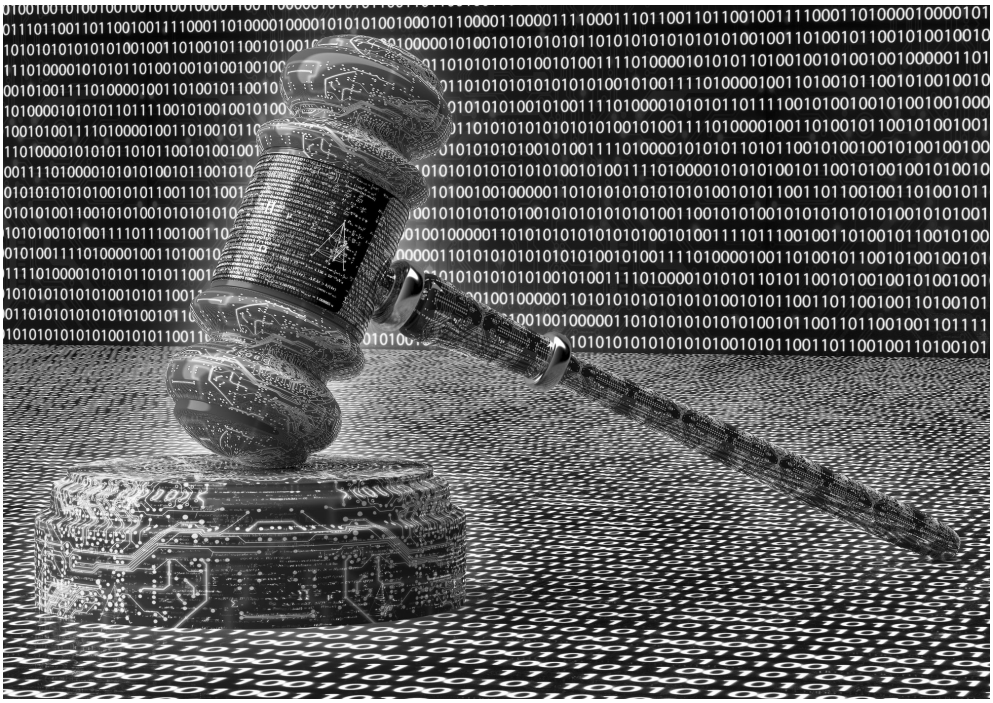
Règlement général relatif à la protection des données personnelles

Le régime novateur des sanctions



FRANÇOIS BOUCARD

Docteur en droit, Avocat au Conseil d'État et à la Cour de cassation

Le nouveau règlement européen de protection des données personnelles alourdit considérablement les sanctions des manquements aux obligations définies par le texte, mais surtout opère une remise à plat totale du système de sanctions existant dans notre droit. Pour autant, ce régime de sanctions novateur n'offre pas une sécurité juridique suffisante et suscite à juste titre l'inquiétude des professionnels.

Les sanctions constituent le volet sans doute le plus novateur du futur régime de protection des données à caractère personnel. Le règlement instaure plusieurs types de sanctions. Tout d'abord, il rappelle que les auteurs d'un manquement aux obligations créées par le règlement sont responsables du préjudice qu'ils doivent réparer. Le texte prévoit également des sanctions pénales mais il laisse aux États membres le soin d'en déterminer le régime. Le règlement se borne à préciser que ces sanctions doivent être effectives, proportionnées et dissuasives (art. 84). Les dispositions les plus substantielles concernent les amendes administratives, auxquelles seront exclusivement consacrés les développements qui suivent. Elles se caractérisent par leur montant considérablement élevé puisqu'il peut atteindre 20 000 000 euros ou 4 % du chiffre d'affaires annuel mondial total. Ces montants contrastent singulièrement avec les sanctions pécuniaires que la CNIL peut aujourd'hui prononcer, lesquelles sont limitées à 150 000 euros et, en cas de récidive, à 300 000 euros. Les évolutions consacrées par le nouveau règlement ne concernent pas que le montant des amendes administratives. Le nouveau texte opère une remise à plat totale du système de sanctions existant dans notre droit. Il institue un régime sophistiqué dont l'étude commande de distinguer les manquements sanctionnés (I.) et le prononcé des sanctions (II.).

