ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 12657	De **Mme Karine Lebon** (Gauche démocrate et républicaine - NUPES - Réunion)	**Question écrite**

Ministère interrogé > Économie, finances, souveraineté industrielle et numérique	**Ministère attributaire** > Intérieur et outre-mer

Rubrique >banques et établissements financiers	**Tête d'analyse** >Usurpation d'identité et accès au Ficoba	**Analyse** > Usurpation d'identité et accès au Ficoba.

Question publiée au JO le : **07/11/2023**
Réponse publiée au JO le : **02/04/2024** page : **2612**
Date de changement d'attribution : **12/01/2024**

Texte de la question

Mme Karine Lebon interroge M. le ministre de l'économie, des finances et de la souveraineté industrielle et numérique sur les possibilités de développement de nouveaux outils permettant de lutter plus efficacement et plus rapidement contre l'usurpation d'identité. L'usurpation d'identité, délit défini comme le fait de prendre délibérément l'identité d'une autre personne vivante, généralement dans le but de réaliser des actions frauduleuses commerciales, civiles ou pénales, est un mal qui touche près de 200 000 personnes en France chaque année. À l'aide de tactiques toujours plus sophistiquées, la moindre information privée mise à la disposition de l'usurpateur peut engendrer des conséquences néfastes pour le quotidien de leurs victimes. Avec la simple photocopie d'une pièce d'identité et un justificatif de domicile, beaucoup de choses sont possibles : il pourra par exemple ouvrir des comptes en ligne et souscrire à des services financiers particuliers (augmentation des plafonds bancaires, souscriptions à des assurances...). C'est alors une véritable spirale qui s'enclenche : des plaintes peuvent être déposées contre les victimes elles-mêmes et de nombreux problèmes financiers peuvent survenir (interdit bancaire, fichage à la Banque de France, endettement). Afin de mettre un terme à ce cercle vicieux, les victimes doivent engager des démarches longues et fastidieuses, sans garantie de succès. Les pouvoirs publics ont mis en œuvre certains dispositifs afin d'aider et d'accompagner les victimes d'usurpation d'identité, mais force est de constater que leur efficacité n'est pas à la hauteur des enjeux et de la détresse vécue par ces particuliers. En interrogeant le Ficoba - fichier des comptes bancaires - la Cnil aide les victimes d'usurpation d'identité à localiser les comptes bancaires ouverts à leurs noms, de façon à en obtenir la fermeture. On y retrouve les références de chaque compte avec les numéros RIB, BIC et IBAN, la nature du compte qu'il soit courant ou d'épargne, le nom et l'adresse de la banque auprès de laquelle le compte est ouvert. Si l'intérêt de ce fichier n'est plus à démontrer, son efficacité dans la lutte contre l'usurpation d'identité est remise en question par les délais très longs d'obtention de ces informations par ceux qui en font la demande. À l'heure actuelle, une victime d'usurpation d'identité doit attendre entre six mois et un an pour obtenir le document référençant l'ensemble des comptes bancaires ouverts à son nom, délai durant lequel l'usurpateur peut continuer de sévir et aggraver davantage la situation personnelle de sa victime. Elle lui demande donc ce qui explique ce délai et souhaite connaître les mesures que ses services comptent mettre en œuvre pour accompagner de manière plus efficace les personnes victimes d'usurpation d'identité.

Texte de la réponse

L'usurpation d'identité est un délit qui désigne l'utilisation d'informations personnelles permettant d'identifier une

