N° 385019
Société Orange

10ème et 9ème sous-sections réunies
Séance du 7 décembre 2015
Lecture du 30 décembre 2015

CONCLUSIONS

Mme Emilie BOKDAM-TOGNETTI, rapporteur public

La présente affaire vous confrontera, pour la première fois, aux conditions d'application de l'article 34 bis de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (dite « loi CNIL »), issu de l'ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques, qui impose aux fournisseurs de services de communications électroniques accessibles au public, en cas de violation de données à caractère personnel contenues par un traitement dont ils sont responsables, d'avertir sans délai la Commission nationale de l'informatique et des libertés (CNIL). Elle vous conduira, en particulier, à vous pencher sur son articulation avec le principe selon lequel nul n'est tenu de s'incriminer lui-même.

Au printemps 2014, le serveur informatique de la société XL Marketing, sous-traitant de la société Gutenberg Networks, prestataire de la société Orange chargé de réaliser des campagnes de marketing direct, a fait l'objet d'une attaque informatique, ayant permis l'accès illicite d'un tiers non autorisé à des fichiers contenant des données personnelles de 1,3 millions de clients ou prospects de la société Orange (nom, prénoms, date de naissance, adresse électronique, numéro de téléphone fixe ou mobile).

Après avoir pris des mesures techniques destinées à rétablir la sécurité de ses systèmes d'information, la société Orange a notifié à la CNIL, en application de l'article 34 bis de la loi du 6 janvier 1978, cette violation de données. Elle a également informé ses clients de cette fuite de données, laquelle a par ailleurs fait l'objet d'échos dans la presse.

Les 12 et 14 mai 2014, la CNIL a procédé, en application de deux décisions du 6 mai 2014 de sa présidente, à une mission de contrôle dans les locaux de la société Orange ainsi que ceux de son sous-traitant et de son prestataire secondaire. Au regard des éléments révélés par le contrôle sur les mesures de sécurité prises par la société Orange et ses sous-traitants, une procédure de sanction a été initiée par la présidente de la CNIL à l'égard de la société Orange, qui a abouti à l'adoption par la formation restreinte de la CNIL, le 7 août 2014, d'une délibération prononçant un avertissement à l'encontre de la société et décidant que cette sanction serait rendue publique. Cette décision a été notifiée et publiée sur le site internet de la Commission le 25 août suivant.

C'est la décision dont la société Orange vous demande aujourd'hui l'annulation.

Vous écarterez d'abord le moyen tiré de ce que la CNIL aurait pris cette décision au terme d'une procédure irrégulière au regard de l'article 77 du décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dès lors qu'il ne serait pas établi par ses visas et ses motifs que la formation restreinte a statué hors la présence du rapporteur et du commissaire du gouvernement. D'une part, aucun texte ni aucun principe n'impose de telles mentions dans la délibération et d'autre part, il ne résulte pas de l'instruction que le rapporteur et le commissaire du gouvernement auraient assisté au délibéré.

Le moyen suivant est tiré de ce que la CNIL a inexactement appliqué les articles 34 et 34 bis de la loi du 6 janvier 1978 et commis une erreur de droit en prononçant un avertissement à l'encontre de la société Orange, alors que celle-ci avait satisfait à l'obligation de notification de la violation de données à caractère personnel. La société estime que seul le fait de ne pas procéder à la notification imposée est susceptible de faire l'objet d'une sanction, et que dès lors que le fournisseur a satisfait à son obligation d'information, il ne peut plus être sanctionné pour la violation de données à caractère personnel divulguée.

