ACTUALITÉS DPO CONSULTING BFC

Plein de nouveautés chez DPO Consulting BFC !

Nous participerons au Salon de la Prévention **le jeudi 14 octobre** et **le vendredi 15 octobre** à Vesoul au Parc des expositions. Entrée gratuite.

Nous vous attendons sur notre stand !

* * *

Nous serons également présents lors du congrès de l'Ordre régional des experts-comptables de Bourgogne-Franche-Comté qui se déroulera le **jeudi 4 novembre 2021 à Micropolis**.

* * *

Vous souhaitez former vos collaborateurs ? En attendant la certification Qualiopi, **notre agence est Datadockée** ! N'hésitez donc plus à nous solliciter pour vos besoins en sensibilisations ou formations RGPD ne serait-ce que pour amorcer votre mise en conformité.

* * *

Dernière nouvelle, **Stéphanie BROGGINI**, Consultante RGPD et DPO externe, vient d'être **certifiée auprès d'AFNOR selon le référentiel CNIL qui reconnait les compétences des Délégués à la Protection des Données**.

Faire appel à un DPO certifié est gage de confiance quant aux compétences et savoir-faire de ce dernier dans la mise en conformité de ses clients.

L'usurpation d'identité

Un phénomène chiffré à plus de 474 millions d'euros par an pour les victimes et assureurs

L'investigation menée par l'équipe de Julien COURBET pour l'émission « Arnaques ! » diffusée sur M6 le 16 août dernier, nous apprend que 50% des victimes d'usurpation d'identité **n'ont jamais perdu leurs papiers**. L'interception des justificatifs nécessaires passe généralement par internet, lors d'une transmission de documents d'identité officiels sur des sites ou par mail. Plus basiquement cette récupération peut résulter d'un ramassage de poubelles dans lesquelles il n'est pas rare d'y trouver des factures d'électricité par exemple, constituant un justificatif de domicile. Ce document, couplé à une copie de pièce d'identité, suffit à contracter des crédits au nom de la victime.

Si l'usurpation peut résulter d'une erreur de la victime (perte, négligence, mot de passe faible…) elle peut également découler d'une violation de données dans une entreprise dans laquelle sont traitées les données personnelles de celle-ci. C'est ce que rappelle la CNIL au sujet de la perte majeure de données qu'a connu l'AP-HP (Assistance Publique-Hôpitaux de Paris). Cette dernière a subi une fuite d'1,4 millions de données de personnes telles que : noms, prénoms, date de naissance, numéro de sécu, adresse postale et électronique… La CNIL précise que cette violation de données est telle qu'elle est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes, notamment l'usurpation d'identité.

DPO Consulting franchise Bourgogne Franche-Comté
SAS MCC au capital de 31 490 € - ZA les Salines - 25115 POUILLEY-LES-VIGNES
RCS Besançon 434 463 683 - TVA FR 24 434 463 683
Éric CUENOT / Président & Data Privacy Officer 06 65 91 28 76 eric.cuenot@dpo-consulting.com
Stéphanie BROGGINI / Data Privacy Officer 07 55 58 02 80 stephanie.broggini@dpo-consulting.com

Bon nombre d'usurpations d'identité ne sont pas poursuivies, les faits n'étant pas constatés à temps par les victimes ou les autorités compétentes.

La médiatisation a tout de même pour conséquence que les Français sont un peu plus vigilants aujourd'hui face à ce phénomène ; la CNIL relève une croissance de 70% des demandes d'accès au FICOBA (fichier des comptes bancaires et assimilés) au premier semestre 2021 par rapport à l'année précédente, rapporte le journal *Les Echos*. Ces demandes visent à vérifier les comptes ayant été souscrits sous tel ou tel nom. Dans 35% des cas, elles étaient motivées par une usurpation d'identité réelle ou redoutée.

Dans un rapport d'information présenté à l'Assemblée nationale le 8 juillet 2020 par la mission d'information sur l'identité numérique, a été relayé un sondage du CSA publié en 2012, qui indiquait que 8% des Français avaient été victimes, dans la décennie qui précédait, d'une usurpation d'identité en ligne.

