ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 2302	De **Mme Marianne Dubois** (Les Républicains - Loiret)	**Question écrite**
Ministère interrogé > Numérique	**Ministère attributaire** > Justice	
Rubrique >moyens de paiement	**Tête d'analyse** >Achat sur le net, suppression des données bancaires	**Analyse** > Achat sur le net, suppression des données bancaires.
Question publiée au JO le : **24/10/2017** Réponse publiée au JO le : **11/09/2018** page : **8100** Date de changement d'attribution : **24/04/2018**		

Texte de la question

Mme Marianne Dubois attire l'attention de M. le secrétaire d'État, auprès du Premier ministre, chargé du numérique, sur la difficulté de nombreux utilisateurs d'applications d'achat pour supprimer définitivement leur compte. En effet, une fois qu'un utilisateur a enregistré ses données bancaires sur certaines applications d'achat, il lui est impossible de revenir sur cet enregistrement et de supprimer ses données. Certes, ses données ne sont pas utilisées à son insu mais il n'est pas normal que des données de cette importance ne puissent être effacées. Par ailleurs la multiplication des piratages de données d'importantes sociétés justifierait la possibilité donnée aux usagers de supprimer leurs données. Ainsi elle lui suggère d'obliger toute application d'achat en ligne à proposer une option de « suppression définitive des données bancaires » à ses utilisateurs.

Texte de la réponse

L'article 32-II de la loi no 78-17 relative à l'informatique, aux fichiers et aux libertés, transposant l'article 5 (3) de la directive 2002/58/CE 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) prévoit, s'agissant des données enregistrées dans une application, que le responsable du traitement ou son représentant doit informer l'utilisateur ou l'abonné d'un service des moyens dont il dispose pour s'opposer à l'accès aux informations stockées dans son équipement, en l'occurrence, l'application présente sur son ordinateur ou son ordiphone. La plupart des données de compte ou données bancaires constituent des données à caractère personnel au sens de l'article du paragraphe 1er de l'article 4 du règlement (UE) 2016/679 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), applicable depuis le 25 mai 2018. Le traitement de telles données doit donc respecter ce règlement. Conformément au principe de limitation de la conservation prévu à l'article 5 du règlement (UE) 2016/679, les données à caractère personnel 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 (…) ». Par ailleurs, l'article 17 de ce même règlement prévoit plusieurs possibilités d'effacement de données, par exemple si les données ne sont plus nécessaires au regard des finalités ou si le traitement de données a pour base le consentement de la personne concernée. Ce droit à l'effacement ne s'applique cependant pas dans la mesure où le traitement est nécessaire pour respecter une obligation légale qui requiert le traitement (article 17.3 b) ou dans la mesure où les données seraient nécessaires à la constatation, à l'exercice ou à la défense de droits en justice (article 17.3 e). Ainsi, les données relatives aux cartes bancaires peuvent être

conservées jusqu'à paiement effectif, qui peut être différé à la réception du bien, augmenté, le cas échéant, du délai de rétractation prévu pour les contrats conclus à distance et hors établissement, conformément à l'article L. 221-18 du code de la consommation. De même, dans le cas d'un paiement par carte bancaire, le numéro de la carte et la date de validité de celle-ci peuvent être conservés pour une finalité de preuve en cas d'éventuelle contestation de la transaction, en archives intermédiaires, pour la durée prévue par l'article L. 133-24 du code monétaire et financier, à savoir treize mois suivant la date de débit. Ce délai peut être étendu à quinze mois afin de prendre en compte la possibilité d'utilisation de cartes de paiement à débit différé. De telles données ne peuvent cependant être utilisées qu'en cas de contestation de la transaction. Les données conservées à cette fin doivent ainsi faire l'objet de mesures de sécurité particulières, ainsi que l'exige la Commission nationale de l'informatique et des libertés dans sa délibération no 2013-358 du 14 novembre 2013 portant adoption d'une recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance. Enfin, les données relatives aux cartes bancaires peuvent être conservées plus longtemps sous réserve d'obtenir le consentement exprès de la personne concernée et pour des finalités précises comme la facilitation de paiement réguliers. Ce consentement doit traduire une « manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, (…) » (article 4 du règlement (UE) 2016/679). Dans ce cas, le consentement peut être retiré à tout moment (article 7 du règlement). Il convient par ailleurs de rappeler que, afin d'éviter les piratages, l'article 32 du règlement (UE) 2016/679 impose la mise en place de mesures de sécurité appropriées au risque. Dans sa délibération no 2016-264 du 21 juillet 2016, la CNIL suggère à cet égard, comme mesure de sécurité, que « les données relatives au cryptogramme visuel ne [soient pas] conservées au-delà du temps nécessaire à la réalisation de chaque transaction, y compris en cas de paiements successifs ou de conservation du numéro de la carte pour les achats ultérieurs ». Dans ces conditions, le cadre juridique applicable apparaît suffisant, sans qu'il soit besoin d'obliger toute application d'achat en ligne à proposer une option de suppression définitive des données bancaires à ses utilisateurs.