La société feint en partie de confondre les articles 34 bis et 34 et d'ignorer l'article 45 de la loi CNIL. L'article 45 prévoit en effet que la formation restreinte de la CNIL peut prononcer un avertissement, ayant le caractère d'une sanction, à l'égard du responsable d'un traitement qui ne respecte pas les obligations découlant de la loi. Quant aux articles 34 et 34 bis, ils font peser deux obligations différentes sur le fournisseur : l'article 34 dispose que le responsable du traitement est tenu de « *prendre toutes précautions utiles (...) pour préserver la sécurité des données et, notamment, empêcher (...) que des tiers non autorisés y aient accès* », tandis que l'article 34 bis énonce une obligation propre aux responsables de traitements mis en œuvre dans le cadre de la fourniture au public de services de communications électroniques, distincte de celle de l'article 34, bien qu'elle puisse en apparaître sinon le corollaire, du moins un complément utile voire nécessaire : celle de notifier toute violation de données. Un responsable de traitement peut donc être sanctionné aussi bien pour non respect de son obligation de notification, s'il méconnaît l'article 34 bis, que pour manquement à son obligation de sécurité résultant de l'article 34, y compris lorsque cette méconnaissance de l'article 34 ne se double pas d'une violation de l'article 34 bis.

A l'appui de l'interprétation et de l'application de l'article 34 bis qu'elle appelle de ses vœux, la société invoque, d'une part, l'article 4 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002, dite « vie privée et communications électroniques », tel que modifié par la directive 2009/136/CE du 25 novembre 2009 pour la transposition de laquelle a été créé l'article 34 bis de la loi CNIL, en faisant valoir qu'il prévoit la possibilité de sanctionner le fournisseur qui a manqué à son obligation d'information sur l'existence d'une violation de données à caractère personnel, mais ne prévoit pas la faculté de prendre une sanction pour des faits ayant donné lieu à telle notification.

S'il est exact que l'article 4 n'évoque pas la faculté de sanctionner le fournisseur ayant manqué à ses obligations de sécurité, il ne saurait s'en inférer que la directive s'opposerait à une telle sanction. Au contraire, à côté de l'obligation de notification prévue par le 3 de l'article 4, ce même article fait peser sur le fournisseur d'autres obligations de sécurité. En particulier, son 1 bis prévoit que le fournisseur doit assurer la sécurité des données à caractère personnel qu'il détient et les protéger des accès illicites. Or l'article 15 bis, en cohérence avec le considérant 47 de la directive, prévoit que les États membres déterminent le régime des

sanctions applicables aux violations des dispositions nationales prises en application de la directive et prennent toute mesure nécessaire pour assurer la mise en œuvre de celles-ci, les sanctions ainsi prévues devant être effectives, proportionnées et dissuasives et pouvant être appliquée pour couvrir la durée de l'infraction, même si celle-ci a été ultérieurement corrigée. L'argumentation de la société, reposant sur une lecture tronquée de la directive, ne saurait donc prospérer sur ce premier terrain.

La société invoque, d'autre part, le principe selon lequel nul n'est tenu de contribuer à sa propre incrimination protégé par l'article 6 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (convention EDH) et par les articles 47 et 48 de la Charte des droits fondamentaux de l'Union européenne, en faisant valoir qu'interpréter les articles 34, 34 bis et 45 de la loi CNIL comme permettant de sanctionner un responsable de traitement pour des faits ayant donné lieu à notification méconnaîtrait ce principe. Le moyen d'erreur de droit sur la portée de l'article 34 bis de la loi nous paraît, à cet égard, devoir être regardé comme doublé d'un moyen tiré d'une méconnaissance en l'espèce par la CNIL du principe de non auto-incrimination.

Les articles 47 et 48 de la Charte des droits fondamentaux de l'UE nous paraissent invocables dans le présent litige, dès lors que la décision attaquée a été prise en application des dispositions des articles 34 et 34 bis de la loi CNIL, lesquelles transposent et mettent en œuvre le droit de l'Union (v. CE, 4 juillet 2012, *Confédération française pour la promotion sociale des aveugles et des amblyopes*, n° 341533, p. 261 ; CJUE, 26 septembre 2013, *IBV c/ Région wallonne*, aff. C-195/12 : application de la Charte à une mesure nationale prise dans le cadre établi par des directives européennes). Mais vous n'aurez pas à prendre expressément parti sur ce point, dès lors que le principe selon lequel nul n'est tenu de contribuer à sa propre incrimination est en tout état de cause invocable en l'espèce en tant qu'il est consacré par la convention EDH.