I. LES MANQUEMENTS SANCTIONNÉS

Les manquements sanctionnés ne font l'objet d'aucune définition dans le règlement. Si l'on s'en tient au texte relatif aux amendes administratives, l'article 83, la définition du manquement ne suscite pas de difficulté apparente. Le premier paragraphe de cet article dispose en effet que les amendes administratives sont imposées pour des « *violations du présent règlement* ». Et comme l'application du règlement incombe au premier chef au responsable du traitement et au sous-traitant[1], on conçoit sans peine qu'une sanction soit encourue lorsque ces derniers méconnaissent une disposition du règlement. Mais à y regarder de plus près, le texte européen manque de précision, qu'il s'agisse de déterminer les règles dont la méconnaissance peut entraîner une sanction (1.) ou d'identifier les personnes à l'encontre desquelles une sanction peut être prononcée (2.).

1. Les normes dont la violation justifie une sanction

La violation d'une disposition du règlement entraîne, bien sûr, le prononcé d'une sanction. Il suffit de se reporter à l'énumération figurant à l'article 83, § 4 et 5 (*v. infra*, II-2). La difficulté provient de ce que, s'agissant des sanctions, le règlement se borne à sanctionner les violations de ses propres dispositions sans autre précision. Or ce texte est incomplet et renvoie à d'autres autorités le soin d'édicter des normes en matière de protection des données. Il existe donc des sources complémentaires, prévues par le règlement lui-même, qui donnent naissance à un droit dérivé.

Il s'agit tout d'abord des textes de droit interne ayant pour objet d'apporter des précisions ou des limitations aux règles prévues par le règlement[2]. Si ce dernier est d'effet direct, il prévoit toutefois que certaines de ses dispositions peuvent ou doivent être complétées par les États membres, afin de garantir la cohérence et de clarifier le droit positif[3]. C'est ainsi, par exemple, que les États membres peuvent ajouter au règlement des règles relatives au traitement des données à caractère personnel des personnes décédées[4] au sujet duquel le texte européen ne dit rien. Ils doivent prévoir des sanctions pénales en complément des amendes administratives (art. 84).

En outre, le règlement prévoit que les autorités de contrôle doivent contribuer au développement des codes de bonne conduite qui s'imposent aux responsables de traitement. Bien que ces dispositions ne s'incorporent pas au règlement, il semble qu'elles puissent faire l'objet d'une sanction ainsi qu'il résulte de l'article 41, § 4 du règlement[5].

Par ailleurs, le règlement délègue à la Commission européenne le pouvoir d'adopter certains actes concernant notamment la certification, les éventuelles mesures spécifiques à prendre pour les micros, petites et moyennes entreprises ainsi que les codes de conduite et les clauses type de protection[6]. La méconnaissance de ces actes est assimilée à la violation d'une disposition du règlement, ainsi que le prévoit le considérant 146.

La même question se pose à propos des normes adoptées par le Comité européen de la protection des données (CEPD) auquel le règlement confère une compétence normative non négligeable. Le CEPD a vocation à remplacer le G29 institué par l'article 29 de la directive 95/46. À la différence de ce dernier, le CEPD est expressément qualifié d'organe de l'Union européenne et le règlement lui attribue la personnalité juridique. Il a notamment pour mission d'établir des lignes directrices dans de nombreux domaines énumérés à l'article 70, § 1 (pts d à m). Ces lignes directrices ont, dans l'ensemble, pour objet de préciser certaines des dispositions du RGPD notamment « *d'établir les violations de données à caractère personnel* » (art. 70, § 1, pt g) et de préciser, à l'intention des autorités de contrôle nationales, la fixation des amendes administratives, la mise en œuvre des pouvoirs d'enquête et l'application de mesures dites « *correctrices* » telles qu'un avertissement, un rappel à l'ordre ou une mise en demeure (art. 70, § 1, pt k, par renvoi à l'art. 58, § 1 à 3). Le RGPD ne précise pas si la méconnaissance des directives du CEPD est susceptible d'entraîner une sanction, qu'elle soit pénale ou administrative.

Le règlement prévoit également que les entreprises peuvent adopter des règles contraignantes qui, par nature, confèrent des « *droits opposables* » aux personnes concernées par le traitement de données à caractère personnel. Ces règles sont approuvées par l'autorité de contrôle et, en cas de méconnaissance de l'une d'elles, le responsable de traitement peut voir sa responsabilité engagée. Le texte ne précise pas si cette responsabilité est engagée envers les personnes concernées par un traitement de données ou bien à l'égard de l'autorité de contrôle qui pourrait alors prononcer une sanction. Mais ces règles ayant pour objet de conférer des droits aux personnes concernées par un traitement, il semble que leur méconnaissance ne soit susceptible d'entraîner qu'une simple responsabilité du responsable de traitement à l'égard des personnes concernées. L'auteur du manquement sera donc tenu de réparer le dommage qu'il aura causé. Aucune des dispositions du règlement ne prévoit qu'un manquement à une règle d'entreprise contraignante puisse faire l'objet d'une amende administrative. Les règles d'entreprise contraignantes n'appartiennent donc pas au bloc de normes dont la méconnaissance peut justifier une sanction prévue par le règlement.

