaume-Uni, op. cit.*, spec. p. 32.

[381] Art. 11 § V, Assemblée Nationale, projet de loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions, n° 418, en date du 9 mai 2020.

[382] CC, décision n° 2020-800 DC, 11 mai 2020, *Loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions*, § 77, « *en vertu de l'article 21 de la Constitution et sous réserve de son article 13, le Premier ministre exerce le pouvoir réglementaire à l'échelon national. Ces dispositions n'autorisent pas le législateur à subordonner à l'avis conforme d'une autre autorité de l'État l'exercice, par le Premier ministre, de son pouvoir réglementaire. Dès lors, le mot « conforme » figurant à la première phrase du paragraphe V de l'article 11 est contraire à la Constitution.* ».

184. La CNIL a pu s'illustrer différemment lors de son avis sur le projet en demandant la transparence du dispositif « *StopCovid* »[383] en allant au-delà des droits garantis par le RGPD et la LIL[384]. En effet, elle a considéré qu'

> « *une transparence renforcée quant au mode de fonctionnement et aux finalités de traitement, est un élément déterminant pour assurer la confiance dans le dispositif et favoriser son adoption par une partie significative de la population* »[385]

185. Concrètement, cette transparence renforcée se caractérise par d'une part la recommandation et la publication d'une analyse d'impact, d'autre part, la recommandation par la CNIL d'un accès aux protocoles et au code source de l'application, et aux paramétrages du serveur gérant les notifications. Le but étant notamment « *de permettre à la communauté scientifique de contribuer à l'amélioration constante du dispositif et à la correction des éventuelles vulnérabilités* », notamment afin que des remarques puissent nourrir le débat au sein de la communauté scientifique et soient prises en compte. Il est à noter que selon la commission, la communication de ces informations n'a pas pour but principal d'assurer la transparence vis-à-vis de l'ensemble des citoyens, ce qui serait sans doute d'un intérêt limité car trop technique, mais de s'assurer de la conformité du traitement par une garantie collective par l'intermédiaire de la société civile.

186. Finalement, dans sa délibération du 25 mai 2020 portant sur le projet de décret instaurant ce traitement[386], le gouvernement ne souhaitait pas transmettre l'intégralité du code source de l'application ainsi que certains paramétrages du serveur central au motif qu'il existerait un danger pour « *l'intégrité et la sécurité de l'application* ». La commission n'a pas hésité à insister sur la nécessité de diffuser ce code conformément aux engagements du secrétaire d'Etat du numérique, Cédric O, lors de ses déclarations. Elle a rappelé que *« même si le paramétrage des logiciels utilisés et le détail des mesures de sécurité n'ont pas vocation à être rendus publics, il est important que l'intégralité du code source soit quant à lui rendu public »*, ce que le décret final repris[387]. Elle a par ailleurs incité à ce que le code source de « *TousAntiCovid*

[383] Selon le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « *StopCovid* » il s'agit d'un traitement « *qui permet à ses utilisateurs d'être informés lorsqu'ils ont été à proximité d'au moins un autre utilisateur diagnostiqué ou dépisté positif au virus du covid-19, grâce à la conservation de l'historique de proximité des pseudonymes émis via la technologie Bluetooth* ». Il est désormais appelé « *TousAntiCovid* ».
[384] *Supra.*, n° 80 et s.
[385] CNIL, délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « *StopCovid* ».
[386] Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « *StopCovid* ».
[387] Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « *StopCovid* ».

Vérif », application utilisée afin d'assurer la validité du passe sanitaire, soit rendu public mais « *expurgé, le cas échéant, des secrets permettant de sécuriser les transmissions de données avec les serveurs centraux* »[388].

187. La CNIL peut également publier certains avis consultatifs, notamment afin qu'ils soient repris par la presse, ce qui exerce par cet intermédiaire une influence sur les autres acteurs. Néanmoins, ce rôle de proposition, de droit souple, demeure faible, car il ne s'agit plus d'un avis conforme, et elle ne peut donc s'opposer à la mise en œuvre d'un tel traitement quand bien même il serait liberticide, alors que cette institution était pourtant initialement pensée pour être un contre-pouvoir de nature technique[389] par le législateur originel.

PARAGRAPHE 2 - Les pouvoirs permettant l'observation du traitement

188. Initialement, lors des débats parlementaires, la CNIL ne devait pas être une AAI, mais un Comité de surveillance muni d'un pouvoir d'investigation permettant d'une part de recueillir les plaintes des personnes physiques, et d'autre part d'enquêter sur ces éventuelles violations à la législation de la LIL. Ce comité ne disposant pas quant à lui d'une compétence juridictionnelle, il avait la faculté de saisir une section du Tribunal administratif de Paris agissant en qualité de Tribunal de l'informatique[390].

189. Dans ce cas de figure, l'observation du traitement s'effectue *a posteriori*, c'est-à-dire lorsque le traitement est mis en œuvre dans les faits. Ces pouvoirs consistent donc en leur observation, afin, le cas échéant, de remédier aux manquements du responsable du traitement ou de leur sous-traitant.

190. De manière générale, les autorités de contrôle indépendantes, dont la CNIL, disposent aussi bien d'un pouvoir d'enquête (A) que de coercition (B). Et eu égard à ce pouvoir de

[388] CNIL, délibération n° 2021-067 du 7 juin 2021 portant avis sur le projet de décret portant application du II de l'article 1er de la loi n° 2021-689 du 31 mai 2021 relative à la gestion de la sortie de crise sanitaire, p.8.
[389] *Supra.*, n° 183.
[390] FOYER M., Rapport n° 3125 sur le projet de loi relatif à l'informatique et aux libertés de l'Assemblée nationale, 5e législature, fait au nom de la commission des Lois, enregistré à la Présidence de l'Assemblée nationale le 4 octobre 1977 relatant la proposition de loi n° 1454 par M. Poniatowski. Une proposition de loi sénatoriale (n° 144-1973-74 déposée par M. Caillavet) visait également à la création non pas d'un comité de surveillance, mais d'un directoire de l'informatique bénéficiant toutefois des mêmes compétences.

coercition, la CNIL dispose d'un pouvoir juridictionnel au sens d'un pouvoir de sanction comme de nombreuses autres AAI[391].

A - Le pouvoir d'investigation

191. Dès lors qu'une autorité de contrôle dispose des compétences et de la confiance des citoyens, ce qui n'est pas par ailleurs sans poser la question de la transparence de l'action de cette institution, il n'est pas inconsidéré d'attendre que l'information soit médiée par cette autorité à l'utilisateur s'il s'agit de procédés sensibles remettant en cause les droits fondamentaux d'autrui. Mais cela implique qu'elle bénéficie de tous les pouvoirs permettant de s'assurer de la conformité effective des traitements. En effet, la crainte légitime est que les responsables du traitement utilisent les secrets protégés par la loi pour pérenniser l'opacité de ces systèmes.

192. Les plaintes et réclamations[392] des personnes concernées, voire d'autres acteurs, auprès de la CNIL, jouent un rôle majeur en matière de transparence dans la mesure où elles vont éveiller les soupçons sur certains manquements. En effet, lorsque les griefs sont corroborés par des éléments probants, elles engendreront des enquêtes pouvant déboucher sur des constatations de violation. C'est donc un rôle d'alerte indispensable sur les traitements opérés, et ce d'autant plus que la société civile œuvre également au signalement des mauvaises pratiques. A titre d'exemple, de nombreux utilisateurs signalent sur Twitter à la CNIL les manquements qu'ils découvrent au quotidien. Les autres autorités de contrôle indépendantes des Etats membres de l'Union peuvent également lui adresser des signalements[393]. La Commission peut de plus se saisir de sa propre initiative.

193. Toutefois, ces dernières années, la CNIL ne semble pas avoir la capacité de faire face à l'afflux de plaintes, notamment car les traitements de données personnelles se sont immiscés dans d'innombrable domaines et de nombreux acteurs sont encore dans la méconnaissance de la nouvelle réglementation, alors que les moyens matériels et humains de cette institution

[391] En ce sens, lire BRUNET F., « De la procédure au procès : le pouvoir de sanction des autorités administratives indépendantes », *RFDA*, 2013, p. 113-126.
[392] Art. 8 § I 2° b) de la LIL modifiée et art 57 § 1 f) du RGPD.
[393] Art. 57 § 1 f), g) et h) du RGPD.

demeurent minces au regard de l'enjeu. A ce titre, certains justiciables se désintéressent des autorités de régulation en intentant directement des actions en justice[394].