En effet, la formation restreinte de la CNIL, lorsqu'elle se prononce sur des agissements pouvant donner lieu à l'exercice de son pouvoir de sanction, doit être regardée comme décidant du bien-fondé d'accusations en matière pénale au sens de l'article 6 de la convention EDH (CE, 12 mars 2014, *Société Pages Jaunes Groupe*, n° 353193, aux Tables sur ce point). Or parmi les exigences qu'une telle qualification emporte figure, selon la jurisprudence de la Cour de Strasbourg, le respect du principe selon lequel nul ne doit être contraint de contribuer à sa propre incrimination (v. 25 février 1993, *F.... France*, n° 10588/83). Pour rechercher si une procédure a anéanti la substance même du droit de ne pas contribuer à sa propre incrimination, la Cour EDH examine la nature et le degré de la coercition, l'existence de garanties appropriées dans la procédure et l'utilisation qui est faite des éléments ainsi obtenus.

Ce principe importé d'un univers très éloigné de celui des sanctions édictées par des autorités administratives doit être manié avec précaution afin, tout en assurant son effectivité au stade du prononcé de sanctions relevant de l'article 6 §1, de ne pas désarmer et priver de leur nécessaire efficacité les procédures administratives de contrôle, souvent caractérisées par l'existence d'une obligation de coopération du contrôlé.

Nous ne croyons pas que ce principe soit méconnu lorsque la CNIL sanctionne pour manquement à son obligation de sécurité un opérateur qui a notifié une violation de données personnelles en application de l'article 34 bis de la loi du 6 janvier 1978.

Tout d'abord, il convient de noter que si la notification prévue par l'article 34 bis s'exerce bien sous la contrainte, non seulement de la loi CNIL, mais aussi de l'article 226-17-1 du code pénal, rendant passible de cinq ans d'emprisonnement et de 300 000 € d'amende le fait de ne pas y procéder, elle a lieu très en amont de la procédure « pénale », puisqu'elle se situe non seulement la procédure de sanction, mais aussi la procédure de contrôle, qui n'a été diligentée qu'ultérieurement, et que son objet n'est pas pénal.

Dans votre décision *Société Predica* du 30 mars 2007 (n° 277991, T. p. 693, concl. L…), vous avez jugé, après avoir relevé que l'engagement d'une procédure disciplinaire puis l'infliction d'une sanction n'était pas l'objet de la mission de surveillance et n'étaient qu'une possibilité ouverte, le cas échéant, à l'issue des contrôles diligentés, que le principe de non auto-incrimination était inopérant au stade du contrôle devant la commission de contrôle des assurances, des mutuelles et des institutions de prévoyance.

Toutefois, dès lors que ce principe impose à l'accusation de fonder son argumentation sans recourir à des éléments de preuve obtenus par la contrainte ou la pression au mépris de la volonté de l'accusé, et qu'il s'intéresse donc à tout ce qui affecte le recueil des preuves utilisées dans le cadre d'une procédure pénale, vous ne pouvez ici vous borner à ce constat et devez rechercher si, en l'espèce, il a été fait dans le cadre de la procédure de sanction dont la société a fait l'objet une utilisation de la notification constitutive d'une méconnaissance de ce principe (v., sur ce point, l'arrêt de grande chambre *Saunders c/ Royaume-Uni* de la Cour EDH du 17 décembre 1996, n° 19187/91, qui portait sur l'utilisation faite pour un procès pénal d'informations obtenues sous la contrainte dans le cadre d'une enquête administrative conduite en application de la loi sur les sociétés).

