



ASSEMBLÉE NATIONALE

15ème législature

Traitement et utilisation des données personnelles par les créanciers

Question écrite n° 34489

Texte de la question

Mme Danièle Obono alerte M. le secrétaire d'État auprès des ministres de l'économie, des finances et de la relance, et de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques, sur l'entrave que posent le traitement et l'utilisation des données personnelles par les créanciers (et notamment les banques) pour la protection suffisante du droit matériel au respect à la vie privée et des droits processuels d'égalité des armes et de procès équitables, droits protégés dans le système juridique interne et au niveau supranational. Le Règlement général sur la protection des données personnelles (RGPD) du 27 avril 2016 a pour objectif une meilleure protection par un meilleur contrôle des individus du traitement et de l'utilisation de leurs données personnelles, en cohérence avec les droits garantis dans la Charte des droits fondamentaux de l'Union européenne. Ainsi au paragraphe 39 des considérants du RGPD est soulignée l'obligation de licéité et de loyauté pesant sur les responsables de traitement et leurs sous-traitants. De plus, l'article 226-16 du code pénal renforce ce principe de licéité dans le traitement des données personnelles avec une obligation de résultat, précisant que la négligence ne peut être un motif d'exonération du respect des formalités normatives concernant le traitement de données. Le respect des principes de loyauté et de licéité tels que posés dans le RGPD a d'autant plus d'importance que les disparités de pouvoir et les liens de dépendance sont grands entre les personnes dont les données font l'objet d'un traitement et les responsables de traitement ou leurs sous-traitants. Ces disparités et les liens de dépendance sont particulièrement importants lorsque sont en jeu des questions de créances, notamment lorsque des banques sont impliquées. La ou le débiteur défaillant, s'il veut contester le traitement qui est fait de ces données par un organisme bancaire, contester les méthodes employées dans le cadre du recouvrement d'une créance à l'aide des données collectées, ou tout simplement contester des pratiques frauduleuses, doit s'appuyer en grande partie sur des données qui lui appartiennent mais qui sont traitées par la banque. Il s'avère que, du fait de leur position et de leur rôle, les banques ont la capacité de prévenir un contentieux ou de remettre gravement en cause les règles du procès équitable - dont le principe d'égalité des armes - par des mesures de dissimulation des preuves nécessaires au débiteur défaillant requérant, par l'utilisation de techniques bancaires en leur possession pour empêcher l'utilisation des moyens de paiement nécessaires pourtant à une défense effective. Ces méthodes sont possibles du fait des structures mêmes de l'intranet bancaire et de leur architecture en réseaux. La vérification *a posteriori* de l'utilisation conforme du traitement des données est de ce fait très complexe, voire impossible. Ces possibilités techniques aux mains des organismes bancaires, alors même que l'utilisation des données personnelles dans le cadre du recouvrement de créances peut conduire à des situations ressenties comme du harcèlement pour les personnes visées, puisqu'elles ne sont pas en capacité de rembourser, doivent donc faire l'objet d'une réglementation particulière permettant de garantir, par la voie d'une protection accrue des droits processuels des débiteurs dits défaillants, le principe de l'égalité des armes et d'un droit effectif au procès. Elle souhaite connaître son avis sur le sujet.

Texte de la réponse

La collecte de données personnelles est encadrée au niveau européen par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD). Ce règlement prévoit notamment qu'un traitement ne peut être considéré comme licite que si la personne concernée a consenti au traitement de ses données pour une ou plusieurs finalités spécifiques. Par ailleurs, le RGPD entérine à son article 20 un droit pour les utilisateurs d'accès à leurs données personnelles, les responsables de traitement étant dans l'obligation de fournir sur demande aux utilisateurs les données à caractère personnel les concernant qu'elles ont fournies, sans que le responsable de traitement puisse y faire obstacle. Ce droit d'accès, qui s'inscrit dans le droit à la portabilité des données, permet ainsi à tout utilisateur de vérifier les informations à caractère personnel le concernant dont dispose une société. Ces mesures sont de nature à assurer la transparence des sociétés quant aux données à caractère personnel qu'elles détiennent sur leurs clients. Toute société qui méconnaîtrait les dispositions du règlement précité s'expose par ailleurs à un régime de sanctions très strict fixé par le même règlement, pouvant aller jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial de l'entreprise concernée. En ce qui concerne plus spécifiquement le sujet de la dissimulation de preuve, celle-ci est déjà, en droit français, tant en matière pénale qu'en matière civile, prohibée et passible de sanctions. L'ensemble de ces éléments est ainsi de nature à prévenir les risques évoqués.

Données clés

Auteur : [Mme Danièle Obono](#)

Circonscription : Paris (17^e circonscription) - La France insoumise

Type de question : Question écrite

Numéro de la question : 34489

Rubrique : Numérique

Ministère interrogé : [Transition numérique et communications électroniques](#)

Ministère attributaire : [Économie, finances et relance](#)

Date(s) clé(s)

Question publiée au JO le : [1er décembre 2020](#), page 8621

Réponse publiée au JO le : [18 mai 2021](#), page 4220