194. Le pouvoir d'investigation des autorités de contrôle est essentiel puisqu'il permet de constater ou non la conformité effective des traitements algorithmiques à la réglementation. A cette fin, le RGPD et le droit national prévoient certaines compétences en matière d'enquête. Toutefois, au sens de la directive « Police-Justice »[395], la CNIL est exclue du contrôle des traitements opérés par les juridictions dans le cadre de leurs missions, logiquement pour des raisons de séparation des pouvoirs[396].

195. L'autorité de contrôle bénéficie du pouvoir de se faire communiquer « *toute information dont elle a besoin pour l'accomplissement de ses missions* » aussi bien de la part du responsable du traitement que du sous-traitant[397]. Elle peut également mener des audits afin de constater ou non la conformité des algorithmes au RGPD, ce qui nécessite d'accéder au traitement, assurant une transparence de ces derniers auprès de l'autorité de contrôle[398]. Un comité d'audit du système national des données de santé a par ailleurs été institué par la LIL[399].

196. Dans le cadre de ce pouvoir d'enquête, le contrôleur est susceptible d'accéder aux locaux du responsable du traitement, et le cas échéant du sous-traitant, ainsi qu'à « *toute installation et à tout moyen de traitement* »[400]. Plus généralement, le contrôleur peut accéder à toutes les données à caractère personnel, ainsi qu'à toutes les informations afférentes, dans le cadre de ses prérogatives[401]. Le recours à des experts par la Commission est de plus précieux notamment pour effectuer des audits et bénéficier du plus d'éléments possibles sur le traitement

[394] MANANCOURT V., Have a GDPR complaint ? Skip the regulator and take it to court, *Politico.eu*. 30 août 2020, mis à jour le 1er septembre 2020. [Consulté le 04 octobre 2020]. Disponible à l'adresse : https://www.politico.eu/article/have-a-gdpr-complaint-skip-the-regulator-and-take-it-to-court/

[395] Directive (UE) 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

[396] Art. 55 § 3 du RGPD.

[397] Art. 58 § 1 a) du RGPD.

[398] Art. 58 § 1 b) du RGPD.

[399] Art. 77 de la LIL modifiée.

[400] Art. 58 §1 f) du RGPD. L'article 19 III de la LIL modifiée précise par ailleurs 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 10 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. Le procureur de la République territorialement compétent en est préalablement informé* ».
En cas de refus du responsable du traitement ou de son sous-traitant, le juge des libertés et de la détention peut néanmoins autoriser lesdites vérifications, y compris dans un lieu privé. Voir en ce sens, art. 25 à 32 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[401] Art. 58 § 1 e) du RGPD et dans les conditions prévues à l'art. 19 de la LIL modifiée.

mis en œuvre[402]. Toutefois, l'article 19 III de la LIL précise que « *le secret ne peut leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou, sous réserve du deuxième alinéa du présent III, par le secret médical* ». Des contrôles en ligne[403] et des auditions[404] sont par ailleurs susceptibles d'être effectués.

197. Au-delà de ces pouvoirs de contrôle des traitements mis en œuvre, force est de constater que la CNIL demeure une AAI pourvue de seulement 225 agents en 2020, dont le département de la conformité ne représente que 24% de l'effectif, ce qui n'a permis d'aboutir seulement à 74 contrôles sur pièce sur ladite année[405]. Cette faible performance en matière de contrôle n'est pas due aux circonstances exceptionnelles de la pandémie de SARS-CoV-2 puisqu'en 2019 ce chiffre n'était que de 45[406]. Elle s'explique surtout par son faible budget annuel de 20,1 millions d'euros[407].

198. En matière d'enquête, il convient de noter que les transferts de données vers les Etats tiers à l'Union européenne sont un défi majeur. Or, à titre d'exemple, en vertu du principe de compétence territoriale, l'autorité de contrôle irlandaise se retrouve être en première ligne car le siège social européen de nombreux géants du numérique s'y trouve, ce qui a pour incidence qu'elle exerce ce pouvoir d'enquête à l'encontre de ces sociétés en tant que chef de file[408]. C'est donc en grande partie elle qui est la garante de l'effectivité du RGPD, y compris pour les requêtes formulées à l'encontre de ces géants dans d'autres Etats de l'Union. Même si les autorités de contrôle européennes coopèrent mutuellement[409], des enjeux politiques et économiques nationaux sont susceptibles de nuire à l'effectivité de la réglementation européenne sur les données personnelles. Une résolution du Parlement européen met en exergue ce risque au sujet de cette autorité irlandaise. Les parlementaires notent que le commissaire irlandais a laissé en suspens de nombreuses réclamations et plaintes relatives à des suspicions de violations du RGPD par ces grands groupes. Les députés remettent par ailleurs en cause la

[402] Art. 35 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[403] *Ibid*., art. 33.
[404] *Ibid*., art. 34.
[405] CNIL, Rapport d'activité 2020 de la Commission Nationale de l'Informatique et des Libertés, p. 7, *www.cnil.fr* [en ligne]. Juin 2020. [Consulté le 27 août 2021]. Disponible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/cnil_-_41e_rapport_annuel_-_2020.pdf.
[406] CNIL, Rapport d'activité 2019 de la Commission Nationale de l'Informatique et des Libertés, p. 3, *www.cnil.fr* [en ligne]. Juin 2020. [Consulté le 27 août 2021]. Disponible à l'adresse : https://www.cnil.fr/sites/default/files/atoms/files/cnil-40e_rapport_annuel_2019.pdf
[407] CNIL, Rapport d'activité 2020 de la Commission Nationale de l'Informatique et des Libertés, *op. cit.*
[408] Art. 56 du RGPD.
[409] Art. 60 du RGPD.

compétence de l'institution qui ne serait pas suffisamment dotée en moyen humain pour saisir les enjeux technologiques. Ainsi, et au regard des risques pour l'effectivité des droits des personnes, le législateur européen demande à la Commission européenne « *d'engager une procédure en manquement à l'encontre de l'Irlande pour absence de contrôle satisfaisant de l'application du RGPD* »[410].

199. Lorsque l'on constate l'impossibilité d'enquêter sur place afin de constater le véritable fonctionnement des traitements algorithmiques de ces sociétés, il n'est pas étonnant que la CJUE[411] ait décidé d'invalider le *privacy shield,* non pas sur le fondement de preuves de violation de droits fondamentaux, mais sur le risque théorique, en l'absence de garanties suffisantes, que pouvait engendrer le transfert des données à caractère personnel des personnes physiques de l'Union vers les Etats-Unis d'Amérique. Cette approche fondée sur les risques, nous serons amenés à l'étudier de manière approfondie lorsque nous aborderons le projet de règlement général sur l'IA[412].

200. Il est à noter que la CNIL n'est pas compétente pour enquêter à propos de certains traitements intéressant la sûreté de l'Etat[413], ce qui nuit à son action. Bien que d'autres autorités administratives puissent être compétentes à cet effet, elles n'offrent toutefois pas le même niveau de garantie sur la transparence de ces traitements.

B - Les pouvoirs coercitifs

201. Ses pouvoirs sont généraux, allant de l'avertissement[414], de la mise en demeure[415] à des sanctions[416]. En cas de non-respect des obligations prévues par le RGPD, l'autorité peut rappeler à l'ordre le responsable du traitement ou un sous-traitant lorsque le traitement est contraire au RGPD[417] ou bien les avertir le cas échéant qu'ils sont susceptibles de violer des obligations en matière de transparence notamment[418]. Dans l'hypothèse où l'exercice des droits de la personne physique comme le droit à l'information ou d'accès au traitement est remis en

[410] Résolution du Parlement européen du 20 mai 2021 sur l'arrêt rendu par la Cour de justice de l'Union européenne le 16 juillet 2020 dans l'affaire C-311/18, Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems (« arrêt Schrems II »).
[411] CJUE, Grande chambre, affaire C-311/18, 16 juillet 2020.
[412] *Infra.*, n° 946 et s.
[413] En ce sens, art. 19 IV de la LIL modifiée. Nous aborderons ce point en détail plus tardivement lors de nos propositions, *Infra.*, n° 707 et s.
[414] Art. 20 I de la LIL modifiée.
[415] Art. 20 II de la LIL modifiée.
[416] Art. 20 III de la LIL modifiée.
[417] Art. 58 § 2 b) du RGPD
[418] Art. 58 § 2 a) du RGPD

cause, l'autorité peut ordonner cette mise en conformité[419]. En effet, nous ne pouvons pas seulement compter sur la bonne foi des entreprises et de leur DPD[420], quand bien même celui-ci serait certifié par la CNIL. Elle est également à même d'infliger une interdiction de traitement des données à caractère personnel définitive ou pour une durée déterminée[421].