Des hésitations du même ordre rendent délicate la détermination des personnes susceptibles d'être sanctionnées.

1. Dans le règlement, le responsable du traitement et le sous-traitant sont soumis à des dispositions qui, pour l'essentiel, sont identiques. Dans la suite de cet article, nous utiliserons l'expression « responsable du traitement » pour désigner à la fois le responsable du traitement et le sous-traitant. Nous nous référerons à la notion de « sous-traitant » pour examiner les seules dispositions propres à ce dernier.
2. Sur les règlements qui ne sont pas « auto-suffisants » et les conséquences qui en découlent sur leur invocabilité en droit interne, voir E. Dubout et B. Nabli, *Droit français de l'intégration européenne*, LGDJ 2015, p. 127.
3. Voir le considérant 8 du règlement.
4. Considérant 27 du règlement.
5. « *Sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente et des dispositions du chapitre VIII* […] », étant précisé que le chapitre VIII est consacré aux sanctions.
6. Il peut s'agir d'actes délégués ou d'actes d'exécution. Sur le régime juridique et la distinction entre ces actes, voir S. Van Raepenbusch, *Droit institutionnel de l'Union européenne*, Larcier 2011, p. 250, ainsi que J.-P. Jacqué, « Commission européenne après Lisbonne, déclin ou changement de paradigme ? » *in Liber Amicorum en l'honneur du professeur Vlad Constantinesco*, Bruylant, 2015, p. 256.

2. Les personnes susceptibles d'être sanctionnées

La détermination de la personne susceptible d'encourir une sanction soulève des difficultés pour les raisons suivantes. L'article 83 du règlement, relatif aux amendes administratives, prévoit un montant maximal, autrement dit un plafond. En réalité, il existe deux plafonds et donc deux niveaux de sévérité des amendes en fonction de la gravité des manquements. S'agissant des amendes les moins sévères, le texte précise expressément les personnes à l'encontre de qui elles sont susceptibles d'être prononcées. Il s'agit du responsable du traitement, de l'organisme de certification et de l'organisme chargé du suivi des codes de conduite, pour les obligations leur incombant respectivement (art. 83, § 4). Mais en ce qui concerne les amendes administratives les plus élevées, le texte définit le manquement susceptible d'en justifier le prononcé sans indiquer la personne qui encourt la sanction. C'est dans cette hypothèse que les dispositions du RGPD, par leur imprécision, laissent le justiciable dans le flou.

C'est au premier chef au responsable du traitement qu'incombe la mise en œuvre des dispositions du règlement ainsi que le prévoit l'article 24, § 1 : « *le responsable de traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement effectué est conforme au présent règlement* ». La sanction peut bien sûr également être prononcée à l'encontre d'un sous-traitant, ainsi qu'il résulte de l'article 28 du règlement. Il en va de même lorsque le responsable du traitement se trouve en dehors du territoire de l'Union européenne. Ce dernier doit alors obligatoirement désigner un représentant qui sera l'interlocuteur de l'autorité de contrôle compétente (art. 4, § 17 et 27, § 4). Le considérant 81 ajoute que le représentant peut faire l'objet de « *procédures coercitives* » dont le règlement ne donne aucune définition. Il semble que ce terme général inclue les procédures de sanctions.

En revanche, le règlement prévoit une immunité de sanction au profit des juridictions dans l'exercice de leurs fonctions juridictionnelles : les autorités de contrôle ne sont pas compétentes pour contrôler les opérations de traitement effectuées dans ce cadre (art. 55). Il y a donc lieu d'en déduire que le responsable d'un tel traitement échappe aux sanctions prévues par le règlement.

Aussi précises puissent-elles paraître, les dispositions du règlement présentent un caractère lacunaire qui suscite plusieurs difficultés.

S'agissant tout d'abord des organismes publics, ils ne sont susceptibles de faire l'objet d'une sanction pour violation du règlement que dans la mesure où le droit de l'État membre dont ils relèvent le prévoit expressément (art. 83, § 7).

