La cybercriminalité a l'heure du droit des successions

A l'heure où le monde se numérise, les attaques informatiques deviennent de plus en plus nombreuses. Beaucoup d'héritiers sont de plus en plus victimes de vol de leur identité par des inconnus, s'en prenant ainsi à leurs successions ou parts successorales.

Pour la résolution de vos problèmes relatifs de succession, nos avocats sont disposés à vous aider.
Téléphonez-nous au : 01 43 37 75 63 ou remplissez le formulaire en cliquant sur le lien

Les infractions servant de base légale à la répression de la cybercriminalité ont toutes pour point commun d'utiliser les systèmes et réseaux numériques tantôt en tant qu'objets de l'infraction, tantôt encore en tant que supports de

l’infraction, tantôt enfin en tant que moyens de l’infraction.

« La cybercriminalité », également appelée criminalité informatique, consiste en la réalisation de délits commis à l’aide d’équipements informatiques et d’Internet. Parmi les exemples classiques de cybercriminalité, il est possible de citer la diffusion de virus informatiques, le téléchargement illégal, les actes de phishing, le vol d’informations personnelles telles que des données bancaires ou données à caractère personnelles.

La cybercriminalité est une des formes de délinquance qui connaît la croissance la plus forte. La rapidité et la fonctionnalité des technologies modernes renforcent la facilité de l’anonymat et ainsi entraînent de nombreux délits notamment l’usurpation d’identité. Ce délit peut avoir des conséquences importantes dans le cadre d’une succession.

En outre, la cybercriminalité est une délinquance protéiforme, dont l’ampleur reste difficile à évaluer. Ses auteurs comme ses victimes présentent des profils variés : de simples particuliers, des organisations criminelles, des États peuvent être impliqués. Il est cependant certain que la cybercriminalité représente une menace croissante en raison de la place grandissante qu’occupe le numérique dans nos économies et nos sociétés.

Lorsque les systèmes et réseaux numériques sont l’objet de l’infraction, les atteintes aux systèmes de traitement automatisé de données, les infractions en matière de fichiers ou de traitements informatiques et enfin la cryptologie constitue aujourd’hui le cœur des incriminations.

Quant au droit des successions, c’est tout simplement la transmission de tout le patrimoine du De cujus à ses éventuels héritiers, légataires ou légataires à titre universel.

Deux infractions seront évoquées à ce stade : il s’agit de l’usurpation d’identité et arnaque sur internet : l’exemple de

l’héritage.

Le délit d’usurpation d’identité prévu et réprimé par l’article 226-4-1 du Code pénal suppose qu’il soit fait usage de l’identité d’un tiers en vue de troubler sa tranquillité ou celle d’autrui, ou de porter atteinte à son honneur ou à sa considération.

Encourt la cassation l’arrêt qui déclare une personne coupable de ce délit, alors qu’il constate que l’identité prétendument usurpée correspond aussi à celle qui avait été attribuée au prévenu dans des circonstances extrinsèques à savoir, lorsqu’il était mineur, à la demande d’une personne s’étant présentée comme son père de sorte que ni le fait d’usurper l’identité d’un tiers ni la volonté d’en faire usage en vue de troubler la tranquillité du tiers ou celle d’autrui, ou de porter atteinte à son honneur ou à sa considération ne peuvent être caractérisés **(1).**

I. L’usurpation d’identité

L’usurpation d’identité désigne l’utilisation d’informations personnelles permettant d’identifier une personne à son insu pour réaliser des actions frauduleuses. Cette cyber-menace peut avoir des incidences en droit des successions.

Un traitement de données à caractère personnel a été créé auprès du ministère de l’Intérieur (Arr. 9 nov. 2011, NOR : IOCD1130891A : JO, 29 nov. mod. par. Arr. 27 nov. 2014) à fin de gestion des dossiers instruits dans le cadre de la lutte contre la fraude documentaire et de l’usurpation d’identité sur les cartes nationales d’identité et les passeports (art. 1er).

A. Éléments matériels

- Comportement

Usurpation d’identité

L’usurpation d’identité est une infraction dont se servent les arnaqueurs pour pouvoir dépouiller les héritiers.

Le terme usurpation ne soulève pas de difficultés particulières. Il correspond au fait de s’attribuer sans droit, et donc de manière illégitime, l’identité d’un tiers, dans le but de se faire passer pour lui. Il peut être remarqué que dans le projet de loi, il était fait référence non pas à l’usurpation, mais à la simple utilisation de l’identité d’autrui.