202. Les sanctions peuvent par ailleurs être très strictes dès lors qu'elles sont « *effectives, proportionnées et dissuasives* »[422], y compris en cas de non-respect aux obligations du RGPD, et donc du principe de transparence en matière de données personnelles. Comme nous le verrons ultérieurement, le mécanisme de certification joue un rôle important dans le respect de la transparence des traitements, et il est à noter qu'en cas de violation des obligations, il est possible pour l'autorité de retirer une certification ou d'imposer à l'organisme certificateur un tel retrait[423] ainsi que d'interrompre le flux de données à caractère personnel vers un Etat tiers à l'Union européenne par l'intermédiaire d'une procédure d'urgence nationale[424]. Les sanctions administratives peuvent donc être prononcées cumulativement à ces mesures[425].

203. A titre d'exemple, dans le cadre d'un contrôle des systèmes automatisés de données, utilisés lors de l'urgence sanitaire relatif à la crise de la Covid 19, dont celui de « *StopCovid* », la CNIL a opéré un contrôle de conformité. Il est apparu que cette application n'était pas conforme au décret l'instaurant[426], y compris en matière de transparence. Elle a rappelé que les traitements de données à caractère personnel « *doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée* » conformément à l'article 5 § 1 a) du RGPD. Il est intéressant de noter que la transparence est un principe fondamental en ce qu'il permet de s'assurer que les traitements sont conformes au droit, ce qui aboutira notamment à une mise en demeure du ministère des Solidarités et de la santé[427].

---

[419] Art. 58 § 2 c) et d) du RGPD.
[420] Le délégué à la protection des données est institué par l'article 37 du RGPD remplace le correspondant informatique et libertés. Il vise à assurer la mise en conformité d'un organisme avec la réglementation. En vertu de l'article 37 § 1 du RGPD, le recours à un DPD est obligatoire lorsque « *a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;*
b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou
c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ».
[421] Art. 58 § 2 f) du RGPD.
[422] Art. 83 § 1 du RGPD.
[423] Art. 58 § 2 h) du RGPD.
[424] Art. 58 § 2 j) du RGPD.
[425] Art. 83 § 2 du RGPD.
[426] Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « *StopCovid* ».
[427] Décision n° MED-2020-015 du 15 juillet 2020 mettant en demeure le ministère des solidarités et de la santé. Cette mise en demeure fut par ailleurs clôturée après régularisation par la décision n° 2020-015 du 3 septembre 2020.

204. La CNIL dispose d'une mission significative en matière de sanctions administratives lorsqu'elle intervient en tant que Tribunal[428]. Les sanctions sont en théorie particulièrement dissuasives. Lorsque les violations portent sur le droit des personnes concernées, et donc aux obligations de droit à l'information et à la transparence ainsi qu'au droit d'accès par exemple, la condamnation peut s'établir jusqu'à 4% du chiffre d'affaires mondial de l'entreprise mettant en œuvre le traitement, et ce dans la limite d'un plafond de 20 millions d'euros[429]. En revanche, en cas de violation au principe de responsabilité[430], de certification, de la protection des données dès la conception, de registre ou d'analyse d'impact tels que nous les étudierons, parce qu'ils concourent à la compréhension de ces systèmes, une amende administrative d'un montant de 2% du chiffre d'affaires mondial de l'entreprise peut être infligée, dans la limite d'un plafond de 10 millions d'euros[431].

205. En ce sens, la première sanction ayant été prononcée par la CNIL[432] en application des dispositions du RGPD portait d'ailleurs sur un défaut d'information sur le fondement des articles 6, 12 et 13 de cette règlementation, donc de transparence. La formation restreinte de la Commission a également constaté que la communication des informations aux personnes physiques concernées était en l'espèce difficilement accessible, car se trouvant dans de multiples documents différents telles que les conditions générales d'utilisation. De plus, concernant le caractère aisément compréhensible des informations fournies, la collecte des données et l'information afférente, ne permettait pas à l'utilisateur de prendre conscience de l'ampleur du traitement réalisé, alors que « *considérée isolément, la collecte de chacune de ces données est susceptible de révéler avec un degré de précision important de nombreux aspects parmi les plus intimes de la vie des personnes dont leurs habitudes de vie, leurs goûts, leurs contacts, leurs opinions ou encore leurs déplacements. Le résultat de de la combinaison entre elles de ces données renforce considérablement le caractère massif et intrusif des traitements dont il est question* »[433].

206. Compte tenu des errements de son homologue irlandaise en matière de respect de la règlementation générale sur les données personnelles[434] par les principaux géants du numérique

[428] Art. 58 § 2 i) du RGPD.
[429] Art. 83 du RGPD.
[430] *Infra*., n° 208 et s.
[431] *Ibid.*
[432] A titre d'exemple, voir délibération de la CNIL formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC. Cette délibération a par ailleurs été confirmée par le Conseil d'Etat dans un arrêt du 19 juin 2020, n° 430810.
[433] *Ibid*.
[434] *Supra*., n° 198.

puisqu'elle est l'autorité chef de file du fait de l'établissement de leur siège social, la CNIL les sanctionne par contournement. Elle recourt à des dispositions spéciales relatives aux traceurs (cookies) prévues par la directive « *ePrivacy* »[435] et sa transposition en droit national qui n'imposent pas ce guichet unique. Ainsi, l'autorité peut se fonder sur un manquement aux obligations d'information à des fins de consentement à ces traceurs[436]. A ce titre, elle a par exemple condamné le 7 décembre 2020 la société Google à une amende de 100 millions d'euros (40 millions d'euros à Google Ireland Limited et 60 millions d'euros à l'encontre de Google LLC)[437].

207. Au-delà de ces pouvoirs traditionnels conférés aux autorités de contrôle que nous venons de voir, le RGPD compte avant tout sur une logique de responsabilisation des acteurs.

SECTION 2 - UNE CONFORMITE A GEOMETRIE VARIABLE PREVUE PAR LE RGPD

208. Nous traiterons seulement des dispositions relatives à la conformité permettant au responsable du traitement de démontrer que les informations qu'il fournit, au titre des articles 12, 13, 14, 15 et 22 du RGPD[438], représentent dans les faits la réalité du traitement. En effet, sans ces dispositifs de conformité, en dehors des contrôles effectués par la CNIL qui restent marginaux[439], il ne serait pas possible de vérifier que les informations fournies aux personnes physiques sont correctes. De la conformité dépend l'effectivité des droits des personnes concernées au titre du RGPD, mais également des violations des libertés impactées par les traitements algorithmiques, bien que cela n'ait pas été philosophiquement pensé comme tel. En effet, la transparence prévue par cette réglementation semble être mise en œuvre seulement pour garantir l'exercice des autres droits protégés par le RGPD, ni plus ni moins.

---

[435] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

[436] L'article 82 de la LIL modifiée dispose en effet que sauf exception « *Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :*
1° De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;
2° Des moyens dont il dispose pour s'y opposer ».

[437] CNIL, Délibération SAN-2020-012 du 7 décembre 2020. Pour un commentaire de cette sanction, voir CRICHTON C., « Cookies : la CNIL sanctionne Google et Amazon », *Dalloz actualité*, 17 décembre 2020.

[438] *Supra.*, n° 80 et s.

[439] *Supra.*, n° 206 et s.

209. Parmi les obligations générales incombant au responsable du traitement, nous retrouvons ce que le règlement nomme « *responsabilité* »[440]. Cette obligation de « responsabilité », émanant de l'anglais « *accountability* » doit surtout être entendue comme un principe de conformité, de redevabilité et donc d'adéquation, le plus souvent mou, car relevant essentiellement du droit souple contrairement aux mécanismes mettant en œuvre les droits individuels de transparence tels que le droit à l'information ou encore d'accès aux traitements algorithmiques.

