L'extinction du contrat et le sort des données personnelles

Emmanuel Netter, MCF HDR à l'Université d'Avignon, LBNC (EA3788)

Le sujet qui nous a été confié supporte deux interprétations différentes. Dans le sens de lecture qui est celui de la langue française, il dévoile d'abord « l'extinction du contrat », et ensuite seulement « le sort des données personnelles ». Il faudrait alors s'intéresser à la question de savoir, une convention ayant disparu, ce qu'il convient de faire des traitements de données à caractère personnel dont elle constituait le soubassement nécessaire. Lire le sujet de droite à gauche, en revanche, c'est renverser la chronologie ; c'est intervertir la cause et la conséquence : cette fois-ci, la (mauvaise) gestion des données constitue la raison pour laquelle le contrat a pris fin.

Il y a certes de l'artifice à traiter, dans une seule contribution, de deux questions qui sont intellectuellement bien distinctes. Mais il y aurait de la paresse à en écarter une, alors qu'elles sont d'une égale richesse en difficultés théoriques et pratiques. Aussi envisagerons-nous le sort réservé aux données comme cause d'extinction du contrat (I), puis le sort à réserver aux données comme conséquence de l'extinction du contrat (II). Précisons que le seul contrat qui sera envisagé ici sera celui qui unit le responsable de traitement à la personne dont émanent les données, dans la mesure où des contributions spécifiques sont consacrées aux contrats entre co-responsables de traitement d'une part, et aux contrats entre responsables de traitement et sous-traitants d'autre part.

I - Le sort réservé aux données comme cause d'extinction du contrat

Lorsqu'un responsable de traitement adopte un comportement blâmable à l'égard des données personnelles qu'il manipule, on songe aussitôt à lui imputer une violation du RGPD. Mais dans certains cas, le même comportement constituera également la violation d'un contrat passé avec la personne concernée, par exemple sous la forme d'une politique de confidentialité. Deux analyses sont alors possibles. On peut considérer que ce qui est avant tout violé, c'est une norme générale et impersonnelle, une norme légale au sens large – qu'il s'agisse du RGPD, de la loi informatique et libertés ou d'un décret -, ce qui plaiderait en faveur de la responsabilité civile délictuelle[1]. Ou bien on peut, considérant que les prévisions des parties ont été déjouées, appliquer les remèdes à l'inexécution du contrat. De là découleront des différences de régime juridique bien connues : faut-il mettre en demeure le responsable de traitement, peut-on demander l'exécution forcée de la convention, soulever une exception d'inexécution, obtenir réparation du préjudice même non prévisible lors de la conclusion du contrat, invoquer les dispositifs de lutte contre les clauses

1 En ce sens, V. A. Danis-Fatome, « Quelles actions judiciaires en cas de violation du RGPD ? », CCE, avril 2018, dossier 18, note 23 : « Dans l'hypothèse où un contrat unissant la personne concernée et le responsable de traitement constitue le fondement du traitement, les obligations qui incombent à ce dernier pourraient avoir une nature contractuelle et leur violation déboucher sur une responsabilité de cette nature. Il faut cependant rappeler que les obligations contractuelles n'ont pas en principe pour vocation d'imposer des règles de conduites (V. G. Viney, P. Jourdain et S. Carval, ouvrage préc. note n° 10, n° 168-1). Les obligations contenues dans le RGPD garderont donc dans ce cas une nature légale et déboucheront donc sur une responsabilité délictuelle ».

abusives...[2] ? Nous tenterons d'analyser la nature, contractuelle ou extra-contractuelle, des manquements imputables au responsable de traitement (A) avant d'en tirer des conséquences s'agissant des sanctions applicables (B).

A - Les manquements

Partons d'hypothèses simples : une personne souhaite faire fonctionner un compte de réseau social, se faire livrer par un e-commerçant à son domicile, confier à son employeur des informations dans le cadre de leur relation de travail. Ici, un contrat unit la personne concernée au responsable de traitement, et sa bonne exécution rend nécessaire la manipulation de données personnelles. Les devoirs qui pèsent sur le responsable de traitement en vertu du RGPD ont-ils de surcroît une nature contractuelle ?