La modification intervenue au cours des travaux préparatoires s’explique par la volonté du législateur de ne pas faire entrer dans le champ d’application de l’incrimination les comportements consistant seulement à citer le nom d’un tiers sans qu’ils aient pour finalité, dans le même temps, de se faire passer pour celui-ci.

C’est pourquoi la seule mention du nom d’autrui dans un journal ne saurait relever de l’article 226-4-1 du Code pénal. Elle peut néanmoins être éventuellement sanctionnée pénalement sur le fondement de la loi du 29 juillet 1881 relative à la liberté de la presse si le propos tenu à l’encontre de la personne citée se révèle diffamatoire ou injurieux.

C’est la raison pour laquelle il peut être considéré que « l’identité au sens de l’article 226-4-1 du Code pénal apparaît ainsi pétrie du nom de la personne, mais entendu dans un sens large, celui qu’elle a reçu par la naissance, celui qu’elle a pris à l’occasion d’un changement officiel de nom ou, en fait, celui qu’elle s’attribue. Bref, l’identité en ce sens, c’est la façon dont la personne s’appelle ou se fait appeler »

Usage d’une ou de plusieurs données de toute nature permettant d’identifier un tiers.

Le concept d’usage est plus large que celui d’usurpation. Il y a en effet usage par la seule utilisation de ce qui en constitue l’objet, indépendamment de la fin consistant à se faire passer pour autrui. La distinction avec l’usurpation peut paraître ténue, mais elle n’en est pas moins réelle, ne serait-ce que d’un point de vue théorique. Ainsi, il y a usage, et non pas usurpation, dans le fait de se servir des identifiants d’un tiers pour bénéficier des services qu’ils permettent d’obtenir sans que cette utilisation implique spécialement la volonté de se faire passer pour ce tiers.

La finalité de l’usage, à l’inverse de celle de l’usurpation, peut donc consister dans la satisfaction de besoins exclusivement matériels. Il semble pourtant qu’il faille admettre qu’appliquée à l’infraction définie à l’article 226-4-1 du Code pénal, la distinction perd un peu de son effectivité. La raison en est qu’aux termes du texte d’incrimination, l’usage doit être fait en vue de troubler « la tranquillité [du tiers] ou celle d’autrui, ou de porter atteinte à son honneur ou à sa considération ».

Or, un tel objectif est plus difficile à atteindre lorsqu’il n’y a pas de volonté de se faire passer pour la personne dont les données permettant de l’identifier sont utilisées.

Comme pour l’identité, le législateur n’a pas pris le soin de définir ce que sont « les données de toute nature permettant d’identifier » un tiers. Son silence n’est pas sans présenter de nombreux inconvénients au regard du principe de légalité.

- Résultat

L’usurpation d’identité ou l’usage de données de toute nature permettant d’identifier un tiers doit avoir pour finalité soit de troubler sa tranquillité ou celle d’autrui, soit de porter atteinte à son honneur ou à sa considération.

À lui seul, le texte d’incrimination laisse relativement ouverte la question de l’identification de la valeur sociale

protégée. Il paraît donc nécessaire pour résoudre la difficulté de s'intéresser à la place de l'infraction dans le Code pénal. En effet, il s'agit d'une donnée non pas seulement formelle, mais également fondamentale en ce qu'elle fournit de précieux éléments d'information sur la valeur sociale que le législateur a entendu protéger à travers l'incrimination.

Le résultat légal ne coïncidant pas avec le résultat redouté qu'il précède, le délit de l'article 226-4-1 doit être rattaché à la catégorie non pas des infractions matérielles, mais à celle des infractions formelles. Le texte présente l'intérêt de pouvoir être sollicité de manière anticipée puisqu'il peut être retenu avant que la valeur sociale protégée soit effectivement atteinte, et ce sans qu'il soit pour autant besoin d'appliquer la théorie de la tentative.

Le délit d'usurpation d'identité est étendu à « l'hameçonnage » ou « phishing ». Ce dernier est défini comme le « vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge.

En effet, un système d'authentification est simulé par un utilisateur malveillant, qui essaie de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime. Le phishing ou hameçonnage vise à obtenir du destinataire d'un courriel d'apparence légitime qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion à des services financiers, afin de lui dérober de l'argent

Il s'agit de l'un des principaux vecteurs de la cybercriminalité. Ce type de pratique est courant en droit des successions. Par exemple, un cybercriminel qui se fait passer par un membre de la famille et entretient une relation de confiance virtuelle avec la victime et, une fois, la confiance établie, lui demande une aide financière importante (argent qui peut être destiné au partage successoral), avant de couper brutalement le contact.