210. Ce principe n'est pas nouveau puisqu'il avait été envisagé par le G29. Dans son avis n° 3/2010 portant sur le principe de responsabilité en date du 13 juillet 2010[441], il avait mis en exergue la nécessité d'une telle obligation pour les responsables du traitement dans la mesure où cette dernière favoriserait la protection effective des données[442]. Or, le plus souvent, c'est bien l'effectivité des droits et libertés qui font défaut dans le cadre des traitements algorithmiques. Par rapport à la directive 95/46/CE, le RGPD modifie l'approche de la protection sur les données personnelles. Il fait basculer un régime de formalités préalables à un régime de responsabilisation des acteurs à des fins de simplification. Il était important de prendre en considération les risques inédits inhérents à l'ampleur de la nouvelle économie de la donnée dans un cadre réglementaire modifié. Ce principe participe également à ce que les autorités chargées de la protection des données, comme la CNIL, exercent une meilleure surveillance des responsables du traitement[443]. Mais est-ce vraiment le cas ?

211. L'article 24 paragraphe 1 du RGPD a repris cette obligation en précisant que *« le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement* ». Mais le texte précise que le degré de redevabilité est variable « *compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques* ».

212. Cette obligation n'est donc pas absolue puisque laissée en grande partie à l'appréciation des acteurs eux-mêmes, ce qui n'est pas la solution la plus protectrice pour les personnes

[440] Art. 5 § 2 du RGPD.
[441] G29, avis n° 3/2010 sur le principe de responsabilité, WP 173, adopté le 13 juillet 2010.
[442] *Ibid*., p. 2.
[443] *Ibid*., § 74, p. 21.

physiques faisant l'objet d'un traitement de leurs données personnelles[444]. L'approche du RGPD peut sembler novatrice en la matière, mais il ne peut être exclu que dans la pratique nous assistions à une dénaturation de l'esprit du texte, qui selon nous, repose trop à certains égards sur la bonne volonté des acteurs tels que les responsables du traitement.

213. Ce même esprit se retrouve à l'article 24 paragraphe 2 du RGPD puisque si les activités de traitement ont des incidences sur les personnes physiques[445], des « *politiques appropriées en matière de protection des données par le responsable du traitement* » devront être mises en œuvre. Toutefois, une fois de plus, tel est uniquement le cas si cela est proportionné à l'activité de traitement, sans pour autant définir quels sont les cas de figure concernés par cette obligation.

214. Il s'agit donc surtout d'une relation entre d'une part l'autorité de contrôle et les acteurs, le plus souvent privés, qui participent à l'élaboration du droit, sans que la société civile n'y soit conviée. C'est essentiellement une relation entre les autorités gouvernementales et les entreprises. Les tiers ne peuvent pas constater les violations effectuées en interne par les entreprises.

215. Il est question d'aborder les principaux mécanismes du RGPD concourant à la transparence des traitements. Nous retrouvons parmi eux aussi bien des mécanismes de conformité de droit contraignant (Paragraphe 1) que de droit non contraignant (Paragraphe 2).

PARAGRAPHE 1 - Les mécanismes de droit contraignant concourant à la transparence des traitements au titre du principe de responsabilité

216. Les nouveaux mécanismes de conformité contraignants sont nombreux. Il s'agit de la protection des données dès la conception (A), de l'analyse d'impact relative à la protection des données (AIPD), de la consultation préalable (B), de la tenue d'un registre des opérations (C) et de la désignation d'un DPD (D).

A - La protection des données dès la conception

217. L'article 25 du RGPD instaure une obligation de protection des données dès la conception d'un programme et par défaut. L'objectif est que les responsables du traitement

[444] DEBET A., « Les nouveaux instruments de conformité », *Dalloz IP/IT*, 2016, p. 592.
[445] Conformément à l'article 24 § 2 du RGPD.

imaginent dès sa création la conformité à leurs obligations, ce qui inclut donc le respect aux exigences de transparence par l'intermédiaire *« (…) tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées »*[446]. Les « *mesures techniques et organisationnelles appropriées* » en question ne sont cependant pas définies par le texte, sans doute pour ne pas prendre parti pour des techniques particulières qui tomberaient en désuétude et dénatureraient la disposition. Sa mise en œuvre est fonction de l'état de l'art. Le considérant 78 du RGPD précise également que la protection dès la conception vise *« à garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel* ».

218. Le G29, dans sa documentation relative à la transparence, confirme également le rôle de la protection dès la conception à des fins de transparence. Il précise que « *les mécanismes de transparence devraient être intégrés à des systèmes de traitement dès le départ afin que toutes les sources des données à caractère personnel reçues par une entreprise puissent être suivies et retracées jusqu'à leur source à tout moment pendant le cycle de vie du traitement des données* »[447]. La faculté de pouvoir retracer le processus du traitement pendant la durée de son cycle de vie est toutefois compromise dans la mesure où certaines techniques d'IA empêchent par nature une telle implantation dans le système, ce qui leur vaut le qualificatif de boîte noire, y compris pour les concepteurs. Ce mécanisme se retrouve par ailleurs dans la directive « Police-Justice »[448].

219. Cette approche est pourtant très intéressante car elle modifie la logique répressive d'un traitement qui ne serait pas conforme au RGPD par un volet préventif à des fins d'adéquation aux exigences de transparence. Même si l'objectif est naturellement de pouvoir le cas échéant mieux renseigner la personne physique concernée par un traitement au titre du droit à l'information ou à l'explicabilité des décisions individuelles exclusivement automatisées, la mise en œuvre effective de cette mesure est complexe[449]. Au même titre que la protection des données dès la conception se décline en « *privacy by défaut* »[450], nous regrettons qu'il ne se

[446] Art. 25 § 1 du RGPD.
[447] G29, Lignes directrices sur la transparence au sens du RGPD du 11 avril 2018, p. 35.
[448] Art. 20 § 1, Directive (UE) 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.
[449] DARY M., BENAISSA L., « Privacy by Design : Un principe de protection séduisant mais complexe à mettre en œuvre », *Dalloz* IP/IT, 2016, p. 476 à 480.
[450] Art. 25 § 2 du RGPD et art 20 § 2 de Art. 20 § 1 la Directive (UE) 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

décline pas, comme nous le proposerons dans la seconde partie de ces travaux en « *transparency by design* » afin que ces traitements, et le cas échéant d'autres systèmes, soient conçus de manière impérative en tenant compte techniquement des méthodes les plus appropriées pour les expliquer, et auxquels cas, dans certains domaines, une telle impossibilité aboutirait à l'exclusion de certains méthodes d'IA qualifiées d'opaques[451]. En effet, au-delà des responsables du traitement, des obligations nouvelles de transparence doivent porter sur les fournisseurs de ces produits indépendamment de la bonne volonté des acteurs d'y recourir par la contractualisation[452].

220. Le CEPD a récemment eu l'occasion de préciser dans ses lignes directrices les éléments devant être contenus par la protection des données dès la conception et par défaut. De manière non exhaustive, sont visés la

> *« - Clarté - Les informations doivent être formulées en des termes clairs et simples, concis et compréhensibles.*
>
> *- Sémantique - La communication doit avoir une signification claire pour le public concerné.*
>
> *- Accessibilité - Les informations doivent être aisément accessibles pour la personne concernée.*
>
> *- Contextualité - Les informations doivent être fournies au moment opportun et sous la forme appropriée.*
>
> *- Pertinence - Les informations doivent être pertinentes et applicables à la personne concernée spécifique.*
>
> *- Conception universelle – Les informations doivent être accessibles à toutes les personnes concernées et inclure l'utilisation de langages lisibles par machine pour faciliter et automatiser la lisibilité et la clarté.*
>
> *- Compréhensibilité - Les personnes concernées doivent avoir une juste compréhension de ce qu'elles peuvent attendre en ce qui concerne le traitement de leurs données à caractère personnel, en particulier lorsqu'il s'agit d'enfants ou d'autres groupes vulnérables.*

[451] *Infra*., n° 893 et 961 et s.
[452] DOUVILLE T., *Droit des données à caractère personnel : droit de l'Union européenne, droit Français*, *op. cit.*, p. 207.

- Canaux multiples - Les informations devraient être fournies par différents canaux et médias, au-delà du texte, afin d'accroître la probabilité que les informations parviennent effectivement à la personne concernée.

- Structuration par couches – Les informations devraient être structurées par couches de manière à résoudre la tension entre l'exhaustivité et la compréhension, tout en tenant compte des attentes raisonnables des personnes concernées »[453].