La principale difficulté concerne le délégué à la protection des données[7]. En effet, le règlement ne prévoit aucune immunité à son égard ce dont il résulte qu'en cas d'inexécution des obligations qui pèsent sur lui, une sanction pourrait être prononcée. Il semblerait que l'article 83, relatif aux amendes administratives, consacre cette possibilité. Le doute provient, là encore, de la rédaction imprécise du texte qui énonce que peuvent faire l'objet d'amendes administratives « *les obligations incombant au responsable du traitement et au sous-traitant en vertu des articles [...] 25 à 39 [...]* ». Cette énumération inclut l'article 38 relatif à la fonction de délégué à la protection des données et l'article 39 consacré aux missions de ce même délégué. Et pourtant, l'article 83 précise bien que les amendes sont prononcées en cas de méconnaissance d'une obligation incombant au responsable du traitement. On a du mal à concevoir que la violation d'une disposition de l'article 39, relatif à la mission du délégué à la protection des données, puisse incomber au responsable du traitement. Par exemple, le paragraphe d de l'article 39 impose au délégué à la protection des données de coopérer avec l'autorité de contrôle. Il paraît naturel que le manquement à cette obligation puisse justifier une amende administrative à l'encontre du délégué ; on peine à y voir la méconnaissance d'une obligation incombant au responsable du traitement. Mais le G29, qui sera remplacé par le Comité européen à la protection des données, lequel dispose, on l'a vu, d'un pouvoir normatif très étendu, a d'ores et déjà précisé, dans des lignes directrices du 13 décembre 2016 consacrées au délégué à la protection des données, que ce dernier n'est pas personnellement responsable en cas de non-conformité au RGPD[8]. Compte tenu des dispositions précitées du règlement sur ce point, la légalité des lignes directrices exonérant le délégué à la protection des données de toute responsabilité est incertaine. C'est à la Cour de justice de l'Union européenne qu'il appartiendra de se prononcer.

Le doute existe également à l'égard des personnes qui, agissant, sous l'autorité du responsable du traitement, ont accès à des données à caractère personnel. L'article 29 du RGPD leur interdit formellement de traiter de telles données, sauf si elles ont reçu des instructions en ce sens du responsable du traitement ou si elles y sont tenues à un titre ou à un autre par le droit de l'Union ou la législation d'un État membre. Que se passera-t-il si une telle personne méconnaît une disposition du RGPD ? Aucune réponse ne se trouve dans le règlement. L'on pourrait donc en déduire que cette personne encourt une sanction du second groupe, c'est-à-dire l'une des plus graves.

Les manquements sanctionnés ayant été examinés, il convient maintenant d'analyser les dispositions du règlement relatives au prononcé des sanctions.

7. Voir X. Tracol, « Le règlement et la directive relatifs à la protection des données à caractère personnel », *Rev. Europe*, octobre 2016, p. 1 ; I. Gheorghe-Badescu, « Le nouveau règlement général sur la protection des données », *Rev. de l'Union européenne*, 2016, p. 466.

8. Ces lignes directrices, dont seule la version anglaise est en ligne, énoncent : « *DPOs are not personally responsible in case of non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions (Article 24(1)). Data protection compliance is a responsibility of the controller or the processor.* » (« *Les DPO ne sont pas personnellement responsables de la violation du présent règlement. Le RGPD indique clairement que c'est le responsable du traitement ou le sous-traitant qui doit vérifier et être en mesure de démontrer que le traitement est effectué conformément à ses dispositions. La conformité en matière de protection des données relève de la responsabilité du responsable du traitement ou du sous-traitant* »).

II. LE PRONONCÉ DE LA SANCTION

Les règles entourant la procédure de sanction (1.) seront examinées avant celles gouvernant le choix de la sanction (2.).

1. La procédure de sanction

Il convient de distinguer les règles de compétence, qui permettent de déterminer les titulaires du pouvoir de sanction (1.1.) et les garanties procédurales dont bénéficient les personnes susceptibles d'être sanctionnées (1.2.).