Par ailleurs, l'usurpation d'identité numérique peut conduire l'auteur d'hameçonnage à s'introduire dans un système de traitement automatisé de données (STAD) pour prendre, par exemple, la racine d'une adresse électronique et ainsi se crédibiliser aux yeux de la victime.

Le comportement est incriminé en droit pénal des biens, à l'article 323-1 du Code pénal initialement introduit par la loi Godfrain n° 88-19 du 5 janvier 1988 (infractions propres à l'informatique). Le texte vise le fait « d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données », la peine passant de deux ans à cinq ans d'emprisonnement et de 60 000 à 150 000 € d'amende lorsque ce STAD est mis en œuvre par l'État (songeons à une adresse mail « impot.gouv » qui serait falsifiée)

La loi ne définit pas ce qu'est un STAD. Il a toutefois été jugé que les services de messagerie électronique d'une entreprise constituent « de façon incontestable » un STAD. L'infraction est ainsi caractérisée par le fait d'usurper, frauduleusement, des adresses électroniques d'expéditeurs et d'en faire usage par l'envoi de messages depuis les services de messagerie électronique de cette entreprise (TGI Le Mans, 7 nov. 2003).

L'hameçonnage passe aussi le plus souvent par du ***spamming***. L'auteur adresse en effet par mail le site internet contrefait à des milliers de personnes en même temps.

Le *spamming* est réprimé à l'article 226-18-1 du code pénal comme le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection. Il s'agit ici de protéger de nouveau la vie privée de la personne, mais davantage dans sa tranquillité et, plus encore, l'atteinte à son droit d'opposition à la réception de courriels.

La loi informatique et liberté du 6 janvier 1978 a conduit à intégrer au Code pénal l'article 226-18 qui réprime de cinq ans d'emprisonnement et 300 000 € d'amende le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite. Le droit pénal retrouve ici sa place de droit sanctionnateur, d'*ultima ratio* de la réaction sociale. En effet, le délit est assurément intentionnel. Sur le plan matériel, on notera que l'incrimination vise le fait de collecter et non mémoriser ou stocker.

B. Élément moral

- Dol général

Le dol général consiste ici, au regard de ce qui constitue la matérialité de l'incrimination, dans la seule volonté consciente d'usurper l'identité d'un tiers en l'occurrence d'un héritier ou de faire usage de données de toute nature permettant d'identifier cet héritier.

- Dol spécial

Aux termes de ce dernier, l'usurpation d'identité d'un héritier ou l'utilisation de données de toute nature permettant de l'identifier doit avoir été commise « en vue » de troubler la tranquillité, l'honneur ou la considération. Il s'agit donc de l'archétype de l'infraction dont la constitution est subordonnée à l'existence d'un dol spécial tel qu'il a été précédemment défini. Il en ressort que la volonté de l'agent de porter atteinte à la tranquillité, l'honneur ou la considération d'autrui doit être établie pour que l'infraction puisse être consommée, et ce alors même qu'il n'est pas nécessaire qu'un tel résultat ait été atteint puisque, matériellement, il reste parfaitement indifférent, du fait du caractère formel de l'incrimination.

II. Arnaque sur internet : l’exemple de l’héritage

Internet constitue sans aucun doute une bonne occasion pour les délinquants de multiplier leurs exactions, dans ce monde virtuel pour certains, mais rémunérateur pour d’autres. C’est ce que révèle l’étude de plusieurs décisions de jurisprudence rendues ces dernières années, qui ont retenu la qualification d’escroquerie pour des opérations commises via internet.

L’Escroquerie définie par l’article 313-1 du Code pénal, « l’escroquerie est le fait, soit par l’usage d’un faux nom ou d’une fausse qualité, soit par l’abus d’une qualité vraie, soit par l’emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d’un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. L’escroquerie est punie de cinq ans d’emprisonnement et de 375 000 euros d’amende ».

A. Réalisation d’escroqueries grâce à internet

De manière assez exceptionnelle, internet peut simplement faciliter l’escroquerie à petite échelle. C’est le cas par exemple de personnes se disant détentrices d’un héritage. Ces personnes contactent souvent les vrais héritiers et leur demandent leurs coordonnées bancaires.

