Les cyberfraudes : un fléau à combattre en urgence

Myriam QUEMENER
Magistrat honoraire
Docteur en droit

Les fraudes numériques se sont multipliées et surtout diversifiées avec le recours croissant à l'intelligence artificielle. Après avoir fait un point sur l'ampleur de cette délinquance, il conviendra de proposer des clefs et solutions afin d'éviter de tomber dans les pièges des cyberescrocs.

Le constat

L'IA Les cyberfraudes sont aujourd'hui en pleine expansion et visent aussi bien les entreprises, les collectivités territoriales et les citoyens. Les cybercriminels se sont adaptés à leurs cibles, avec par exemple du phishing bien réalisé et avec des logos parfaitement imités. Les cyberfraudes sont en fait une manifestation de la cybercriminalité qui est de plus en plus une délinquance financière.

Ainsi, malgré une baisse historique des fraudes à la carte bancaire, le montant total des escroqueries progresse en France, porté par l'essor rapide de nouvelles formes d'arnaques fondées sur la manipulation des consommateurs et les virements. Les fraudes par manipulation ont en effet représenté 245 millions d'euros au premier semestre 2025, en hausse de 37 %, selon les derniers chiffres de l'Observatoire de la sécurité des moyens de paiement de la Banque de France[1].

Récemment, la Fédération bancaire française (FBF) a publié une étude sur les Français et la cybersécurité chez les jeunes de 18 à 34 ans qui montre qu'ils sont les plus exposés aux fraudes aux moyens de paiement. Près de 2 jeunes sur 3 ont déjà été visés par une tentative d'arnaque, un niveau nettement supérieur à celui de l'ensemble de la population. Malgré cette vulnérabilité, ils se montrent moins inquiets, adoptent davantage de comportements à risque et restent moins bien sensibilisés aux enjeux de cybersécurité. Sur Internet, les moins de 35 ans constituent la cible privilégiée des fraudeurs. 63 % déclarent avoir déjà fait la cible d'une tentative d'arnaque, soit 9 points de plus que la moyenne nationale (54%). 14 % affirment d'ailleurs avoir été victimes d'une fraude aux données bancaires, contre 11% des Français. Cette exposition élevée s'explique par leur forte présence en ligne et la diversité des usages quotidiens : achats, streaming, réseaux sociaux.

La fraude en ligne ou la cyberfraude, correspond à diverses activités malveillantes réalisées par l'intermédiaire de plateformes numériques dans le but de tromper, de manipuler ou de voler des personnes, des organisations ou des institutions.

Cette forme de fraude s'appuie sur la technologie pour mener des activités frauduleuses, impliquant

[1] https://www.banque-france.fr/fr/actualites/communique-de-presse-de-lobservatoire-de-la-securite-des-moyens-de-paiement

souvent des transactions financières ou la fuite d'informations personnelles.

IA et fraudes numériques

L'IA générative change l'échelle des cyberfraudes avec des courriels et des sites frauduleux sans faute, automatisation des approches, personnalisation des arnaques grâce aux données publiques. Les deepfakes de voix et de visage permettent des usurpations d'identité crédibles, de la fraude au président aux ordres de virement urgents, en passant par la manipulation d'opinion. Les crypto-actifs, offrent aux fraudeurs des rails de paiement pseudonymes, accélérant escroqueries, ransomwares et « rug pulls » [2].

Le spoofing - affichage d'un numéro ou d'une identité légitime - amplifie l'effet de confiance et contourne les réflexes de vigilance. Les enjeux sont multiples : économiques, juridiques et humains. On constate la présence d'une véritable palette de scénarios, du phishing aux deepfakes, des faux ordres de virement aux arnaques d'investissement en crypto monnaies.

L'ouvrage « Cyberarnaques, comprendre, anticiper, se défendre » [3] qualifie les infractions qui s'y rattachent comme l'escroquerie, l'usurpation d'identité, le blanchiment, l'extorsion, l'accès frauduleux dans un système de traitement automatisé de données, et dresse le portrait des acteurs de la riposte.