Christophe Naudin, criminologue spécialiste en criminalité identitaire, considère que cette forme de délinquance est devenue la deuxième infraction en France, devant les cambriolages et derrière les vols de voiture.

Vol des données personnelles, de multiples techniques utilisées

- Par mail, technique la plus utilisée. En effet, le Cabinet Deloitte rapporte que l'envoi d'emails frauduleux est à l'origine de 91% de l'ensemble des cyberattaques. Dans ces mails, pouvant parfois être extrêmement personnalisés et donc plus crédibles aux yeux de la personne visée, le cybercriminel va essayer de créer assez de confiance en sa rouerie pour que la victime transmette ses informations personnelles.
- Sur les réseaux sociaux. Les faussaires se créent de faux comptes sous le nom des victimes afin de nuire à leur réputation ou inspirer la confiance de leurs proches pour les escroquer.
- Par l'usurpation du numéro de téléphone. Cette technique vise à faire payer un appel surtaxé. Le malfaiteur peut également tenter de convaincre de divulguer des informations personnelles importantes.
- Par l'adresse IP. L'usurpateur va faire croire à un ordinateur que les informations envoyées à un utilisateur sont une source fiable, afin de leur permettre de passer cette sécurité.
- Par les sites web. L'escroc copie un site internet légitime afin d'amener la victime à délivrer ses informations personnelles.
- Par la publication d'offres frauduleuses. Il s'agit souvent d'annonces immobilières attrayantes visant à piéger des individus pressés ou peu vigilants. L'escroc demande à la victime de lui transmettre un dossier complet de documents, qui lui permettra par exemple de contracter des petits crédits où l'identité du souscripteur est peu contrôlée, mais également d'ouvrir des comptes sur des banques en ligne, encore trop négligentes sur ces questions.

Dans son rapport d'activité de 2020, la plateforme **Cybermalveillance.gouv.fr** a relevé que parmi toutes les recherches d'assistances effectuées par les particuliers en 2020, était en tête l'hameçonnage, suivi du piratage de compte et du faux support technique. Ces trois formes de cybermalveillance peuvent toutes avoir pour conséquence une violation des données personnelles de la victime, pouvant mener à une usurpation d'identité. Du côté des professionnels, qu'ils soient du secteur public ou privé, on retrouve en première recherche les rançongiciels, suivis des piratages informatiques et des piratages de comptes.

Les conséquences désastreuses d'une usurpation d'identité pour les victimes

Une fois que les usurpateurs disposent d'informations personnelles sur une personne, comme sa carte d'identité et un justificatif de domicile, il leur est alors très simple d'ouvrir des comptes bancaires en ligne au nom de leur victime, d'emprunter de grosses sommes, de souscrire à des assurances, etc…

Les conséquences sont multiples et graves.

Elles sont d'abord psychologiques, la victime vivant mal le vol de son identité et le fait d'être assimilée à un escroc aux yeux de la société… et elles sont matérielles et financières, la cible pouvant être interdit bancaire, fichée à la Banque de France, ce qui anéantit tout projet personnel sur le plan financier, à court comme à long terme.

De plus, cette personne peut être assignée en justice pour les infractions qu'a commis son usurpateur et doit donc faire face à toute la machine judiciaire pour espérer faire constater l'usurpation et se retourner contre son malfaiteur… encore faut-il qu'il soit identifié.

Le journal *La Dépêche* rapportait en novembre 2020, le cas d'un Toulousain de 49 ans ayant perdu sa carte d'identité en 2017, malheureusement récupérée par un faussaire. Ce dernier a pu obtenir un avis d'imposition, ce qui lui a permis d'ouvrir des comptes bancaires au nom de sa victime et d'effectuer des achats en ligne sur des sites marchands grâce aux données personnelles contenues dans cet avis. Depuis qu'il s'est fait usurper son identité, ce Toulousain est sommé de rembourser les sommes dues aux créanciers de son faussaire. Étant dans l'impossibilité de le faire, il est alors interdit bancaire et fiché à la Banque de France. Il doit en outre déposer, à chaque plainte portée contre lui par les créanciers impayés, une plainte complémentaire pour que des poursuites soient menées contre son usurpateur. Cet homme témoigne encore se voir refuser ses moyens de paiement actuels par de nombreux commerces et services.