Le mieux est donc de prévenir plutôt que guérir et retenir qu’en matière d’héritage, le notaire vous contactera, mais on ne vous demandera jamais de virer de l’argent sur le compte d’un soi-disant professionnel, avocat ou notaire afin que vous puissiez percevoir ce beau présent, il existe « toute une procédure » et des actes pour officialiser votre qualité d’héritier cela ne se fait pas par deux trois échanges de

mails.

Ainsi, se rend coupable d'escroquerie l'individu qui a usurpé deux identités, en utilisant sous le couvert de celles-ci des moyens de paiement qu'il s'était procuré illégalement, soit en achetant sur internet, des numéros de carte bancaire, soit en ouvrant des comptes bancaires au moyen de faux documents (faux bulletins de salaire, fausses quittances), comptes dont il savait qu'ils étaient dépourvus de toute provision et, par ces moyens frauduleux, ont trompé l'ensemble des commerçants et particuliers qui lui ont remis des marchandises ou des services **(2).**

De même, un individu a intercepté un courrier adressé par la banque à ses parents contenant les codes d'accès bancaire par internet à l'aide desquels il a procédé à des virements à son profit. La chambre criminelle **(3)** relève que l'escroquerie est parfaitement caractérisée en ce sens que les manœuvres frauduleuses ont eu pour effet de déposséder la banque de fonds détenus pour le compte de clients auxquels elle était tenue de les représenter.

Tel est également le cas de celui qui, par l'usurpation des identités de trois clients, donne des ordres de virements par internet et télécopie afin de faire transférer de leur compte réel ouvert auprès de la banque néerlandaise ING, au moyen de comptes ouverts en France, des sommes approchant un à deux millions d'euros **(4).** Certains tentent aussi de profiter de cette technologie pour commettre des escroqueries dans le cadre de leur profession pour escroquer d'éventuels héritiers réservataires **(5).** (En ce sens, V. le cas d'un médium).

B. Escroqueries sur internet

La plupart du temps, internet constitue le cœur du processus d'escroquerie notamment parce qu'il permet de réaliser l'infraction à l'encontre d'un nombre important de personnes. C'est notamment ce qui se produit lors des actes de phishing

par lesquels les individus, après avoir récupéré, par la voie de robots, des milliers d'adresses électroniques ciblées et filtrées (ex. : adresse en « fr »), envoient des courriers électroniques invitant les destinataires à se connecter en ligne par le biais d'un lien hypertexte sur une page < web > factice, qui ressemble à s'y méprendre à celle du site original (c'est la technique du pharming). Le courriel demande en général au destinataire, sous couvert d'un problème technique ou d'une rénovation totale du site, de mettre à jour ses identifiants, mots de passe, numéro de compte, etc.

Lorsque, parmi les destinataires du message, certains sont effectivement clients de la banque en question, les escrocs parviennent parfois à obtenir les éléments demandés, soit parce que le client les divulgue comme demandé, soit parce que le courrier électronique envoyé contient en pièce jointe un cheval de Troie qui, dès l'ouverture du courrier, met en place sur l'ordinateur de la victime une fonction de captation des données confidentielles et les envoie, via un keylogger-logiciel qui enregistre les frappes au clavier sur des serveurs en général basés à l'étranger. Quelque temps après, le compte de ces clients est débité, à leur insu, par un virement bancaire à destination d'un tiers.

Le compte crédité est en fait celui d'une « mule », une personne ignorant tout de l'escroquerie qui se voit proposer par courriel de travailler pour une société internationale spécialisée dans les placements financiers qui la rémunérera par une commission de 5 à 10 % du montant des fonds transférés.

Cette mule reçoit donc les fonds et les transfère, via les services d'une entreprise financière spécialisée dans le transfert de fonds (ex. : Western Union), à un destinataire qui lui sera précisé ultérieurement. Ainsi, un étudiant qui a créé un faux site du Crédit Lyonnais, réussissant à voler une douzaine de personnes pour un montant de 20 000 €, a été condamné pour escroquerie par phishing plutôt que pour

contrefaçon – car les peines sont plus sévères – par le tribunal correctionnel de Strasbourg le 2 septembre 2004 (www.zdnet.fr).

Par ailleurs, il a déjà été considéré que se faire passer faussement pour un banquier a été réprimé sur le fondement de l'escroquerie (Crim. 16 mars 1987). Le code pénal de 1810 précisait que les manœuvres de l'escroc devaient être de nature « à persuader l'existence de fausses entreprises ».