221. La CNIL publie par ailleurs sur un site internet dédié des exemples de bonnes pratiques en matière d'information des personnes physiques concernées par un traitement de données personnelles[454].

B - L'analyse d'impact relative à la protection des données et la consultation préalable

1 – L'analyse d'impact relative à la protection des données

222. L'AIPD est obligatoire dans de nombreux cas. Elle est censée aboutir à une conception respectueuse de l'outil, conformément aux obligations du responsable du traitement, tout en assurant la démonstration de la conformité de ce dernier. Elle doit donc avoir lieu avant que le traitement ne soit mis en œuvre[455].

223. Elle est obligatoire lorsqu'un traitement est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.* »[456]. Elle est également requise pour trois types de traitement visés par le RGPD, à savoir

« *a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le*

[453] CEPD, Lignes directrices 4/2019 relatives à l'article 25, protections des données dès la conception et protections des données par défaut, version 2.0, adoptées le 20 octobre 2020, p. 17 et 18.
[454] *Site Données & Design par LINC* [en ligne] [Consulté le 23 février 2021]. Disponible à l'adresse : https://design.cnil.fr/
[455] Art. 35 § 1 du RGPD.
[456] Art. 35 § 1 du RGPD. Bien que le protocole 108+ laisse aux parties l'appréciation des mesures appropriées dans le but de la conformité aux obligations de la convention (art. 10 § 4), l'article 10 § 2 du protocole précise tout de même que « *chaque Partie prévoit que les responsables du traitement, ainsi que, le cas échéant, les sous-traitants, doivent procéder, préalablement au commencement de tout traitement, à l'examen de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des personnes concernées, et qu'ils doivent concevoir le traitement de données de manière à prévenir ou à minimiser les risques d'atteinte à ces droits et libertés fondamentales* ».

profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire; b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou c) la surveillance systématique à grande échelle d'une zone accessible au public. »[457]

224. L'analyse d'impact est réalisée par le responsable du traitement aussi bien sur les algorithmes que sur les données utilisées, ce qui n'est pas sans poser la question de la véracité entre ce qui est déclaré par le responsable du traitement et ce qu'il est ou adviendra réellement du traitement, décorrélant le traitement de la fiction juridique découlant de cette disposition. De plus, le caractère facultatif de certaines AIDP, laissée à l'appréciation du responsable du traitement, ne peut que dénaturer l'intention première, à savoir la philosophie du texte dans la mesure où ce mécanisme est censé offrir une traçabilité du traitement. Cela illustre la façon dont le déploiement de certaines techniques juridiques ne sert pas nécessairement le but initialement poursuivi, puisque au contraire, il rend inopérant l'esprit de la disposition. Il est à noter que la frontière entre une APID obligatoire et facultative est floue, notamment car il existe des exceptions[458], raison pour laquelle le responsable du traitement doit être attentif aux lignes directrices du G29, de la CNIL et autres recommandations, avis, ou encore règlements types susceptibles de l'imposer. Des opérations de traitement sont notamment soumises à l'obligation d'analyse d'impact. A cette fin, des listes sont publiées par les autorités de contrôle[459].

225. Pourtant, l'AIPD est en mesure de renseigner sur de nombreuses caractéristiques du traitement et est censée protéger à la fois le responsable du traitement d'éventuelles violations à la réglementation, mais aussi les personnes physiques concernées par ce traitement. Ainsi, elle doit au minimum contenir

[457] Art. 35 § 3 du RGPD.
[458] Voir en ce sens à titre d'exemple l'article 35 § 10 du RGPD, « *Lorsque le traitement effectué en application de l'article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.* ».
[459] Art. 35 § 4 et 5 du RGPD.

« a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement; b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités; c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées »[460].

226. Nous regrettons par ailleurs que le recours aux audits ne soit pas davantage utilisé par le RGPD pour suivre l'évolution du traitement alors que la conformité du traitement dans le temps avec l'analyse d'impact ne devrait pas être laissée à l'appréciation du responsable du traitement[461]. Naturellement, il convient de reconnaître que ces opérations ont un coût, mais il est essentiel à l'effectivité des droits et libertés.

227. Comme a pu le préciser le G29 dans ses lignes directrices relatives à l'AIPD, bien que le RGPD n'impose pas de publier ces analyses, il « *serait utile pour susciter la confiance dans les opérations de traitement du responsable du traitement et pour donner des gages de responsabilité et de transparence* »[462], surtout lorsque « *des citoyens sont affectés par l'opération de traitement* »[463]. Nous ne comprenons pas que la publication de ces AIPD ne soit pas obligatoire, même si cela impliquerait que certaines mentions soient occultées pour des raisons de conciliation entre la transparence directe et la sécurité ainsi que le secret des affaires par exemple. Mais une telle publication participerait nécessairement à ce que la société civile puisse concourir à la conformité quand bien même serait-elle mineure compte tenu du faible nombre d'informations publiées.

228. L'autorité de contrôle dispose toutefois de tous les éléments si elle en fait la demande, ou bien si la communication est obligatoire. On retrouve donc ici une transparence effectuée par l'intermédiaire d'un tiers de confiance. La confiance dans cette autorité doit alors être

[460] Art. 35 § 7 du RGPD.
[461] Art. 35 § 11 du RGPD.
[462] G29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, p. 21.
[463] *Ibid.*

certaine, ce qui nécessite de la part du citoyen un important contrôle au sujet de son action, et une augmentation de ses moyens afin que cette conformité soit correctement réalisée.

2 - La consultation préalable

229. Comme nous l'avons évoqué, sauf dans de rares situations, la nouvelle règlementation a mis fin au régime d'autorisation préalable[464]. Le RGPD prévoit dans certains cas que le responsable du traitement consulte l'autorité de contrôle[465] afin qu'il lui transmette des informations sur le traitement[466], en vue de le conseiller et de formuler un avis, ce qui concourt à la transparence vis-à-vis du régulateur et est susceptible de l'alerter sur de nombreuses irrégularités, et le cas échéant de cibler des contrôles pour qu'elle s'assure qu'elles ont été comblées lorsque le traitement est mis en œuvre. La CNIL joue parallèlement, dans le cadre de cette procédure, un rôle de conseil auprès du responsable du traitement. Il s'agit, au même titre que l'AIPD d'une intervention en amont, c'est-à-dire avant que n'entre en fonctionnement le traitement.

230. Elle s'applique dans l'hypothèse où l'AIPD conclut à ce « *que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque* »[467]. Le G29 précise que « *lorsque le responsable du traitement ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable (à savoir que les risques résiduels demeurent élevés), une consultation de l'autorité de contrôle est obligatoire* »[468].

231. La CNIL est donc amenée à se prononcer par un avis sur ces éléments si elle estime que le responsable du traitement n'a pas apporté les corrections nécessaires en vue d'atténuer ou d'identifier le risque. La mise en œuvre du traitement restera suspendue jusqu'à ce que l'autorité

---

[464] *Supra*., n° 208 et s.
[465] Art. 36 du RGPD.
[466] « *a) le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement, en particulier pour le traitement au sein d'un groupe d'entreprises;*
b) les finalités et les moyens du traitement envisagé ;
c) les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées en vertu du présent règlement ;
d) le cas échéant, les coordonnées du délégué à la protection des données ;
e) l'analyse d'impact relative à la protection des données prévue à l'article 35 ; et
f) toute autre information que l'autorité de contrôle demande », art. 36 § 3 du RGPD.
[467] Art. 36 § 1 du RGPD.
[468] G29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, p. 22.

de contrôle bénéficie des éléments suffisants, même s'il ne s'agit pas pour autant d'un régime d'autorisation.

C - Le registre des opérations

232. Bien que le G29 ne mentionne pas comme tel le registre des activités de traitement comme une mesure de transparence, il nous apparaît qu'il peut concourir à la compréhension des traitements. C'est un véritable outil de conformité au RGPD. Les organisations de moins de 250 salariés ne sont cependant pas tenues d'avoir un tel registre sauf à manipuler des données sensibles ou si le « *si le traitement effectué est susceptible de comporter un risque pour les droits et des libertés des personnes concernées* »[469].

233. Lorsque la tenue d'un registre est obligatoire pour le responsable du traitement ou son représentant, il contient de nombreuses informations sur le traitement des données tels que la finalité, les transferts de données vers un Etat tiers, les délais prévus pour l'effacement, les noms et coordonnées des responsables du traitement notamment[470]. A cet égard, le registre permet de vérifier la conformité ainsi que la traçabilité du processus.