1- Identifier les obligations contractuelles

Dans certains cas, la réponse paraît nettement positive : lorsque le responsable de traitement décrit la finalité du traitement, le type de données collectées, les durées de conservation, les destinataires des données, le fait qu'elles circulent ou non hors de l'Union européenne. En vertu des obligations de transparence (art. 12 s. RGPD), ces points ont nécessairement figuré dans la convention. Ils ne constituent pas une simple reprise à l'identique de normes légales, mais appliquent au contraire des exigences abstraites au cas concret, leur donnant vie : les donnée sont-elles conservées un mois, six mois, un an ? Le règlement n'apporte pas la réponse, mais oblige le contrat à en fournir une[3].

L'analyse est très différente si l'on considère l'ordre que donne le RGPD au responsable de nommer un délégué à la protection des données, de tenir un registre des traitements, de mener une analyse d'impact. Ces devoirs seront rarement repris par le contrat. Le seraient-ils, la convention des parties ne ferait qu'en rappeler l'existence sans les préciser ni rien y ajouter. Enfin, on peut difficilement considérer que ces devoirs sont édictés dans l'intérêt individuel de chacune des personnes concernées par le traitement prise isolément. Pour toutes ces raisons, il semble difficile d'y voir de véritables créances contractuelles.

Entre ces deux séries de cas faciles à classer, se rencontre une zone plus grise. L'obligation faite au responsable de traitement de mettre en œuvre des moyens adéquats pour assurer la sécurité du traitement en fait sans doute partie. Quand bien même elle ne serait pas stipulée expressément, le juge pourrait facilement la « découvrir » au sein du contrat sur la base de l'article 1194 du Code civil. Chacune des personnes concernées par le traitement peut facilement justifier qu'elle a un intérêt personnel, clair et direct à la bonne exécution de cette obligation. Mais la qualification contractuelle est-elle dans son intérêt ? Peut-être, si elle souhaite arguer d'un défaut dans l'organisation de la sécurité pour soulever une exception d'inexécution et cesser ainsi des paiements. Sans doute pas, si elle agit en responsabilité civile et veut obtenir une réparation du

2 Pour l'application des règles du Code de la consommation relative aux clauses abusives à des clauses relatives à des traitements de données personnelles, V. TGI Paris, 12 février 2019, UFC Que Choisir c. / Google.

3 Le raisonnement pourrait être plus subtil encore. Supposons que la politique de confidentialité ait retenu une durée de conservation des donnéesd'un an, alors que la CNIL estime qu'en pareille situation, elle ne doit pas dépasser six mois. Conserver les données plus d'un an, c'est violer le contrat. Conserver les données huit mois, c'est bien exécuter la convention mais, potentiellement, violer le RGPD, et par conséquent commettre une faute délictuelle.

préjudice même imprévisible – songeons aux victimes de la faille de sécurité du réseau d'infidélité conjugale « Ashley Madison », dont certaines se seraient suicidées[4].

2 - Identifier les contrats

Il était déjà difficile de raisonner à partir du cas le plus simple : celui d'un traitement de données personnelles fondé sur sa « nécessité pour l'exécution d'un contrat ». Supposons à présent qu'il existe toujours un contrat de base, mais que le traitement envisagé ne soit pas nécessaire à son exécution : c'est Google qui propose à l'internaute d'afficher de la publicité ciblée, ou bien l'e-commerçant qui lui suggère d'enregistrer ses données de carte bancaire pour un futur achat. Dans ce cas, le fondement de licéité proposé par le RGPD est « le consentement pour une ou plusieurs finalités spécifiques » (art. 6, a). Ce traitement, facultatif et détachable du contrat principal, sera néanmoins décrit dans une politique de confidentialité au titre des obligations de transparence. Le document obligera implicitement le responsable à respecter les finalités, durées de conservation… qui y sont décrites. N'est-ce pas une forme de pollicitation ? Le consentement spécial envisagé par le RGPD n'est-il pas alors une acceptation ? La réponse nous semble positive, et le fruit de la rencontre des volontés s'annexe alors au contrat de base – il peut en être expurgé si le consentement à la finalité spécifique est repris, ce que l'on doit pouvoir faire sans conséquence, en principe, pour le contrat sous-jacent (art. 7,4).

Un raisonnement analogue peut être proposé lorsque le traitement repose sur la base d'un consentement spécial, en l'absence même d'un contrat de base : une commune recueille les adresses email des habitants volontaires pour les tenir informés de l'avancement de travaux ; une école propose aux élèves qui le souhaitent d'avoir leur photo dans une revue scolaire. La proposition de traitement une fois acceptée forme un contrat – qui ne s'annexe pas, ici, à une convention préexistante. Cela permet à nouveau d'adresser certaines reproches au responsable de traitement sur le terrain des remèdes à l'inexécution du contrat.