Europol dans son dernier rapport 2025 (EU SOCTA), souligne aussi l'augmentation des cyberfraudes accentuée notamment par le recours à l'intelligence artificielle. L'explosion des cyberarnaques, au plan national et international, constitue un phénomène entrant dans le champ de la cybercriminalité, qui est de plus en plus une délinquance financière organisée. En outre, l'IA et les menaces hybrides, comme par exemple des opérations de désinformation, offrent désormais aux criminels des outils sophistiqués pour étendre leur influence, automatiser leurs activités et contourner les mesures de sécurité traditionnelles.

Ces menaces en constante évolution, obligent les forces de l'ordre à repenser leurs méthodes de lutte et à développer des réponses adaptées. Au vu du dernier rapport paru en 2025 de la plateforme cybermalveillance.gouv.fr, il apparaît, par exemple, que l'hameçonnage demeure la menace prédominante tout public confondu avec 1,9 million de personnes visées.

Les réponses juridiques aux fraudes numériques

Plusieurs qualifications juridiques peuvent être retenues pour sanctionner les fraudes numériques.

L'escroquerie

Citons tout d'abord l'escroquerie qui est fréquemment retenue dans les affaires de fraudes numériques. Elle est, selon l'article 313-1 du Code pénal, 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 5 ans d'emprisonnement et de 375 000 euros d'amende, voire de 10 ans d'emprisonnement et de 1 000 000 euros d'amende lorsqu'elle est commise en bande organisée. A noter que la tentative est également punissable.

[2] Un rug pull (littéralement « tirer le tapis ») désigne une fraude où les créateurs d'un projet crypto abandonnent un projet après avoir levé des actifs, laissant ses participants avec des tokens sans valeur.

[3] M. Quéméner, A. Köcke, « Cyberarnaques, comprendre, anticiper, se défendre », Lextenso, 2025

L'infraction est par exemple retenue lorsque l'informatique est le moyen de commission d'une fraude comme dans le cas d'un cyberdélinquant à la tête d'une vaste entreprise d'escroqueries à l'échelle internationale consistant, par une bande organisée, à mettre en ligne sur Internet des annonces de locations d'appartements ou de villas de vacances imaginaires afin de récupérer des arrhes versées par les candidats puis de disparaître (Cass. crim., 13 sept. 2011, nº 11-84.658). La qualification d'escroquerie en bande organisée est fréquemment utilisée pour sanctionner de fausses ventes sur des sites d'enchères sur internet (Cass. crim., 21 mars 2012, nº 11-84.437).

Le blanchiment

L'article 324-1 du Code pénal définit le délit de blanchiment comme « le fait de faciliter, par tout moyen, la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect. Constitue également un blanchiment le fait d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit ». L'infraction de blanchiment, recouvre tant l'intégration du produit d'une infraction dans le circuit financier légal, que la facilitation de ce délit.

Les cybercriminels sont également en lien étroit avec les opérateurs du blanchiment, qui utilisent aussi bien les systèmes traditionnels de la criminalité organisée que les crypto-actifs. Tracfin (Traitement du renseignement et action contre les circuits financiers clandestins) considère les risques élevés que présentent les crypto-actifs en termes de blanchiment de capitaux. Ces risques, identifiés, sont désormais avérés et tiennent « principalement à l'anonymat, en particulier pour les blockchains délibérément développées afin d'effacer la traçabilité des transactions » ainsi qu'aux plateformes proposant des services d'échange de crypto-actifs contre d'autres crypto actifs (services de change dits crypto to crypto).

L'usurpation d'identité

Certains cybercriminels se font passer pour des sociétés autorisées qui reproduisent leur logo, site internet ou documents commerciaux, et insistent souvent pour que vous vérifiiez leur présence sur les registres officiels afin de vous prouver leur « bonne foi ». Ils n'hésitent pas aussi à utiliser les logos d'autorités publiques françaises ou étrangères pour se montrer dignes de confiance. La différence entre leur site et celui qu'ils ont usurpé est parfois minime (par exemple quelques détails comme le changement d'une lettre dans le nom ou l'adresse du site ou d'une adresse mail).

La seule vérification de la présence d'une société sur les registres officiels n'est pas suffisante pour éviter les arnaques. Le délit d'usurpation d'identité, prévu par l'article 226-4-1 du Code pénal sanctionne de 15 000 euros d'amende et de 1 an d'emprisonnement une telle usurpation s'il en résulte une atteinte à la tranquillité, à l'honneur ou à la considération. Par exemple, Infogreffe alerte sur une augmentation importante des fraudes au Kbis. Les préjudices dépassent souvent les 10 000 euros. Le Kbis est facile à se procurer et à modifier. Les entreprises doivent organiser leur veille et leur sécurité documentaires[4].