On peut également citer le cas d'un Parisien, victime du vol de sa carte d'identité qu'il avait communiquée en ligne lorsqu'il cherchait un logement. Le journal *Le Parisien* relate que les malfaiteurs ont créé une société fictive de vente de voiture à son nom, afin de procéder à l'immatriculation de près de 300 véhicules, leur permettant de commettre, du simple stationnement interdit, aux infractions les plus graves comme des braquages, et ce en toute impunité. Le Trésor Public lui réclame alors 200 000€ pour ces infractions routières commises par les usurpateurs. Mis hors de cause pour les délits commis, ce Parisien doit néanmoins contester chaque contravention au Code de la route qu'il reçoit.

Les victimes d'usurpation d'identité font face à deux considérations majeures qui complexifient fortement l'identification de leurs usurpateurs :

- Tout d'abord, les auteurs de ces escroqueries utilisent des moyens toujours plus performants pour brouiller leurs traces.
- Ensuite, si ces malfaiteurs commettent leurs délits depuis l'étranger, les procédures pour tenter de les retrouver peuvent être plus complexes, longues et dispendieuses.

Les personnes morales ne sont pas en reste ! La situation dans laquelle se trouve la société « Le plaisir du Camping-car » basée à SAZE dans le Grand Avignon depuis cet été, est parlant.

Des escrocs ont fait passer des annonces de vente de camping-cars particulièrement attractives au nom de cette société sur le site LEBONCOIN. Utilisant de faux bons de commande, les usurpateurs ont récupéré plusieurs acomptes de la part de particuliers… pour certains de l'ordre de 32 000€ ! Tout était fait pour tromper les particuliers : bon numéro de RCS, entête conforme à celle de la société, logo identique, faux tampon… ces informations sont facilement récupérables sur le net. En tout 45 plaintes ont été déposées contre la société, elle-même victime de cette situation. Le préjudice est conséquent tant financier qu'humain. À peine sorti de la crise du covid, ce gérant est touché par une nouvelle épreuve dont il juge difficile de sortir subissant également des menaces à son intégrité physique, les particuliers victimes ayant identifié cette société comme le véritable escroc…

Les dernières estimations réalisées en 2009 par le Credoc (Centre de Recherches pour l'Étude et l'Observation des Conditions de vie) **chiffre ce délit à plus de 474 millions d'euros par an, pour les assureurs et les particuliers**. Selon le Centre, **le coût global est même beaucoup plus élevé pour l'ensemble de la société, qui se situerait proche des 3 milliards d'euros par an.**

Les conditions pour caractériser l'usurpation d'identité numérique

L'usurpation d'identité numérique est constituée lorsqu'elle porte sur l'identité de la victime, mais aussi sur toute autre donnée permettant son identification. Ce délit peut alors en pratique porter sur le nom, prénom, pseudonyme, les identifiants électroniques, mais aussi l'adresse IP, les mots de passe, logos et images, étant tous des éléments permettant d'identifier leur propriétaire, directement ou indirectement.

Elle est commise sur un *« réseau de communication au public en ligne »*, ce qui comprend les services de messageries électroniques, les sites web, les messages et profils sur les réseaux sociaux.

Le préjudice subi par la victime est constitué par un trouble de sa tranquillité, ou par une atteinte à son honneur ou à sa réputation. Notons que le préjudice peut être subi par la victime de l'usurpation, mais aussi par un tiers à qui on soutire de l'argent ou des informations personnelles à son tour.

S'agissant la position des juges face à ce délit, on peut citer la première condamnation pour usurpation d'identité numérique sur le fondement de l'article 226-4-1 du Code pénal, dans l'affaire du faux site de Mme Rachida DATI.

Un ingénieur informaticien avait créé un faux site internet imitant celui de Madame la députée mairesse du 7ème arrondissement de Paris, en reprenant sa photographie et de nombreux éléments graphiques. Ce site permettait à n'importe quel internaute de publier des messages qui paraissaient alors rédigés par Mme DATI. Un lien présent sur le site créé par le faussaire permettait également de continuer sa navigation sur le site officiel de la victime, renforçant encore un peu plus la prétendue véracité des messages postés par les internautes. Les juges du fond ont considéré que l'élément matériel du délit d'usurpation d'identité numérique était constitué dès lors qu'était reproduite une photographie de Mme Rachida DATI, ainsi que les principaux éléments de son site officiel. Ils vont encore relever que l'élément intentionnel frauduleux était constitué par la seule volonté de créer un site fictif et d'encourager son audience sur les réseaux sociaux.