234. De plus, nous ne pouvons que regretter comme le souligne Christina Koumpli, que ces registres ne soient pas rendus publics aux utilisateurs qui en feraient la demande, ne serait-ce qu'à des fins de contribution d'une plus grande transparence[471]. Il convient toutefois de préciser que conformément aux dispositions du CRPA[472], si une entreprise privée se voit confier un traitement de données à caractère privé à des fins d'une mission de service public, ou d'une administration, il est possible pour l'usager de ce service d'en obtenir la communication, car il s'agit d'un document administratif communicable, sous réserve des secrets protégés par la loi.

235. Dans l'hypothèse où le responsable du traitement omettrait de prévenir la personne physique qu'un traitement s'opère, par la voie d'une mention explicite, l'accès au registre permettrait de découvrir l'existence d'un traitement, et donc de faire valoir ensuite son droit d'accès à ses données personnelles par exemple. Au titre de ses obligations de responsable du

---

[469] Art. 30 § 5 du RGPD.
[470] Art. 30 du RGPD.
[471] Christina Koumpli note à cet égard qu'« *on peut légitimement se demander pourquoi le registre n'est pas directement accessible au public afin de satisfaire plus facilement le droit à la transparence des personnes concernées ? Finalement, il semble paradoxal que les nouvelles technologies aujourd'hui très développées pour le traitement des données ne soient pas aussi utilisées au bénéfice des personnes concernées afin de garantir l'effectivité de leurs droits prévus par la RGPD* », KOUMPLI C., *Les données personnelles sensibles : contribution à l'évolution du droit fondamental à la protection des données à caractère personnel : étude comparée : Union européenne, Allemagne, France, Grèce, Royaume-Uni*, *op. cit*., spec. p. 470.
[472] *Infra*., n° 410 et s.

traitement, la CNIL[473] a notamment eu à publier son registre, mais elle y a fait figurer dans ce document les obligations complémentaires telles que les informations visées par les articles 13, 14 et 15 du RGPD[474], ce qui offre plus de clarté et de transparence[475]. Or, nous ne pouvons que regretter ce caractère facultatif, dans la mesure où le plus souvent ce sont les plus irréprochables qui offrent le plus haut degré de transparence, d'où la nécessité d'imposer un seuil maximal de transparence pour tous les acteurs. La difficulté est au contraire d'obtenir une information véritable de la part de ceux les plus susceptibles de ne pas respecter leurs obligations.

236. L'article L. 121-4-2 du Code de l'éducation concourt également à une certaine transparence des traitements algorithmiques. En effet, lors des discussions de la LIL de 2018[476], a été introduit dans le Code de l'éducation une nouvelle disposition. Ainsi, « *l'autorité responsable des traitements de données à caractère personnel mis en œuvre dans les établissements publics d'enseignement scolaire met à la disposition du public le registre comportant la liste de ces traitements […]* ». La mise à disposition du public d'un registre indiquant la liste des traitements déployés par l'Education nationale permet tout un chacun de consulter ces informations, et donc y compris aux parents d'élèves, ce qui permet d'enquêter sur la base de cette prise de connaissance. Il est effectivement impossible, comme nous l'avons déjà évoqué, d'obtenir la transparence de ces traitements lorsqu'on ignore leur existence. Toutefois, force est de constater que le degré et la nature de ce principe de transparence qui ne dit pas son nom, bien que certains membres de la doctrine l'aient nommé comme tel[477], est imprécis et ne permet pas de connaître l'exactitude du fonctionnement des traitements mis en œuvre dans la mesure où, comme nous l'avons vu, le RGPD n'offre pas toujours une très grande transparence à ce sujet. En effet, la transparence telle que prévue par cette règlementation empêche de rejouer les opérations du traitement, à moins qu'il ne s'agisse d'une décision administrative individuelle, auquel cas, c'est le régime juridique de la transparence se trouvant dans le CRPA qui s'y appliquera[478].

[473] Et comme le considérant 52 incite les institutions de l'UE à le faire pour plus de transparence.
[474] *Supra.*, n° 86 et s.
[475] CNIL, La CNIL publie son registre RGPD, *CNIL.fr* [en ligne], 02 décembre 2019, mis à jour le 13 mai 2020. [Consulté le 10 août 2020]. Disponible à l'adresse : https://www.cnil.fr/fr/la-cnil-publie-son-registre-rgpd ; MAXIMIN N., « Données personnelles : pourquoi la CNIL publie-t-elle son registre RGPD ? », *Dalloz actualité*, 6 décembre 2019.
[476] Art. 22 de la LIL modifiée.
[477] BROGLI M., CATELAN N., CASTETS-RENARD C., DE LA CLERGERIE M., DUBOIS L., FAVRO K., JAULT-SESEKE F., GAULLIER F., GRYNWAJC S., LE BRET A., MARTIAL-BRAZ N., MATSUBARA M., MAXWELL W., PAULIN B., ROCHFELD J, STALLA-BOURDILLON S., TOULOTTE T., ZANOTTI F., ZOLYNSKI, C., *Droit des données personnelles, Les spécificités du droit français au regard du RGPD, Dalloz décryptage*, 2019, spec. p. 116.
[478] *Infra*., n° 435 et s.

D - Le délégué à la protection des données à caractère personnel

237. Il est l'héritier du correspondant à la protection des données à caractère personnel institué par la loi n° 2004-801 du 6 août 2004. Sa désignation n'était que facultative mais ouvrait en contrepartie la possibilité à des simplifications, voire à des dispenses, dans le régime d'autorisation précédant l'entrée en application du RGPD.

238. Très brièvement, car nous serons amenés à évoquer la réforme de cette institution dans le cadre de la seconde partie afin d'étendre ses missions au-delà des données personnelles[479], le DPD concourt à l'effectivité des nombreuses dispositions relatives à la transparence prévues par la réglementation. Lorsqu'il n'est pas entravé dans ses missions il est un atout majeur de la conformité. Il s'agit donc d'un mécanisme de corégulation pragmatique partant du postulat que le régulateur ne peut pas contrôler en permanence tous les acteurs, et qu'il conviendrait mieux d'associer ces professionnels à leur mise en conformité, et ce par l'intermédiaire de cette institution, n'empêchant pas par ailleurs des contrôles opérés par la CNIL[480].

239. Désormais, selon ce texte, sa désignation est obligatoire dans quatre situations, aussi bien pour le responsable du traitement que le sous-traitant, à savoir lorsque

> « *a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;*
>
> *b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou*
>
> *c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à*

[479] *Infra*., n° 883 et s.

[480] TURK A., Rapport public n°218 sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés du Sénat, session ordinaire de 2002-2003, fait au nom des lois constitutionnelles, de législation, du suffrage universel, Règlement et d'administration générale, enregistré à la Présidence du Sénat le 19 mars 2003, « *Leur mise en place doit permettre à la CNIL de disposer d'un réseau de correspondants, ainsi que cela existe déjà dans le secteur public. En effet, une seule autorité de contrôle ne peut pas tout assurer* », p. 95.

l'article 9[481] *ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10* »[482].

240. Enfin, l'Union européenne ou les Etats membres ont par ailleurs la possibilité de le rendre obligatoire pour les responsables du traitement ou leurs sous-traitants ou « *les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants* »[483].

241. Il est une interface aussi bien vis-à-vis de l'autorité de contrôle[484] que des personnes physiques concernées par un traitement, et a également pour mission de conseiller le responsable du traitement ou le sous-traitant qui l'emploie dans sa mise en conformité[485]. Il est un interlocuteur privilégié et l'un des garants de l'exercice des droits, y compris du droit à l'information de la personne physique concernée par un traitement[486] : à cet égard, *« les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le présent règlement* »[487]. Par ailleurs, le DPD exerce un rôle significatif dans l'élaboration et le suivi du registre des opérations, de l'AIPD et de la consultation préalable[488].

242. Il est un outil important de conformité lorsqu'il est compétent, raison pour laquelle la CNIL peut procéder à la certification des compétences du DPD selon deux référentiels qu'elle a établi. Le premier permet à la CNIL d'évaluer le délégué lui-même[489], tandis que l'autre certifie par l'obtention d'un agrément les organismes habilités à certifier les DPD[490]. Toutefois, cette certification n'est pas obligatoire pour exercer cette fonction et il n'est pas pleinement indépendant, notamment car il ne bénéficie pas du statut de salarié protégé[491].