personne sans son accord pour réaliser des actions frauduleuses. En pratique, ces informations ont pu être obtenues à la suite de la perte ou du vol de documents d'identité de la victime, par le biais d'un message d'hameçonnage ("phishing" en anglais), par le piratage d'un de ses comptes en ligne, d'un de ses appareils ou encore le piratage d'un site Internet sur lequel ces informations étaient enregistrées. En fonction des informations recueillies, les escrocs peuvent dès lors commettre diverses infractions au nom de la victime : ouverture de ligne téléphonique ou de compte bancaire, souscription d'un crédit, location de voiture, cyberharcèlement, chantage, extorsion, etc. Nonobstant le préjudice moral, l'usurpation d'identité peut avoir des conséquences très importantes pour les victimes qui peuvent se voir poursuivies et devoir se justifier pour des infractions dont elles ne sont pas les auteurs, ou subir de nombreux désagréments financiers découlant d'un fichage à la Banque de France par exemple. Il existe plusieurs recours possibles en cas d'usurpation d'identité : en premier lieu, pour chaque fait d'usurpation, la victime peut déposer plainte au commissariat de police, à la brigade de gendarmerie ou encore par écrit auprès du procureur de la République. L'attestation de dépôt de plainte permettra à la victime de justifier de sa bonne foi dans ses échanges avec tous les établissements bancaires ou financiers dont elle se trouve être « cliente » de fait, par le biais de l'usurpation d'identité, et complétera utilement une attestation sur l'honneur rédigée à l'attention des organismes qui mettent en cause l'identité usurpée de la victime. Il ne s'agit là que d'un premier pas. Dans un deuxième temps, la victime peut consulter le fichier central des chèques, celui des incidents de remboursements des crédits aux particuliers et le fichier national des comptes bancaires (FICOBA) pour vérifier si des opérations frauduleuses n'ont pas été commises en son nom. Enfin, elle peut contacter la Banque de France pour signaler les faits dont elle est victime. Le FICOBA, géré par la Direction générale des finances publiques (DGFIP), recense tous les comptes bancaires et les comptes assimilés (comptes d'épargne, comptes-titres, etc.) ouverts en France. Les informations enregistrées concernent les opérations d'ouverture (nom de l'établissement, identité du ou des titulaires, personne morale, etc.), de modification et de clôture des comptes. Ces opérations sont déclarées à la DGFIP par les organismes qui gèrent les comptes (établissements bancaires et financiers, centres de chèques postaux, sociétés de Bourse, etc.), à charge pour cette administration de procéder à leur inscription dans le fichier national. Les conditions d'accès à ce fichier sont strictement encadrées par la loi (article L103 du livre des procédures fiscales) qui définit les principales personnes ou organismes habilités à le consulter : agents de la DGFIP ou des douanes, autorités judiciaires, officiers de police judiciaire, huissiers de justice agissant avec un titre exécutoire, personnes chargées de poursuivre le recouvrement de créances alimentaires, agents de la CAF ou des caisses de retraite, agents de Pôle emploi, établissements bancaires, notaires en charge d'une succession, fonds de garantie des victimes des actes de terrorisme, etc. Le titulaire d'un compte (personne physique) peut consulter les informations le concernant et ainsi identifier les comptes ouverts frauduleusement à son identité. Ce droit d'accès s'exerce, en fonction de la demande, auprès du centre des finances publiques (accès aux données d'identification personnelles) ou de la CNIL. C'est auprès de ces organismes que la victime doit formuler une demande de droit d'accès indirect (par courrier ou en ligne via le site internet) pour accéder à la liste des comptes ouverts à son nom et aux informations relatives aux comptes bancaires (la nature et l'identification du compte : numéro, type, caractéristiques du compte, coordonnées de l'établissement gestionnaire du compte, etc.). Le délai de réponse à cette sollicitation reste variable. La CNIL a cependant instauré un suivi qui permet à la victime de connaitre en temps réel l'état d'avancement de sa requête auprès du service du droit d'accès indirect, tous les jours de la semaine, à partir du moment où la demande est datée de plus de deux mois. Ce suivi contribue ainsi à diminuer le temps de réponse. Concomitamment, et dans l'attente de cette réponse, la victime d'usurpation d'identité peut déposer un dossier pour usurpation d'identité auprès de la Banque de France (en mains propres ou en ligne) en joignant des pièces justificatives. Sur la base des éléments transmis, la Banque de France contacte les établissements (banques, sociétés de financement, etc.) qui ont inscrit la victime sur les fichiers d'incidents. Dès lors qu'un de ces établissements reconnaît l'usurpation d'identité, la Banque de France appose une mention particulière dans ses fichiers. Ainsi, l'inscription des incidents dans le (s) fichier (s) avec mention particulière « d'usurpation d'identité » permet d'avertir les établissements financiers qui consultent ces fichiers avant de donner un moyen de paiement ou d'accorder un crédit. Cette procédure contribue ainsi à limiter les dommages que peuvent faire les fraudeurs avec l'identité usurpée. Par ailleurs, la gendarmerie lutte activement contre l'usurpation d'identité notamment au travers de 3 aspects relevant du Commandement de la Gendarmerie pour le Cyberespace (CGC) : La conception et la réalisation d'outils permettant les échanges dématérialisés. Le CCG, dans le cadre de ses partenariats (GIE carte bancaire) et

récemment via son intégration à l'INTER-CERT, fournit régulièrement des informations sur l'état des menaces. La connaissance des modes opératoires des cyber-criminels permet de mettre en œuvre des contremesures techniques. La division technique du CCG travaille avec certains industriels en fonction des vulnérabilités techniques identifiées ; La sensibilisation d'acteurs administrant des données à caractère personnel. Au sein des administrations et/ou des entreprises, les délégués à la protection des données (DPO), les archivistes ou encore les RH ont un rôle déterminant pour s'assurer des dispositifs techniques à mettre en place (ex : coffre-fort numérique) et les process à suivre en cas d'incidents (en cas de fuite de données et/ou vulnérabilité). Ainsi, le CCG est amené à sensibiliser ces personnes soit directement (ex : entreprises de transport aérien) ou auprès d'associations professionnelles (ex : SDIS, entreprises, assureurs ...). Enfin, des partenariats peuvent être signés pour les accompagner (échange d'informations sur la menace, constructions d'outils de sensibilisation) ; La sensibilisation du grand public. Le CCG participe à des événements de sensibilisation au profit du grand public (ex : NANTES cyber DAYS, les 100 ans de BELFORT) en mettant un fort accent sur la fraude à l'identité numérique au travers du phishing. Enfin, l'unité participe activement à la construction d'outils de sensibilisation avec ses partenaires (ACYMA, CAMPUS Cyber). La dernière réalisation est la campagne du "FRAUDE FIGHT CLUB" qui vise à lutter contre la fraude par ingénierie sociale, en s'appuyant sur le réseau social INSTAGRAM.