L'extorsion

L'article 312-1 du Code pénal définit l'extorsion comme « le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation

[4] V. F. Mattatia, L'usurpation d'identité sur internet dans tous ses états : Rev. sc. crim. 2014, p. 331, spéc. p. 336 et 337. 99 Cyberarnaques Extorsion

d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque ». Par exemple, dans le cas d'un rançongiciel, l'extorsion de fonds, punie de 7 ans d'emprisonnement et de 100 000 euros d'amende peut être retenue. Lorsqu'elle est commise en bande organisée, elle est sanctionnée de 20 ans de réclusion criminelle et de 150 000 euros d'amende (C. pén., art. 312-6).

L'accès frauduleux dans un système de traitement automatisé de données

Par ailleurs, la loi nº 88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain a introduit les articles 323-1 et suivants dans le Code pénal qui répriment le mode opératoire permettant la réalisation des fraudes numériques. Ainsi, le Code pénal, notamment ses articles 323 1 à 323-7, traite des délits d'accès frauduleux à un système informatique, d'interception de données, et de modification de données.

Des jurisprudences de plus en plus affinées

Les fraudes au paiement en ligne, compte tenu de leur ampleur, donnent lieu à des jurisprudences de plus en plus affinées.

Si l'utilisateur signale un paiement non autorisé (C. mon. fin., art. L. 133-24), le prestataire de services de paiement a l'obligation de le rembourser (C. mon. fin., art. L. 133-18). En effet, le prestataire doit : rembourser immédiatement l'opération non autorisée ; et, le cas échéant, rétablir le compte débité dans l'état dans lequel il se serait trouvé si l'opération non autorisée n'avait pas eu lieu. Le prestataire doit empêcher toute utilisation de la carte de paiement après avoir été informé de sa perte, de son vol, de son détournement ou de toute utilisation non autorisée de la carte ou des données qui lui sont liées (C. mon. fin., art. L. 133-17).

En cas de fraude ou de négligence grave de l'utilisateur, l'article L. 133-19 IV du Code monétaire et financier ne dispense le prestataire de services de paiement qu'en cas de négligence grave ou d'agissement frauduleux de son client. En effet, selon l'article L. 133-16, alinéa 1 du Code monétaire et financier, « Dès qu'il reçoit un instrument de paiement, l'utilisateur de services de paiement prend toute mesure raisonnable pour préserver la sécurité de ses données de sécurité personnalisées ». En outre, selon l'article L. 133-19 du même code, « Le payeur supporte toutes les pertes occasionnées par des opérations de paiement non autorisées si ces pertes résultent d'un agissement frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave aux obligations mentionnées aux articles L. 133-16 et L. 133 17 du Code monétaire et financier ». Le payeur a donc une certaine responsabilité à porter vis-à-vis des paiements en ligne qu'il effectue.

Cependant, une simple négligence du client ne suffit pas à la banque pour se dispenser de son obligation de remboursement. C'est au prestataire de services de paiement de rapporter la preuve de la négligence grave, et non au client de démontrer qu'il n'a pas commis de faute (C. mon. fin., art. L. 133-23). En effet, la Cour de cassation (18 janv. 2017, nº 15-18.102) a établi qu'il appartient au prestataire de services bancaires « de rapporter la preuve que l'utilisateur, qui nie avoir autorisé une opération de paiement, a agi frauduleusement ou n'a pas satisfait intentionnellement ou par négligence grave à ses obligations ». La banque ne peut pas se baser sur des suppositions pour refuser le remboursement des sommes indûment débitées. En effet, cette preuve ne peut pas consister en la simple déduction du fait que le titre de paiement ou les données confidentielles aient été utilisés pour effectuer des achats frauduleux.

Une jurisprudence spécifique existe concernant l'obligation de remboursement des prestataires de services de paiement en matière d'hameçonnage, Il

existe beaucoup de contentieux en matière d'hameçonnage où les prestataires de services de paiement invoquent un non-respect des obligations de l'utilisateur concernant la protection de ses données de sécurité personnalisées pour ne pas rembourser celui-ci selon l'article L. 133-18 du Code monétaire et financier lorsque l'escroc utilise de manière non-autorisée les données de paiement obtenues frauduleusement.