1.1. Les règles de compétence

C'est en principe l'autorité de contrôle nationale, la CNIL en France, qui dispose du pouvoir de sanction ainsi qu'il résulte des articles 55 et 83 du RGPD. L'autorité de contrôle est compétente pour sanctionner la violation du règlement sur le territoire de l'État membre dont elle relève, et à condition que cette violation soit afférente à un traitement de données qui ne soit pas transfrontalier. S'agissant des juridictions agissant dans l'exercice de leurs fonctions juridictionnelles, les autorités de contrôle sont incompétentes. Le règlement ne précise pas le régime des sanctions en pareille hypothèse. En revanche, l'autorité de contrôle est compétente à l'égard des autorités publiques ainsi qu'à tous les organismes privés en charge d'un traitement de données nécessaire à l'exécution d'une mission d'intérêt public.

Lorsque la violation du règlement concerne un traitement transfrontalier, les règles de compétence sont les mêmes à l'égard des autorités publiques (art. 55, § 2), mais elles varient en présence de personnes privées. En effet, la décision est alors prise par l'autorité compétente dite « chef de file », laquelle est en principe celle de l'État membre sur le territoire duquel le responsable du traitement a son principal établissement (art. 6, § 1). Dans ce cas, le projet de décision est soumis à l'ensemble des autorités de contrôle concernées par le traitement et, au terme d'une procédure complexe, la décision de sanction est prise par le chef de file (art. 60, § 7).

Lorsque l'une des autorités de contrôle manifeste son désaccord sur le projet de décision qu'envisage d'adopter le chef de file, doivent être mises en œuvre les procédures dites « *de contrôle de la cohérence* » (art. 63) et de « *règlement des litiges par le comité* » (art. 64) qui se caractérisent par une extrême complexité. La question de savoir quelle est l'autorité compétente pour édicter une sanction s'avère délicate. Il n'est pas nécessaire de reprendre le détail de ces procédures complexes ; il suffit de retenir que le projet de sanction émanant du chef de file est soumis au Comité européen de la protection des données, lequel émet alors un avis contraignant (articles 63 et 64). Ensuite, de deux choses l'une :
– soit le chef de file se conforme à l'avis du CEPD ; il adopte alors la décision ;
– soit il ne se conforme pas à cet avis. Le CEPD délibère donc de nouveau et adopte une décision contraignante (art. 65, § 1, pt a). Cet avis s'impose au chef de file qui adopte la décision finale et la notifie au responsable du traitement ainsi qu'à la personne concernée par le traitement de données.

En résumé, c'est toujours le chef de file qui prononce la sanction, sauf en cas de désaccord entre ce dernier et les autres autorités de contrôle, et plus particulièrement dans l'hypothèse où le CEPD adopte un avis contraignant. Il faut alors s'interroger sur l'identité de l'auteur de la sanction : celle-ci émane-t-elle du chef de file ou bien du CEPD qui, par un avis contraignant, impose sa décision au chef de file ? Le règlement ne répond pas à cette bien délicate question. Il convient toutefois d'observer que l'article 65, § 1 dispose que, dans ce cas, « *le Comité adopte une décision contraignante* ». Mais nous verrons qu'en pareille hypothèse, le recours doit être porté devant les juridictions nationales (v. infra, 2°).

Une seconde difficulté concerne les opérations menées conjointement par plusieurs autorités de contrôle. On recourt à ces opérations lorsque le responsable du traitement est établi dans plusieurs États membres mais aussi dans l'hypothèse où un traitement est susceptible d'affecter sensiblement un nombre important de personnes dans différents États membres. On retrouve ici les critères de qualification du traitement transfrontalier[9] si bien qu'il semble que ces opérations conjointes puissent être menées lorsqu'est en cause un traitement transfrontalier.

Les opérations conjointes peuvent aboutir à une prise de décision sans mettre en œuvre les procédures que l'on vient d'examiner. En effet, l'article 62 du règlement, relatif à ces opérations conjointes, dispose que des autorités de contrôle participant à une opération conjointe peuvent prendre « *des mesures répressives conjointes* » ce qui semble inclure les sanctions. D'ailleurs, le considérant 150 du règlement prévoit expressément qu'il peut être « *recouru aux mécanismes de contrôle de la cohérence pour favoriser une application cohérente des amendes administratives* ». Dans cette hypothèse, la sanction émanerait de l'ensemble des autorités de contrôle ayant participé à l'opération conjointe. Le règlement ne précise malheureusement pas les modalités de recours à l'encontre d'une telle décision.

1.2. Les garanties procédurales

Ces garanties existent tant avant le prononcé de la sanction qu'une fois celle-ci infligée.