---

[481] Il s'agit des données sensibles prévues à l'article 9 du RGPD. *Supra*., n° 110.
[482] Art. 37 § 1 du RGPD. Il convient d'ajouter que l'article 103 de la LIL modifiée prévoit que les traitements de données personnelles en matière de police et de justice, à l'exception de ceux utilisés par les juridictions dans ce domaine, imposent la désignation d'un DPD. Le cas échéant la désignation d'un seul DPD pour plusieurs services est autorisée.
[483] Art. 37 § 4 du RGPD.
[484] Art. 39 § 1 d) du RGPD.
[485] Art. 39 du RGPD.
[486] Art 13 § 1 b) et 14 § 1 b) du RGPD.
[487] Art. 38 § 4 du RGPD.
[488] *Supra*., n° 216 et s.
[489] CNIL, Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPD).
[490] CNIL, Délibération n° 2018-317 du 20 septembre 2018 portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données (DPD).
[491] SENAT, Statut des délégués à la protection des données, Réponse ministérielle publiée dans le JO du Sénat le 7 février 2019, p. 712, www.s*enat.fr*, [en ligne]. [Consulté le 02 mars 2021]. Disponible à l'adresse :

PARAGRAPHE 2 - Les mécanismes de droit non contraignant

243. Afin de compléter et démontrer cette mise en conformité, le législateur européen propose également le recours au code de conduite[492] ou à la certification[493], ce que rappelle par ailleurs le G29 dans ses lignes directrices sur la transparence[494]. Bien que ces éléments soient à géométrie variable, un mécanisme de droit souple peut toutefois devenir du droit dur si un engagement a été pris par l'acteur concerné. Les codes de conduite (A) et la certification et labels (B) sont cités par le RGPD à des fins de conformité et sont encouragés par les Etats membres afin d'assurer la conformité des traitements notamment aux règles de transparence.

A - Les codes de conduite

244. A la lumière du préambule du RGPD[495], qui a une valeur interprétative du texte, le code de conduite apparaît comme un outil permettant « *la mise en œuvre de mesures appropriées et à la démonstration par le responsable du traitement ou leur sous-traitant du respect du présent règlement* ». Il convient donc logiquement d'en déduire que les codes de conduite participent à la démonstration de la conformité du principe de transparence garanti par le RGPD[496]. En ce sens, le CEPD précise que cet outil est susceptible d'instaurer la confiance en améliorant la transparence du traitement à l'encontre des individus[497].

245. Selon l'article 40 § 1 du RGPD, les codes de conduite peuvent notamment être élaborés afin de préciser les modalités en matière de loyauté et de transparence du traitement[498], la collecte des données à caractère personnel[499], les informations communiquées au public et aux personnes concernées[500] et l'exercice de leurs droits[501]. Ils ne peuvent être pris qu'à l'initiative

https://www.senat.fr/questions/base/2018/qSEQ180102896.html#:~:text=Minist%C3%A8re%20du%20travail-,publi%C3%A9e%20dans%20le%20JO%20S%C3%A9nat,%2F02%2F2019%20%2D%20page%20712&text=Le%20r%C3%A8glement%20est%20un%20acte,de%20son%20entr%C3%A9e%20en%20vigueur

[492] Art. 40 et 41 du RGPD.

[493] Art. 42 du RGPD.

[494] G29, Lignes directrices sur la transparence au sens du RGPD du 11 avril 2018.

[495] Considérant 100 du RGPD.

[496] Conformément au contenu du principe abordé lors du premier chapitre de cette thèse, *Supra.*, n° 86 et s.

[497] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, version 2.0 uniquement en anglais, adopté le 4 juin 2019, « *Codes can be an effective tool to earn the trust and confidence of data subjects. They can address a variety of issues, many of which may arise from concerns of the general public or even perceived concerns from within the sector itself, and as such constitute a tool for enhancing transparency towards individuals regarding the processing of their personal data* », p. 10. Nous traduisons « Les codes peuvent être un outil efficace pour gagner la confiance des personnes concernées. Ils peuvent aborder une variété de questions, dont beaucoup peuvent découler de préoccupations du grand public ou même de préoccupations perçues au sein du secteur lui-même, et constituent donc un outil permettant d'améliorer la transparence envers les individus en ce qui concerne le traitement de leurs données personnelles ».

[498] Art. 40 § 2 (a) du RGPD.

[499] Art. 40 § 2 (c) du RGPD.

[500] Art. 40 § 2 (e) du RGPD.

[501] Art. 40 § 2 (f) du RGPD.

d'associations ou d'organismes du secteur professionnel en question, et sont fortement encouragés[502]. Il est à noter que les projets de code de conduite, incités par les Etats membres et les autorités de contrôle[503], devront être validés par ces derniers afin de s'assurer qu'ils offrent une conformité au RGPD[504]. Bien que l'élaboration d'un code de conduite soit facultative, même si certains Etats membres les ont rendus obligatoires dans certains domaines[505], il n'en demeure pas moins qu'une fois élaboré et validé par l'autorité compétente, il engage ceux qui l'ont adopté à le respecter. Le code de conduite est également fortement recommandé par le Règlement aux responsables du traitement qui ne seraient pas soumis au RGPD[506]. Ce n'est qu'après sa validation, afin de s'assurer de sa conformité à la réglementation[507], que l'autorité de contrôle mentionne son existence dans un registre afin notamment de le mettre à la disposition du public[508], à moins que cette communication ne remette en cause, par exemple, le secret des affaires. A cet égard, la conformité à ces obligations est uniquement réalisée par l'autorité de contrôle de l'Etat membre concerné, ou à défaut par l'autorité de contrôle de l'Union européenne[509]. Il est également possible que ce respect soit assuré par un organisme agrée[510]. Par ailleurs, s'il s'agit d'un code de bonne conduite applicable à l'échelle de l'Union, après avis du CEPD[511], la Commission est susceptible de le rendre d'application générale pour tous les Etats membres[512]. Ce dernier est ensuite enregistré et publié par l'autorité de contrôle[513]. La CNIL a en ce sens été amenée à approuver le premier code de conduite européen initié par l'association européenne de fournisseurs de services d'infrastructure Cloud[514]. Ce code de conduite détaille par ailleurs des exigences de transparence sectorielles, notamment en matière de sécurité[515]. Il s'agit d'un complément à l'effectivité du RGPD, puisque l'adoption d'un tel code, même au niveau européen, ne dispense pas d'éventuels contrôles des autorités nationales de l'Union.

[502] Art. 40 § 2 et cons. 98 du RGPD.
[503] Art. 40 § 1 et cons. 98 du RGPD.
[504] Art. 40 § 5 du RGPD.
[505] Tel est le cas par exemple le cas de la DPA Anglaise pour les traitements journalistiques. En ce sens, voir, TAMBOU O., *Manuel de droit européen de la protection des données à caractère personnel*, *Bruylant*, 2020, p. 299.
[506] Art. 40 § 3 du RGPD.
[507] Art. 40 § 5 du RGPD.
[508] Art. 40 § 11 du RGPD.
[509] Art. 40 § 4 du RGPD.
[510] Organisme agréé par l'art. 41 § 1 en vertu de l'art. 40 § 4 du RGPD.
[511] Art. 40 § 8 du RGPD
[512] Art. 40 § 9 du RGPD
[513] Art. 40 § 11 du RPGD.
[514] CNIL, Délibération n° 2021-065 du 3 juin 2021 portant approbation du code de conduite européen porté par Cloud Infrastructure Service Providers Europe (CISPE).
[515] CISPE, *Code de conduite des Fournisseurs d'infrastructures Cloud relatif à la Protection des données*, du 9 février 2021.

246. Il est intéressant de noter que le code de conduite comporte un volet collaboratif faisant aussi bien participer les autorités de contrôle que les responsables du traitement ou leur regroupement à l'élaboration de leur propre conformité. Cela rejoint parfaitement le qualificatif de gouvernance collaborative, désigné par Margot E. Kaminski. Qu'ils soient de nature privée ou publique, ces acteurs s'associent et participent à l'édiction de la norme juridique de droit souple. En recevant ces propositions, l'autorité de contrôle enrichit le projet de code de conduite afin qu'il soit amélioré puis validé. Mais comme certains auteurs l'indiquent[516], nous pouvons regretter que les personnes physiques faisant l'objet de ces traitements ne soient pas associées à l'élaboration de ces normes alors qu'elles sont susceptibles d'être concernées en premier lieu par leur application[517].