Enfin, même hors de ces deux fondements de licéité (la nécessité pour l'exécution du contrat de base et le consentement spécifique), il peut arriver que le traitement intervienne, pour ainsi dire, dans la sphère d'influence d'un contrat préexistant. Imaginons qu'un GAFA prétende traiter des informations relatives à un utilisateur sur le fondement de son « intérêt légitime » (6, f) car elles permettent d'améliorer la sécurité du service, mais qu'il les revende en réalité à un tiers à des fins de marketing ciblé. Ou bien qu'un employeur traite les taux de prélèvement à la source de ses salariés pour répondre à une obligation légale (art. 6, c), mais en profite pour les classer en fonction de la richesse supposée de leurs foyers et en tirer des conséquences s'agissant des primes à leur verser. De ces deux détournements de finalité, il semblerait logique qu'on puisse tirer des conséquences dans le cadre, pour le premier, du contrat de service en ligne, pour le second, du contrat de travail, en tant qu'ils constituent de graves déloyautés.

Ainsi, dans bien des hypothèses, les manquements d'un responsable de traitement sont susceptibles d'être considérés à travers un prisme contractuel.

4 M. Untersinger, « Suicides, démission, chantage : les conséquences tragiques du piratage du site de rencontres Ashley Madison », article lemonde.fr du 10 décembre 2015.

B - Les sanctions

Si l'on arrive, en suivant les méthodes qui viennent d'être énoncées, à identifier de véritables manquements contractuels de la part du responsable de traitement, l'ensemble des remèdes habituels à l'inexécution du contrat peut théoriquement être mobilisé. En particulier, la résiliation judiciaire du contrat, la responsabilité civile contractuelle ou une combinaison des deux pourront être demandées.

Une question plus incongrue est celle de savoir si un manquement au RGPD peut simultanément constituer une cause de nullité justifiant l'anéantissement rétroactif de la convention. Observons ici que les grilles de lecture du droit des données et du droit civil ne se recoupent pas. Ainsi, la délibération de la CNIL du 21 janvier 2019 dans l'affaire Android affirme que la politique de confidentialité de Google n'était pas compréhensible par les utilisateurs ordinaires, et de surcroît que le consentement au traitement n'a pas été donné par un acte positif clair[5]. Pris au pied de la lettre par le civiliste, ce raisonnement devrait signifier qu'il n'y a pas eu de véritable rencontre des volontés et que, par conséquent, l'apparence de contrat peut être anéantie par la voie d'une action en nullité. Toutefois, la CNIL conduit un raisonnement abstrait, à l'échelle de l'ensemble des utilisateurs, là où le juge civil amené à se prononcer sur un vice du consentement devrait opérer un contrôle concret individu par individu. De surcroît, le droit civil ne nous semble pas disposer d'instruments permettant un examen aussi exigeant et pragmatique, d'une part de la clarté de l'offre, d'autre part de la netteté de l'acceptation, que celui mené par l'autorité administrative indépendante sur la base du RGPD.

II - Le sort à réserver aux données comme conséquence de l'extinction du contrat

Nous postulerons ici qu'un contrat a pris fin. Cela peut être en raison du comportement d'une partie, par simple arrivée du terme, par le jeu d'une condition ; l'anéantissement peut être rétroactif ou non. Le contrat va quoiqu'il en soit emporter dans sa chute un certain nombre de traitements de données dont il était le nécessaire support. La pente naturelle du RGPD est alors à ordonner ou à permettre la suppression des informations concernées (A). Il ne s'agit cependant que d'un principe, qui doit souffrir d'utiles exceptions : il est des données qui méritent de survivre au contrat qui les as vu naître (B).