S'agissant des garanties antérieures au prononcé de la sanction, le règlement rappelle à plusieurs reprises que nombre de mesures sont soumises aux garanties fondamentales. Les garanties fondamentales dont il est question ici sont celles garanties par le droit de l'Union européenne et plus particulièrement de la charte des droits fondamentaux, laquelle renvoie à la Convention de sauvegarde des libertés fondamentales et des droits de l'homme ainsi qu'à la jurisprudence de la Cour européenne des droits de l'homme. Il ne semble pas que les droits et libertés garantis par la Constitution française aient vocation à s'appliquer aux sanctions puisque celles-ci émanent du RGPD, c'est-à-dire d'une norme européenne. Parmi les mesures soumises au respect des garanties fondamentales, on peut citer les limitations temporaires ou définitives de traitement ainsi que des procédures d'enquête (consid. 129). La non-conformité d'une procédure d'enquête aux garanties fondamentales peut entraîner l'annulation de la sanction prononcée sur la base d'une telle enquête. C'est d'ailleurs le caractère irrégulier des visites domiciliaires menées par la CNIL qui

9. Voir la définition qui en est donnée à l'article 4, § 23.

avait conduit à l'annulation de la première sanction prononcée par cette autorité[10]. Les autorités de contrôle doivent bien évidemment respecter les garanties fondamentales lorsqu'elles prononcent une amende administrative ainsi que le rappelle le règlement, tant dans son considérant 148 qu'à l'article 83, § 8. Le considérant 129 indique d'ailleurs que les visites domiciliaires doivent être menées conformément aux exigences du droit procédural de chaque État membre, et notamment à l'obligation d'obtenir une autorisation judiciaire préalable.

Une fois la sanction prononcée, ce sont les recours à l'encontre de celle-ci qui garantissent les droits de la personne à l'encontre de laquelle une amende a été prononcée. Le règlement précise, mais ce rappel était inutile, que ces recours doivent eux aussi respecter les garanties fondamentales d'un procès équitable (art. 78). On a vu la difficulté qu'il pouvait y avoir à déterminer la juridiction auprès de laquelle le recours doit être formé, notamment lorsque la sanction a été prononcée conjointement par plusieurs autorités de contrôle.

S'agissant des décisions prises par le chef de file, conformément à une décision contraignante du Comité européen de la protection des données, le règlement précise que la décision de l'autorité de contrôle peut être contestée devant une juridiction nationale laquelle doit, en cas de doute sur la validité de la décision du CEPD, saisir la Cour de justice de l'Union européenne d'une question préjudicielle (consid. 143, al. 2). Le même texte rappelle, de manière superfétatoire, qu'une telle question préjudicielle n'est pas recevable si la contestation émane d'une personne qui aurait eu la possibilité de former un recours en annulation de la décision du CEPD devant la Cour de justice de l'Union européenne, par application de l'article 263 du TFUE. En effet, cette disposition du traité ouvre un recours en annulation d'un acte pris par une institution ou un organe de l'Union européenne à toute personne concernée directement et individuellement par la décision attaquée. Si celle-ci néglige d'exercer un tel recours dans le délai qui lui est imparti, elle ne pourra plus solliciter un renvoi préjudiciel à la Cour de justice de l'Union européenne.

2. Le choix de la sanction

L'article 83 du règlement distingue deux catégories de violations du règlement. La première regroupe celles assorties des amendes les moins lourdes. Leur montant peut atteindre 10 000 000 euros ou dans le cas d'une entreprise jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, l'autorité de contrôle devant retenir le plus élevé de ces deux montants. Les manquements de la seconde catégorie peuvent faire l'objet d'une amende administrative dont le montant peut s'élever à 20 000 000 euros ou, dans le cas d'une entreprise, 4 % du chiffre d'affaires annuel total de l'exercice précédent. Là encore, c'est le montant le plus élevé que doit retenir l'autorité de contrôle. Entrent dans la première de ces deux catégories certaines des obligations des responsables de traitement, des organismes chargés de la certification ou encore du suivi des codes. Le montant des amendes peut paraître très élevé, mais il ne faut pas perdre de vue qu'en cas de traitement transfrontalier, l'ensemble des autorités de contrôle nationales concernées participe à l'édiction d'une sanction unique pour tout le territoire de l'Union européenne.