B - La certification

247. Conformément au considérant 100 du RGPD et à l'article 42 paragraphe 1 de ce dernier, la certification et les labels ont vocation à ce que les responsables du traitement ou bien leurs sous-traitants, procèdent à des opérations de traitement conformes à la réglementation. En s'assurant de la conformité d'un système à un référentiel préalablement établi par un organisme tiers ou par une autorité de contrôle, elle participe d'une manière générale au respect du RGPD tout en y favorisant une plus grande transparence[518].

248. Cela étant, le texte dispose que les exigences de certification diffèrent en fonction de la taille de l'entreprise, ce qui interroge puisque cela se fait nécessairement au détriment des droits attachés à la personne. Il est important de rappeler que ce n'est pas parce que « les opérations de traitement » ont fait l'objet d'une certification que cela exonère les responsables du traitement et ses éventuels sous-traitants de leurs obligations d'information que nous avons étudiées[519]. La certification est volontaire, et donc non obligatoire. Elle doit toutefois être

[516] KAMINSKI M, E., « Binary Governance : Lessons from the GDPR's Approche to Algorithmic Accountability », *op. cit.,* p. 1609.
[517] En ce sens, le considérant 99 du RGPD se prononce en faveur de cette option, mais il n'a aucune force obligatoire : « *Lors de l'élaboration d'un code de conduite, ou lors de sa modification ou prorogation, les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants devraient consulter les parties intéressées, y compris les personnes concernées lorsque cela est possible, et tenir compte des contributions transmises et des opinions exprimées à la suite de ces consultations* ».
[518] RGPD, considérant 100, « *Afin de favoriser la transparence et le respect du présent règlement, la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données devrait être encouragée pour permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question* ».
[519] *Supra.,* n° 93 et s.

accessible à travers un processus transparent[520]. La disposition précise également que les responsables du traitement qui ne sont pas soumis au RGPD peuvent toutefois recourir à la certification afin de démontrer qu'ils respectent « *des garanties appropriées dans le cadre des transferts de données à caractère personnel vers un pays tiers* ». Concernant les transferts de données prévus à l'article 46 du RGPD, les garanties visées à l'article 46 paragraphe 1 sont satisfaites dès lors qu' *« un mécanisme de certification approuvé conformément à l'article 42, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées* »[521].

249. Il est recommandé par le CEPD dans ses lignes directrices que l'évaluation d'un produit porte notamment sur les opérations de traitement ainsi que sur ses finalités[522]. Néanmoins, la pertinence de la certification est variable puisqu'elle dépend des moyens et de l'intention des sociétés qui décident d'y recourir, ce qui influe de fait sur sa pertinence. La documentation de l'évaluation joue de plus un rôle essentiel car elle permet également une meilleure transparence du mécanisme de certification puisque « *l'évaluation permettra de comparer la documentation de la certification avec la situation réelle sur site et par rapport aux critères de certification.* »[523]. Il est intéressant de souligner que le CEPD porte une attention particulière à l'intelligibilité de la certification auprès des clients de ces produits. En effet, les organismes certificateurs doivent rendre accessible et intelligible un certain nombre d'informations au sujet de la certification des opérations de traitement tels que

> *« (…) la description de la cible d'évaluation ; • la référence aux critères approuvés appliqués à la cible d'évaluation spécifique ; • la méthodologie de l'évaluation des critères (évaluation sur site, documentation, etc.) ; et • la durée de validité du certificat ; et • devraient permettre la comparabilité des résultats par les autorités de contrôle et le public. »*[524]

[520] Art. 42 § 3 du RGPD.
[521] Art. 46 § 2 f) du RGPD.
[522] CEPD, Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement, version 3.0 du 4 juin 2019, § 61, p. 21 [en ligne] [Consulté le 15 juin 2020]. Disponible à l'adresse :
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_fr.pdf
[523] *Ibid.*, § 63 et 64, p. 21.
[524] *Ibid.*, § 66, p. 22.

250. Enfin, concernant le choix des critères de certification, les critères retenus doivent être uniformes et vérifiables à des fins de conformité, notamment *« afin de faciliter l'évaluation des opérations de traitement au titre du RGPD »*[525].

251. En France, ce travail de certification peut être aussi bien opéré par l'autorité de contrôle nationale que par un tiers certificateur bénéficiant d'un agrément délivré par la CNIL[526]. Au-delà de la certification des traitements algorithmiques, il semble curieux que le législateur national ait permis la certification des personnes[527], comme des DPD[528], dans la mesure où cela laisse à penser que les prestations de service de ces personnes seraient nécessairement en conformité avec le RGPD, ce qui pourrait être fallacieux pour les entreprises recourant au service de ces personnes ou le consommateur, quand bien même cette certification peut dans les faits faire l'objet d'un retrait en cas de manquement[529] à la suite d'un contrôle. Une fois délivrée, la durée de la certification ne peut excéder trois ans[530]. Quant à l'agrément dont bénéficie le tiers certificateur, sa durée est de cinq ans maximums renouvelable[531]. Si l'autorité de contrôle a pour mission ce rôle de certificateur, elle se doit d'être particulièrement transparente dans le cadre de cette tâche et veiller à prévenir tout risque de conflit d'intérêt ou de séparation des pouvoirs avec ses compétences en matière d'enquête[532].

252. Pour conclure, la certification reflète à notre sens le fait que le traitement algorithmique est conforme au RGPD à un instant T en fonction des critères préétablis. Or, en informatique, les traitements évoluent en permanence, et nous avons l'impression, qu'au même titre que les labels, la certification est davantage susceptible d'être un argument commercial qu'un véritable gage de conformité à l'inverse d'un audit. Le coût de ces certifications est par ailleurs un frein à leur généralisation.

---

[525] *Ibid*., § 67, p. 23.
[526] Dans les conditions prévues à l'art 43 du RGPD.
[527] Art. 8 h) de la LIL modifiée, au regard de la loi informatique et libertés, la CNIL « *(…) peut décider de certifier des personnes, des produits, des systèmes de données ou des procédures aux fins de reconnaître qu'ils se conforment au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et à la présente loi* ».
[528] *Supra*., n° 237 et s.
[529] Art. 20 III 4° de la LIL modifiée.
[530] Art. 42 § 7 du RGPD.
[531] Art. 43 § 4 du RGPD.
[532] CEPD, Lignes directrices 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement, version 3.0 du 4 juin 2019, *op. cit.*, § 22, p. 11.

CONCLUSION DU CHAPITRE II

253. Comme nous l'avons constaté, le RGPD repose sur une ambivalence. D'une part, il souhaite un haut niveau de protection des droits des individus sur le traitement de leurs données à caractère personnel, et d'autre part, il donne un rôle significatif aux acteurs abordés dans leur mise en conformité afin de faciliter la libre circulation de ces données au sein de l'Union. La synthèse de ces deux objectifs créée un déséquilibre tant les exceptions sont nombreuses et les pouvoirs des autorités de contrôle affaiblis à certains égards puisque l'effectivité du principe ne repose que trop grandement sur la bonne volonté des responsables du traitement.

CONCLUSION DU TITRE I

254. Le droit européen et national ambitionne aussi bien une transparence théorique (les informations à communiquer) qu'effective (les mécanismes de contrôle) des traitements de données à caractère personnel. Ce régime juridique demeure toutefois imparfait. Il s'agit avant tout d'une règlementation visant à fluidifier la circulation des données au sein de l'Union européenne, ce qui se fait souvent au détriment des droits des personnes physiques concernées par les traitements. Le basculement d'un régime d'autorisation vers celui d'une responsabilisation des acteurs repose sur de nombreux mécanismes de droit non contraignant illustrant une certaine naïveté de la part du législateur européen au sujet de responsables du traitement peu scrupuleux.

255. En effet, afin de s'assurer de l'effectivité de cette transparence, les personnes physiques concernées par ces traitements sont dans une situation de vulnérabilité en ce qu'ils ne peuvent vérifier la véracité des informations qui leur sont communiquées au titre de leurs droits. La conformité de ces informations, de plus parfois stéréotypées, ne peut être effectuée que par une autorité publique qui ne bénéficie pas pour l'heure des moyens adéquats. De plus, l'élaboration de nombreux mécanismes de conformité est laissée à l'appréciation des acteurs, donnant l'impression d'une transparence à géométrie variable.