A – Le principe : la suppression des données

C'est l'un des principes essentiels du RGPD : les données doivent être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées » (art. 5, e). Lorsque la disparition d'un contrat entraîne la disparition des finalités de traitement, le responsable du traitement devrait donc en tirer spontanément les conséquences et, en principe, supprimer les informations. L'alternative serait de les anonymiser, ce qui suppose d'empêcher définitivement toute ré-identification des personnes concernées, mais cela se révèle souvent très difficile, et parfois

5 Délibaration SAN-001 du 21 janvier 2019.

impossible. A supposer que cette suppression spontanée par le responsable de traitement n'ait pas été effectuée, elle pourrait avoir lieu à l'initiative de la personne concernée, sur le fondement du droit à l'effacement (art. 17). Si le contrat a été anéanti sans rétroactivité, on mobilisera le a) : « les données à caractère personnel ne sont plus nécessaires au regard des finalités (...) ». S'il a été anéanti rétroactivement, on doit considérer que le traitement qui était fondé sur ce contrat était, dès l'origine, illicite, ce qui renvoie au d).

Ces principes ayant été rappelés, constatons que leur mise en œuvre n'est pas sans poser, parfois, de considérables difficultés. Relevons au préalable que, si l'on exige du responsable de traitement qu'il démontre avoir effacé les données, il lui faudra prouver un fait négatif – qu'il ne subsiste de copies nulle part -, ce qui est à peu près impossible.

L'étendue de l'effacement peut constituer une première difficulté. Imaginons un utilisateur de réseau social qui clôture son compte : le contrat qui fondait le traitement prend fin. La plateforme doit-elle effacer les conversations dans lesquelles il n'était que l'un des interlocuteurs, au risque de porter atteinte aux données des autres ? Ou faut-il caviarder les lignes correspondant à ses interventions ?

Le moment précis auquel l'effacement doit intervenir constitue une deuxième difficulté, considérable. Lorsqu'un avocat, dans une relation de conseil, a des contacts épisodiques avec un client, quand considère-t-on que la prestation prend fin[6] ? La solution consiste, au bout de 12 mois sans événement nouveau, à sortir le dossier de la « base active » accessible aux avocats du cabinet, et à le placer en archive, d'où il ne pourra être ressorti que par l'archiviste, sur présentation d'un motif suffisant. L'archivage restreint ainsi drastiquement les personnes susceptibles d'accéder aux informations, et réduit d'autant les risques pour la vie privée des personnes concernées. L'intérêt est double : pouvoir ressortir le dossier si la relation client reprend vie, mais aussi, bien sûr, conserver la preuve des conseils prodigués en cas de contentieux. Cependant, l'archivage pose lui-même des problèmes redoutables. Un avocat et DPO affirme que, selon la CNIL, il ne faudrait conserver que les données potentiellement utiles dans le cadre d'un contentieux, exercice de tri hautement spéculatif à supposer qu'il soit possible[7]. Le même rappelle qu'en droit civil, certains délais de prescription ont des points de départ glissants avec un délai butoir situé 20 ans après la naissance du droit (art. 2232 du Code civil), ce qui pourrait retarder la suppression des données archivées fort longtemps après la fin du contrat.

On l'aperçoit d'ores et déjà avec la question des archives intermédiaires : l'application du RGPD n'est pas incompatible avec certaines hypothèses de conservation des données bien au-delà de l'extinction du contrat. Développons cette question pour terminer.

B – Les tempéraments : la conservation des données

Certains droits à conserver les données au-delà de la disparition du contrat sont reconnus, tantôt au bénéfice du responsable de traitement, tantôt au bénéfice de la personne concernée.

6 Un problème proche est posé par les comptes d'utilisateurs de services en ligne qui restent longtemps inactifs sans être pour autant clôturés. La politique de confidentialité devrait prévoir qu'après une durée d'inactivité déterminée, les données sont supprimées.