Or à cet égard, la sanction prononcée en vertu de l'article 45 de la loi pour manquement aux obligations résultant de l'article 34 de celle-ci ne nous paraît pas reposer sur la notification prévue à l'article 34 bis ni concerner les mêmes éléments de fait. D'une part, les dispositions de l'article 34 bis n'ont ni pour objet ni pour effet d'obliger le fournisseur à faire état des éventuels manquements lui étant imputables qui seraient à l'origine d'une telle violation ou l'auraient favorisée. D'autre part, il peut y avoir eu violation de données personnelle au sens de l'article 34 bis sans qu'il puisse être reproché au responsable du traitement de manquement aux obligations qui lui incombent en vertu de l'article 34. Rappelons en effet que la loi ne fait pas peser, à son article 34, d'obligation de résultat sur le responsable du traitement, mais seulement une obligation de moyen : il doit avoir pris « toutes précautions utiles ». Ce qui motive la sanction n'est pas l'existence de la violation elle-même, ayant fait l'objet de la notification, mais les manquements en matière de sécurité révélés par la mission de contrôle diligentée par la suite, qui ont pu, le cas échéant, rendre possible cette violation. Dès lors, s'il est indéniable que la connaissance par la CNIL, grâce à cette notification, de l'existence d'une violation de données personnelles peut, en fait, motiver la réalisation d'un contrôle, un tel contrôle ne préjuge nullement de la découverte de manquements du responsable du traitement et, moins encore, de la mise en œuvre ultérieure par la CNIL de ses pouvoirs de sanction.

Au demeurant, qu'il s'agisse du contenu de la notification prévue par l'article 34 bis ou des constats de manquements à l'obligation de moyens posée par l'article 34 en matière de sécurité relevés lors d'un contrôle administratif ultérieur et pouvant donner, le cas échéant, lieu à sanction, ne sont en cause que des éléments de fait, objectifs, à l'exclusion de tout élément subjectif d'intentionnalité ou relatifs au for intérieur d'une personne. Il nous semble que nous nous situons donc dans un univers assez différent de celui qui constitue le cœur du

principe selon lequel nul n'est tenu de s'incriminer soi-même, lequel a notamment pour finalité d'éviter, par l'exercice de pressions pour l'obtention de preuve, les erreurs judiciaires (Cour EDH, Grande Chambre, 29 juin 2007, *O… et E… c/ Royaume-Uni*, n° 15809/02 et 25624/02). A cet égard, il n'est pas inintéressant de noter que, dans son arrêt *Saunders* déjà mentionné, la Cour de Strasbourg a souligné que le droit de ne pas s'incriminer soi-même « *ne s'étend pas à l'usage, dans une procédure pénale, de données que l'on peut obtenir de l'accusé en recourant à des pouvoirs coercitifs mais qui existent indépendamment de la volonté du suspect, par exemple les documents recueillis en vertu d'un mandat* ».

Dans ces conditions, vous écarterez le moyen.

Le moyen suivant est tiré de ce que la formation restreinte de la CNIL aurait commis une erreur de qualification juridique – moyen qui nous semble devoir être reformulé sur le terrain de l'erreur d'appréciation – en considérant que la société a manqué à son obligation d'assurer la sécurité et la confidentialité des données personnelles de ses clients.

L'obligation de prendre toutes les mesures nécessaires à la sauvegarde de la sécurité des données personnelles qui lui sont confiées pesant, en vertu de l'article 34 de la loi CNIL, sur la personne en charge du traitement de données à caractère personnel n'est, comme on l'a dit, qu'une obligation de moyen. Elle nous paraît devoir s'apprécier au regard notamment de l'état de l'art, de la sensibilité des données en cause, des risques présentés par le traitement et du coût des mesures en cause (v. sur ce point l'article 17 de la directive 95/46/CE du 24 octobre 1995).

Pour conclure à l'existence d'un manquement, la délibération relève notamment que la société Orange « *n'a pas fait réaliser d'audit de sécurité sur la version de l'application technique spécifiquement développée par son prestataire secondaire pour répondre à ses besoins, qu'elle communiquait de manière non sécurisée les mises à jour de ses fichiers clients à ses prestataire et qu'aucune clause de sécurité et de confidentialité des données n'était imposée à son prestataire secondaire* » et en déduit que « *les mesures mises en œuvre en termes de sécurité des données par la société (…) étaient insuffisantes et ont contribué à la réalisation du risque que constitue la récupération, par un tiers malveillant, des données des clients* ».