Aujourd'hui, l'article 313-1 utilise une formule plus ramassée : les manœuvres doivent être susceptibles de tromper et être déterminantes dans la remise. Sauf imprudence manifeste de la victime (appréciation *in abastracto*), la caractérisation de manœuvres ne posera guère de difficultés dans l'hameçonnage, la remise de sommes par utilisation d'une carte bancaire ayant déjà été qualifiée d'escroquerie **(6)**.

Il convient, toutefois, de préciser, que l'escroquerie doit conduire à remettre « des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge ». La difficulté consiste ici dans une remise dématérialisée. Cette problématique a été résolue puisque la chambre criminelle assimile les données bancaires scripturales aux espèces.

En définitive, le droit successoral n'est pas à l'abri de la délinquance informatique ou internet. Les cas sont nombreux, les victimes aussi nombreuses.

Tentative. – La tentative d'escroquerie est punie par l'article 313-3 du Code pénal. S'ajoutent aux peines prévues par l'article 313-1 du même Code, sept peines complémentaires prévues par l'article 313-7, ainsi que l'exclusion des marchés publics pour une durée de cinq ans au plus, en vertu de l'article 313-8.

Personnes morales. – La responsabilité pénale des personnes morales est également prévue par l'article 313-9 du Code

pénal, dans les conditions prévues par l’article 121-2 du même Code.

C) L’abus de faiblesse et conséquences sur l’héritage

L’abus de faiblesse est également un type d’arnaque à l’héritage. Dans ce cas, un individu va profiter de la vulnérabilité d’une personne qui n’a pas conscience du préjudice subi, car elle n’a plus toutes ses facultés de discernement.

Cela peut être toute personne physique, qui agit sur la personne vulnérable pour lui faire modifier la clause bénéficiaire d’une assurance-vie par exemple, ou un testament pour les mettre à son profit ou à profit de tiers.

Cette pratique d’abus de faiblesse peut également se produire de manière virtuelle notamment à travers les réseaux sociaux en se faisant passer pour un membre de la famille par exemple. Cela rejoint le délit d’usurpation d’identité.

De manière pratique, si vous versez des frais, le cybercriminel ne donnera en général plus de nouvelle et sera susceptible d’utiliser la partie voire la totalité de l’héritage.

En effet, si vous donnez vos informations bancaires, une transaction d’argent sera fera de votre compte vers celui des escrocs (et non l’inverse) et votre contact ne donnera plus jamais de nouvelles.

Par conséquent, nous préconisons de ne jamais répondre aux messages virtuels en matière d’héritage, car en réalité il n’est question que d’arnaque à l’héritage.

III. Se protéger de la cybercriminalité en droit des successions

Il est nécessaire d'adopter les bonnes mesures pour se protéger contre les délits commis sur internet et grâce à internet. Pour ce faire, l'agence nationale de la sécurité des systèmes d'information (ANSSI) préconise des mesures simples pour que chacun contribue à cette protection. Parmi ces mesures :

-Installer un antivirus et un pare-feu et ainsi les mettre à jour régulièrement.

-Utiliser des mots de passe de qualité, difficiles à trouver par une tierce personne.

-Effectuer des sauvegardes régulières pour conserver une copie de vos données et, dans le cas d'une personne morale, assurer la continuité de votre activité

-Contrôler la diffusion d'informations personnelles, donc limiter la saisie de coordonnées personnelles et sensibles (ex : données bancaires.

-Il ne faut jamais fournir son code confidentiel de carte bancaire. La CNIL a émis en 2019, une recommandation limitant la conservation des numéros de carte par les sites marchands en ligne.

-Éviter de cliquer trop vite sur des liens placés dans un message. Ces liens peuvent, en effet, souvent contenir des codes malveillants.

SOURCES :

1. https://www.legifrance.gouv.fr/juri/id/JURITEXT000032083032?tab_selection=all&searchField=ALL&query=15-80.211&pa

ge=1&init=true
2. https://www.legifrance.gouv.fr/juri/id/JURITEXT000036779530?tab_selection=all&searchField=ALL&query=16-86961+&page=1&init=true
3. https://www.legifrance.gouv.fr/juri/id/JURITEXT000017736219?tab_selection=all&searchField=ALL&query=07-80576+&page=1&init=true
4. https://www.legifrance.gouv.fr/juri/id/JURITEXT000023549381?tab_selection=all&searchField=ALL&query=10-83180+&page=1&init=true
5. https://www.legifrance.gouv.fr/juri/id/JURITEXT000007626580?tab_selection=all&searchField=ALL&query=98-82816+&page=1&init=true
6. https://www.legifrance.gouv.fr/juri/id/JURITEXT000007573410