7 Entretien avec Me Lorette Dubois en date du 20 mars 2019.

1 – Au bénéfice des responsables de traitement

Au bénéfice des responsables de traitement, le RGPD prévoit certaines dérogations au droit à l'effacement. L'hypothèse d'un traitement restant nécessaire « à la constatation, à l'exercice ou à la défense de droits en justice » est expressément prévue (art. 17, e). Peut également perdurer le traitement « à des fins statistiques » (d). La question qui se pose ici est celle de la mémoire à long terme des organisations. Pour leurs services d'actuariat, les assureurs doivent conserver durablement la trace du dénouement des garanties délivrées, associée au profil du risque. Il s'agit bien ici de « statistiques », et il est même parfois possible d'anonymiser les jeux de données, ce qui les fait échapper au champ d'application du règlement. En revanche, imaginons un cabinet d'avocats pénalistes souhaitant conserver le souvenir des défenses assurées aux assises : certains dossiers sont quasiment impossibles à séparer de manière irréversible de l'identité du client défendu, et il ne s'agit pas à proprement parler de « statistiques ». La solution réside peut-être ailleurs. Le RGPD admet parfois qu'un nouveau traitement soit effectué sur des données dont on est déjà en possession, à condition que la finalité nouvelle soit « compatible » avec la finalité initiale (art. 6,4). Le texte se fait alors volontairement abstrait, pour gagner en souplesse, et mobilise des critères flous : « l'existence éventuelle d'un lien entre les finalités » initiales et les finalités nouvelles, le « contexte dans lequel les données à caractère personnel ont été collectées », les « conséquences possibles » du traitement ultérieur pour les personnes concernées, ou l'existence de « garanties appropriées ». L'inévitable contrepartie de cette souplesse, c'est la faiblesse de la sécurité juridique procurée, et le risque de divergences d'interprétation entre autorités de contrôle et responsables de traitement.

2 – Au bénéfice de la personne concernée

Il arrive enfin que la destruction pure et simple des données soit évitée, cette fois-ci au bénéfice de la personne concernée, qui souhaite en disposer comme bon lui semble.

Elle peut en disposer pour elle-même. Elle pourra en particulier exercer son droit à la portabilité (art. 20 RGPD), si elle ne souhaite pas seulement connaître la teneur des informations qui étaient aux mains du responsable de traitement – à cette fin, le droit d'accès est suffisant – mais plutôt réinjecter ces données quelque part – le droit à la portabilité garantissant ici de les recevoir dans un format lisible et exploitable par les machines. Il peut s'agir de les remettre à un nouveau responsable de traitement concurrent du précédent – un autre fournisseur d'emails, un autre gestionnaire de photographies en ligne – mais aussi d'exploiter soi-même les données. En effet, théoriquement, le droit à la portabilité pourrait être exercé à l'encontre d'un supermarché par un client qui souhaiterait procéder à des analyses statistiques sur sa consommation mensuelle de produits gras, telle que révélée par ses données de « carte de fidélité ».

La personne concernée peut enfin disposer des données à l'attention de ceux qui lui survivront. La solution ne découle pas du RGPD, mais des choix propres à la législation française[8]. Il est prévu que la personne puisse laisser des directives générales ou spéciales s'agissant du sort à réserver à ses données. Une telle solution est à l'abri de la critique. En revanche, en l'absence de directives, « les héritiers de la personne concernée » peuvent accéder aux données dans la mesure nécessaire « A

8 Art. 85 de la loi n° 78-17 informatique et libertés

l'organisation et au règlement de la succession du défunt »[9]. La mort de la personne concernée a pu mettre fin au contrat qui constituait le soubassement du traitement : la finalité ayant disparu, nous avons vu que le responsable de ce traitement devrait théoriquement supprimer les informations qu'il exploitait dans ce cadre. Et pourtant, il doit se préparer à ce que des héritiers se manifestent, des mois plus tard, et demandent à accéder aux informations pour le bon règlement de la succession. Voilà qui pose de nombreuses questions. Il semblerait excessif de leur donner accès à tout et de les laisser opérer un tri eux-mêmes. Faut-il qu'ils décrivent par avance, même approximativement, ce qu'ils cherchent[10] ? Si oui, faut-il restreindre leur accès aux données à une période de temps ou à des mots-clés en rapport avec cette requête ? Qui, au cours de ces opérations, doit tempérer les appétits d'information des héritiers : le notaire chargé de la succession, le responsable de traitement lui-même ? Il appartiendra à la pratique et aux familles endeuillées, avec le secours du juge, de faire émerger les solutions concrètes dont le législateur s'est manifestement désintéressé.

9 Art. 85, II, 1°.

10 Le texte ne semble pas en ce sens, qui se poursuit ainsi : « A ce titre, les héritiers peuvent accéder aux traitements de données à caractère personnel qui le concernent afin d'identifier et d'obtenir communication des informations utiles à la liquidation et au partage de la succession ». Mais il est si mal rédigé qu'il supportera les interprétations que la Cour de cassation voudra en faire. Relevons au passage que l'accès « dans la mesure nécessaire » au règlement de la succession cède la place, à la phrase suivante, aux informations simplement « utiles » à la liquidation et au partage, ce qui est tout à fait différent.