Pour contester cette appréciation selon laquelle elle a manqué à son obligation d'assurer la sécurité des données personnelles de ses clients, la société Orange fait notamment valoir, d'une part, qu'elle avait, dans le contexte d'une chaîne de sous-traitance qui était celui de l'espèce, pris toutes les mesures utiles à la bonne conservation des données à caractère personnel, et, d'autre part, que le traitement confié au sous-traitant ne portait que sur des clients ayant donné leur accord à une sollicitation commerciale et que les données ne se rapportaient qu'aux noms et prénoms des intéressés et, dans certains cas, leur adresse électronique, numéro de téléphone et date de naissance, et non sur des données telles que des numéros bancaires.

Toutefois, sur le premier point, vous avez jugé qu'il résultait des dispositions de l'article 35 de la loi du 6 janvier 1978 que la circonstance que des opérations de traitement de données soient confiées à des sous-traitants ne décharge pas le responsable de traitement de la responsabilité qui lui incombe de préserver la sécurité des données, sans que soit méconnu le principe constitutionnel de responsabilité personnelle, dès lors que ces sous-traitants doivent être regardés comme agissant, ainsi que le prévoient ces dispositions, sur son instruction (CE,

11 mars 2015, *Société Total raffinage marketing et autre*, n° 368748, aux Tables sur un autre point).

Dès lors, la seule insertion dans le contrat la liant à la société Gutenberg de clauses imposant à cette société et à ses sous-traitants de prendre « *toutes mesures* » permettant d'éviter un détournement ou une utilisation frauduleuse des données, et de garantir leur intégrité, ou encore stipulant, de manière générale, que Gutenberg se « *porte fort envers Orange du respect de l'obligation de protection des données décrites [au contrat] par son personnel et ses sous-traitants* », ne dispensait pas la société Orange de prendre des mesures destinées à s'assurer elle-même que la sécurité des données était préservée et ne permettait pas, à elle seule, de la regarder comme ayant pris toutes mesures utiles au respect des obligations qui lui incombent en application de l'article 34 de la loi.

Quant au second point, relatif à la « minimisation » des données, il ne saurait conduire à écarter l'existence d'un manquement à l'obligation de la société de protéger les données personnelles de ces clients, dès lors que les données en cause étaient bien des données identifiantes et qu'elles concernaient plus d'un million de personnes.

Enfin, le dernier moyen est tiré de ce que la CNIL aurait pris une sanction disproportionnée aux manquements reprochés et aux circonstances de l'espèce en infligeant à la société un avertissement et en décidant sa publication.

Vous exercez un plein contrôle sur la sanction infligée par la formation restreinte à un responsable de traitement en application de l'article 45 de la loi CNIL (v. CE, 12 mars 2014, *Société Pages jaunes et autres*, n° 353193, aux Tables sur un autre point).

Au regard de ce que nous venons de vous exposer, nous ne pensons pas que la CNIL ait commis une erreur d'appréciation en prononçant un avertissement à l'encontre de la société Orange, alors même que celle-ci a réagi rapidement à la suite de la violation de données personnelles pour prendre des mesures correctrices et qu'il n'apparaît pas que la violation de données en cause ait ultérieurement causé des dommages matériels, tels que des attaques dites de « hameçonnage », aux personnes dont les données ont ainsi été violées.

La sanction complémentaire de publication (v. par ex., sur la nature d'une telle mesure : CE, 12 mars 2014, *Société Foncia Groupe*, n° 354629, aux Tables sur un autre point) ne nous paraît pas davantage disproportionnée, eu égard à la nature des violations constatées et aux moyens humains et financiers dont disposait la société Orange pour les prévenir. Au demeurant, il nous semble que l'image d'Orange a probablement au moins autant souffert de la publicité donnée, en amont, à l'attaque informatique et à la violation de données personnelles en cause, dont la presse s'est largement fait l'écho, que de la publication en aval de l'avertissement qui lui a été infligé par la CNIL.

Quant à l'allégation d'erreurs dans le contenu du communiqué de presse de la CNIL, la société n'en tire en tout état de cause, à strictement parler, aucun véritable moyen.

Par ces motifs, nous concluons au rejet de la requête.