Il faut aussi signaler que le législateur vient encore de renforcer la lutte contre la fraude bancaire. Ainsi, la loi n° 2025-1058 du 6 novembre 2025 visant à renforcer la lutte contre la fraude bancaire consolide en la matière des dispositifs existants, et inaugure un nouveau fichier destiné à répertorier les IBAN douteux[5].

Conseils et informations des victimes de cyberfraudes

Il est essentiel de plaider pour une coopération renforcée entre sphères publique et privée avec par exemple un partage de signaux, des plateformes sécurisées, une harmonisation transfrontalière, afin de poursuivre efficacement les fraudeurs et de restaurer la confiance numérique.

Ensuite, le message principal consiste à informer sur les modes opératoires et à se méfier des annonces alléchantes. Il est préférable d'aller sur les sites connus et ne pas cliquer sur des mails d'inconnus. Pour toutes celles et ceux qui portent la responsabilité du numérique, l'essentiel est d'entretenir une connaissance à jour des fraudes et de leurs évolutions.

La fréquentation de la plateforme Cybermalveillance.gouv.fr[6] a enregistré une hausse significative (+ 47 %) avec 5,4 millions de visiteurs. La forte augmentation de l'audience de la plateforme a été largement portée par les nombreuses violations de données personnelles massives et récentes (Free, France Travail, prestataires de mutuelles de santé, enseignes de la distribution...) ainsi que par les vagues importantes et permanentes de SMS ou mails d'hameçonnage de tout type (livraison de colis, infraction routière...), pour lesquelles les publics de Cybermalveillance.gouv.fr sont venus s'informer et chercher de l'assistance suite à tous ces types de fraudes. Cette plateforme propose des contenus très pédagogiques aussi bien pour les particuliers que pour les entreprises, en particulier sur les méthodes des fraudeurs et les démarches à effectuer pour les victimes de tels agissements et notamment le dépôt de plainte.

Le lancement du 17Cyber à la fin de l'année 2024, équivalent numérique pour les actes de cybermalveillance de l'appel 17, incarne ce rôle prépondérant du GIP, guichet d'entrée pour les victimes d'infractions numériques. Le ministère de l'Intérieur, accompagné de la police et de la gendarmerie nationales, a lancé le service en ligne 17Cyber. Orchestré par la plateforme gouvernementale Cybermalveillance, il établit un diagnostic lorsqu'un utilisateur a été victime d'une attaque numérique. Certains sites Internet partenaires (mutuelles, marketplaces...) proposeront ou ont déjà intégré un module d'accès à la plateforme sur leur page d'accueil. Il est un prolongement numérique du numéro 17 (police secours), dédié aux victimes de cyberdélinquance.

Présenté par Cybermalveillance comme « un guichet unique de la cybersécurité », voué à devenir un réflexe pour la population, il oriente les citoyens vers les démarches à entreprendre, les plateformes éventuelles vers lesquelles se tourner (PHAROS, THESEE...) et les interlocuteurs à contacter. La plateforme, disponible en permanence, fournit un

[5]https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000052533262

[6] https://www.cybermalveillance.gouv.fr/

diagnostic grâce à un questionnaire. L'internaute doit tout d'abord préciser son statut (particulier, entreprise, administration...), identifier le problème (SMS reçu, téléphone mobile, site Internet...) puis les caractéristiques de l'acte de malveillance (suspicion de la présence d'un virus, piratage de compte, contenu du message malveillant...). Une fois ces réponses validées, le 17 Cyber émet son diagnostic, tel le hameçonnage, un virus, etc. Il dispense ensuite des conseils. La page de résultat décline en effet diverses actions visant à trouver une solution technique mais aussi à se défendre à la suite d'une attaque en déposant plainte par exemple, en changeant de mot de passe, en signalant les messages suspects au 33700, ou encore en faisant appel à un prestataire extérieur pour faire vérifier la qualité de son matériel informatique.

Au vu de ce constat inquiétant, il apparaît urgent de créer une véritable politique publique et pénale de lutte contre ce fléau qui atteint la société dans son ensemble, causant souvent des préjudices très importants.