L'article 83 répartit entre ces deux catégories les différents manquements susceptibles de sanction. En l'absence de critères préétablis, on peine à trouver la logique de cette répartition. Par exemple, l'obligation de communiquer clairement avec la personne concernée par un traitement de données est sanctionnée par une amende de la seconde catégorie tandis que l'obligation de communiquer à la même personne une violation des données personnelles n'est sanctionnée que par une amende de la première catégorie dont le montant est plus faible. Au-delà de ces incohérences, il semble que les amendes les plus sévères s'appliquent au respect des principes généraux telles que licéité du traitement, les obligations de transparence, de loyauté et de proportionnalité ainsi qu'aux obligations qui doivent être respectées pour recueillir de manière valable l'accord d'une personne pour que ses données personnelles fassent l'objet d'un traitement. Relèvent encore de cette catégorie les obligations afférentes au traitement des données personnelles sensibles ainsi que les obligations permettant le respect des droits de la personne concernée par un traitement. Il s'agit en réalité des obligations les plus importantes, caractéristiques du régime institué par le règlement. Par opposition, toutes les autres obligations sont sanctionnées par des amendes de première catégorie, c'est-à-dire de montants moins importants.

Une fois que l'autorité de contrôle a identifié que le manquement qu'elle cherche à sanctionner relève d'une catégorie ou d'une autre, il lui reste à déterminer le montant de l'amende puisque le règlement ne fixe que des plafonds. Pour cela, le règlement impose à l'autorité de contrôle de tenir compte des caractéristiques propres à chaque cas pour non seulement décider s'il y a lieu d'imposer une amende administrative mais également pour en fixer le montant. Le paragraphe 2 de l'article 83 énumère une liste des circonstances au regard desquelles l'autorité de contrôle doit se prononcer. Il s'agit notamment de la gravité du manquement, de son caractère délibéré ou non mais également du comportement de la personne sanctionnée ou encore de l'existence de précédentes violations du règlement, qui lui soient imputables. Doivent également être pris en compte le comportement de la personne sanctionnée à l'égard de l'autorité de contrôle et notamment son degré de coopération ainsi que la notification qu'elle aurait pu lui adresser de la violation du règlement. L'autorité de contrôle prend en compte l'application par la personne encourant la sanction des codes de conduite approuvés et des mécanismes de certification ainsi que de toute autre circonstance aggravante ou atténuante, tels que les avantages financiers obtenus ou les pertes évitées du fait de la violation du règlement.

Enfin, le règlement précise, dans son considérant 150, que l'autorité de contrôle doit tenir compte, pour prononcer une amende administrative à l'encontre d'une personne physique, du niveau général des revenus dans

10. CE, section du contentieux, 6 novembre 2009, *société Inter Confort*, n° 304300, *Recueil Lebon*.

l'État membre ainsi que de la situation économique de la personne en cause.

Ces règles, aussi précises soient-elles, soulèvent d'importantes difficultés.

En premier lieu, il existe un doute sur la détermination de l'entreprise dont le chiffre d'affaires doit être pris en compte. L'article 83 précise qu'il s'agit du chiffre d'affaires de l'entreprise, mais de quelle entreprise s'agit-il ? Certes, la notion d'entreprise est définie à l'article 4, § 18 : « *une personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris les sociétés de personnes ou les associations qui exercent régulièrement une activité économique* ». Et le considérant 150 renvoie aux articles 101 et 102 du traité sur le fonctionnement de l'Union européenne[11]. Mais ces indications laissent entière la question de savoir si, en cas de sous-traitance, c'est le chiffre d'affaires du sous-traitant ou celui du responsable du traitement qu'il convient de prendre en compte. De même, dans l'hypothèse où le délégué à la protection des données se verrait infliger une sanction administrative, et dans l'hypothèse où celui-ci est une entreprise, l'amende est-elle fixée en fonction du chiffre d'affaires de ce dernier ou bien de celui du responsable du traitement ? Le règlement reste muet sur ce point.

En second lieu, une difficulté surgit lorsqu'une personne est poursuivie pour plusieurs violations du règlement. Le règlement précise à cet égard que si ces violations se rapportent à la même opération de traitement ou à des opérations de traitement liées, le montant total de l'amende administrative ne peut pas excéder le montant fixé pour la violation la plus grave (art. 83, § 3).

Enfin, la difficulté la plus délicate concerne la pluralité de sanctions. Le règlement fait une distinction entre plusieurs mesures : les sanctions pénales, les amendes administratives, et aussi les « *mesures correctrices* » visées à l'article 58, § 2. En outre, le règlement se réfère parfois à des mesures atypiques telle l'exclusion d'un responsable du traitement de l'application d'un code de bonne conduite. Ces mesures peuvent-elles se cumuler ?