Ce système créé par le prévenu venait alors troubler la tranquillité, porter atteinte à l'honneur et à la considération de sa victime.

C'est avec la réunion de ces 3 conditions que le prévenu sera condamné jusqu'en cassation.

Victime d'usurpation d'identité, que faire ?

La plateforme nationale **Cybermalveillance.gouv.fr** a pour objet de sensibiliser les particuliers et professionnels aux risques de cybermalveillance et d'assister les personnes qui en sont victimes. Sur cette plateforme, on peut alors retrouver de nombreux conseils sur l'attitude à adopter dans différents cas de figure.

Avant tout, il est possible de demander au responsable du site internet de cesser toute diffusion de ses informations personnelles en ligne en les supprimant. Certains grands réseaux sociaux comme Facebook, Twitter ou Instagram disposent d'un formulaire à cet effet.

La CNIL, même si elle ne dispose d'aucune autorité s'agissant de l'usurpation d'identité, propose sur son site des modèles de courrier afin de formuler la demande de suppression des données personnelles en ligne auprès du responsable du site internet.

Dans le même temps, il convient de se constituer un dossier de preuves, comprenant l'ensemble des éléments permettant de prouver l'infraction, et que ce ne sont pas les données d'un homonyme. Ce dossier peut alors contenir des captures d'écrans, l'URL du site malveillant, etc…

L'usurpation d'identité constituant un délit pénal, les victimes peuvent porter plainte tant devant les services de polices judiciaires que devant le Procureur de la République.

Il est également recommandé de faire connaître cette plainte à un maximum d'institutions, comme votre banque, la banque de France, les entreprises de téléphonies, EDF…

À titre préventif, plusieurs sites internet offrent la possibilité de vérifier si son adresse électronique a déjà fait l'objet d'un piratage. L'un des plus connus est le site **haveibeenpwned.com**, développé par Troy Hunt, expert en sécurité. Cette plateforme va analyser les différentes violations de données de sites web qu'elle répertorie. Ce site internet permet également de vérifier des identifiants sur différents portails web.

On rappellera de ne pas jeter à la poubelle tel quel les différentes factures : téléphonie, gaz, électricité, mais également les copies de cartes d'identité, les livrets de famille, les cartes grises, les actes de mariage, les contrats d'assurance, de gardiennage, d'entretien… Dès lors qu'une donnée identifiante est présente dans le document, il vaut mieux prendre certaines précautions lorsque l'on souhaite s'en débarrasser.

Plus encore, il est nécessaire d'adopter une politique de mots de passe forte. Vos mots de passe sont la clés permettant à certains faussaires d'accéder à toutes vos informations : ils doivent donc être difficiles (min 8 caractères avec majuscules, chiffres et caractères spéciaux), différents à chaque compte et changés aussi souvent que possible.

Me Sylvie NOACHOVITCH, présente dans l'émission « Arnaques ! », précise que si la transmission d'une pièce d'identité par internet est absolument requise, il convient de barrer la pièce d'identité de deux traits et d'indiquer la personne à qui cette copie est destinée.

Vol de données en entreprise ?

Les entreprises regorgent de données personnelles et notamment celles de leurs salariés. Quelques soient les finalités, les données personnelles des salariés, clients, fournisseurs doivent faire l'objet d'une sécurité accrue. Plus encore lorsque l'organisme gère et traite des données sensibles.

En tant que responsables de traitements ou sous-traitants de la donnée personnelle, les articles 33 et 34 du RGPD notamment, font peser sur elles des obligations de mettre en place des mesures pour prévenir les violations de données et réagir de manière adaptée le cas échéant, tel que nous l'avons développé dans nos anciennes notes d'information.

Vous pouvez retrouver nos précédentes notes d'informations sur le site internet :

- la conformité des sites web
- la responsabilité du sous-traitant avant et après le RGPD
- la prospection commerciale sur LinkedIn
- la charte informatique