S'agissant tout d'abord des mesures correctrices, l'article 58 en donne la liste. Il s'agit des mesures qu'une autorité de contrôle peut prendre, tels que la délivrance d'un avertissement, d'un rappel à l'ordre, d'une mise en demeure d'avoir à se conformer au règlement, d'une injonction de respecter le règlement. Il peut également s'agir d'imposer une limitation temporaire ou définitive, voire même une interdiction du traitement. L'autorité de contrôle peut aussi retirer une certification.

Certaines de ces mesures constituent assurément des sanctions administratives. Il s'agit notamment de l'avertissement et du rappel à l'ordre. La limitation imposée à un traitement et son interdiction constituent sans doute des sanctions, de même que le retrait de la certification. Actuellement, notre droit positif qualifie expressément de sanction un avertissement ou une injonction de cesser un traitement[12]. Or le règlement dispose que l'autorité de contrôle peut imposer une amende administrative aux lieu et place de ces mesures correctrices (art. 58, § 2, pt i). Il prévoit également et surtout que les amendes administratives peuvent se cumuler avec ces mesures dites correctrices (art. 83, § 2). De manière plus générale, le règlement énonce que « *l'application d'une amende administrative ou le fait de donner un avertissement ne porte pas atteinte à l'exercice d'autres pouvoirs des autorités de contrôle ou à l'application d'autres sanctions en vertu du présent règlement* » (consid. 150). Ce cumul de sanctions de même nature, administrative, semble contraire au principe *ne bis in idem*. Le problème se pose avec plus d'acuité au sujet des sanctions pénales[13]. L'article 84 précise à cet égard que les États membres déterminent le régime des autres sanctions applicables en cas de violation de ces dispositions, « *en particulier pour les violations qui ne font pas l'objet des amendes administratives* ». L'expression « *en particulier* » implique que d'autres sanctions dont on ne peut exclure qu'elles soient pénales, peuvent être édictées pour des violations du règlement déjà sanctionnées par une amende administrative. Le considérant 149 du règlement précise toutefois que l'application cumulée des sanctions administratives et pénales ne doit pas conduire à la violation du principe *ne bis in idem* tel qu'interprété par la Cour de justice de l'Union européenne. On sait en effet que ce principe est garanti par la charte des droits fondamentaux (art. 50), laquelle se réfère à la Convention de sauvegarde des libertés fondamentales et des droits de l'homme ainsi qu'à la jurisprudence de la Cour européenne des droits de l'homme[14].

La question du cumul des sanctions se pose également à l'égard des mesures prises par les organismes chargés du suivi d'un code de bonne conduite. En effet, un tel organisme peut prendre « *des mesures appropriées* » en cas de violation du code par un responsable du traitement et notamment suspendre ou exclure ce dernier de l'application du code (art. 41, § 4). Il semble bien qu'il s'agisse là de véritables sanctions, dont l'article 41, § 4 précise qu'elles sont prononcées sans préjudice des amendes administratives infligées par l'autorité de contrôle.

Le règlement établit un régime de sanctions novateur qui n'offre pas une sécurité juridique suffisante. Le montant des amendes, d'une part, la complexité des nouvelles règles et leur imprécision, d'autre part suscitent à juste titre l'inquiétude des professionnels. Ceux-ci seront enclins à contester les sanctions qui pourraient leur être infligées, et ce d'autant plus que la légalité de certaines des dispositions du règlement est douteuse. Mais pour l'exercice de ces contentieux, il conviendra de faire preuve de vigilance, notamment en raison de la délicate articulation des recours de droit Internet et de droit de l'Union européenne. ■

11. Curieusement, ces deux articles du TFUE, qui énoncent des règles de concurrence, plus précisément l'interdiction des ententes et des abus de position dominante, ne donnent aucune définition de la notion d'entreprise. Sans doute faudra-t-il se référer à la jurisprudence de la CJUE rendue en application de ces textes.

12. Article 45 de la loi 78-17 du 6 janvier 1978, relatif à l'informatique, aux fichiers et aux libertés.

13. Dans le même sens, voir : E. Jouffin, X. Lemarteleur et M.-N. Gibon, « Le règlement sur la protection des données : les dix commandements à connaître pour passer de la théorie à la pratique », RDBF n° 4-2016, juillet-août, p. 11, n° 65.

14. En dernier lieu, sur l'application du principe « *ne bis in idem* », voir CEDH *A et B c/ Norvège*, n° 24130/11 et 29758/11, du 15 novembre 2016.