CREDOC

CAHIER DE RECHERCHE

L'escroquerie en ligne et à la téléphonie en France

Ampleur du phénomène et profils des victimes

Kelly Perrotte
Patricia Croutte
Lucie Brice Mansencal
Sandra Hoibian

Cette recherche a bénéficié d'un financement au titre de la subvention recherche attribuée au CRÉDOC

DÉCEMBRE 2021

CRÉDOC

CENTRE DE RECHERCHE POUR L'ÉTUDE ET L'OBSERVATOIRE DES CONDITIONS DE VIE

L'escroquerie en ligne et à la téléphonie en France : ampleur du phénomène et profils des victimes

Kelly Perrotte, Patricia Croutte, Lucie Brice Mansencal et Sandra Hoibian

Cahier de recherche n°354 - Décembre 2021

142 rue du Chevaleret – 75013 Paris – www.credoc.fr

RÉSUMÉ

Avec le recours croissant aux nouvelles technologies de l'information et de la communication et l'amplification de l'usage d'Internet, la population est confrontée à une nouvelle forme de criminalité : la cybercriminalité, au sein de laquelle figure en bonne place l'escroquerie en ligne et par téléphone. La présente recherche brosse un état des lieux du phénomène à partir des différentes sources disponibles et montre qu'une personne sur deux est exposée à ce type de méfaits, et autour d'un million de personnes perd des deniers chaque année suite à des arnaques en ligne ou par téléphone. Probablement en liaison avec leur posture de défiance envers autrui et leur culture des données personnelles, les Français se montrent plus sensibles à ces questions que la moyenne des Européens. Ils se disent plus inquiets et plus souvent victimes de ces forfaitures. Les risques d'usurpation d'identité, d'escroquerie bancaire ou de piratage de son réseau social les inquiètent tout particulièrement. Moins fréquents que d'autres, ces types d'attaques sont en effet plus lourds de conséquences durables dans un monde où l'identité numérique devient un enjeu central. Mais nos concitoyens ne semblent pas prêts pour autant à renoncer à la gratuité des usages ou à brider ces derniers en échange de garanties plus fortes. Ils tentent de se protéger en mobilisant différentes précautions. Les publics qui se protègent le plus sont aussi mécaniquement le plus souvent victimes d'arnaques en ligne, car ils sont les plus actifs sur la toile.

Le phénomène des escroqueries en ligne augmente à mesure que la société se digitalise. Et de ce fait, la pandémie a récemment étendu le champ des publics concernés, invitant donc à se saisir plus particulièrement de ce phénomène à la fois pour le mesurer et pour accompagner ces nouveaux utilisateurs de la toile.

Table des matières

INTRODUCTION

L'escroquerie n'a pas attendu Internet. L'histoire regorge d'exemples célèbres : de l'affaire du Collier de la Reine en 1785 qui conduisit le Cardinal de Rohan à la Bastille, en passant par la « vente » de la Tour Eiffel par Victor Lustig dans les années 20, jusqu'à l'affaire Madoff, du nom de l'homme d'affaires condamné en 2009 à 150 ans de prison pour avoir mis en place un système de Ponzi[1]… Les techniques, multiples, sont si bien rodées, qu'elles ont pu être baptisées par des noms évocateurs comme ceux de « La prisonnière espagnole » (qui consiste à envoyer un message demandant de l'argent pour venir en aide à une princesse/personne emprisonnée, dans le besoin, etc) ou encore, de la « vente pyramidale » dans laquelle le profit ne provient pas de la vente de prétendus produits mais du recrutement de nouveaux membres…

*Il y a escroquerie lorsqu'une personne se fait remettre un bien, de l'argent ou se fait fournir un service **en trompant** sa victime. L'auteur des faits exploite la victime en dissimulant la vérité. La victime donne son bien ou son argent **volontairement**, car elle a été trompée sur les intentions de l'auteur.*

La tromperie peut notamment porter sur les points suivants :

- *Nom (usage d'une fausse identité)*
- *Faux état (en prétendant être un professionnel du droit ou de la santé ou en se servant d'une fausse situation de famille comme se dire veuf alors que l'époux est toujours vivant)*
- *Abus de la confiance attachée à certaines professions, certaines fonctions (maire, délégué syndical, président d'association...)*

Faux document (un faux diplôme ou une fausse facture par exemple)

Source : https://www.service-public.fr/particuliers/vosdroits/F1520

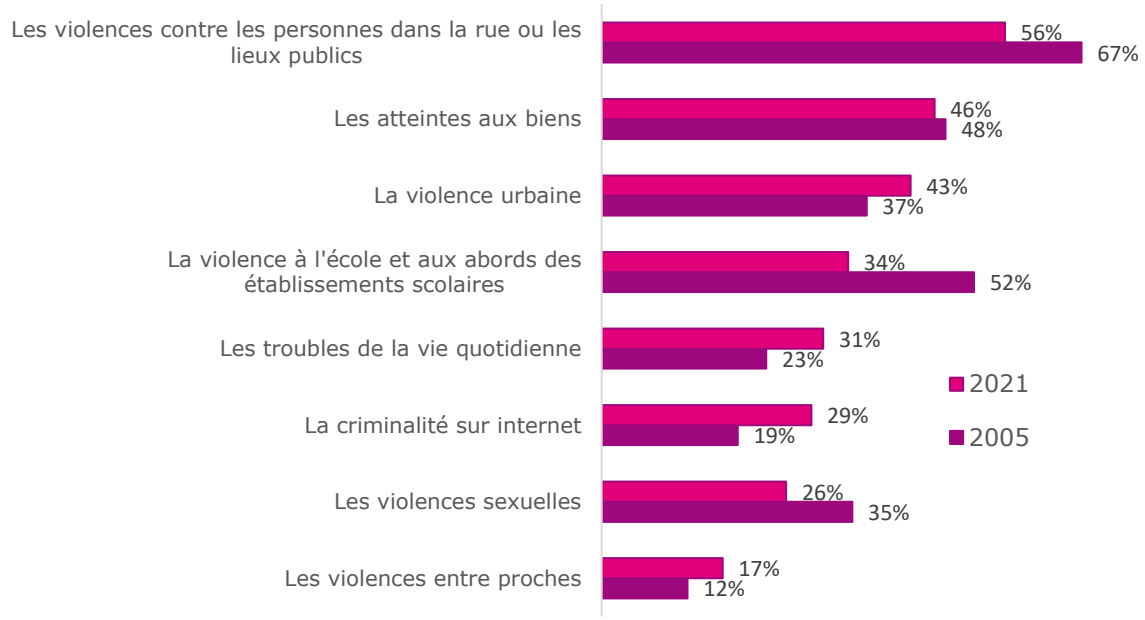
La digitalisation du monde a, sans surprise, offert de nouveaux espaces aux cupides et malhonnêtes, avec toutefois quelques caractéristiques propres aux mondes numériques :

- La facilité à **internationaliser** les escroqueries et donc une complexification des démarches pour obtenir réparation.
- La **répartition de plus en plus fréquente d'une chaine de responsabilité** entre plusieurs acteurs, aussi appelée *dropshipping* (séparation des fonctions de commercialisation d'une plateforme, de gestion du stock et de l'expédition de la marchandise assumée par le fournisseur), limitant la possibilité de recours des consommateurs.
- La **désintermédiation** (vente de pairs à pairs) qui court-circuite la fonction de garantie que pouvaient réaliser les anciens tiers de confiance. Les systèmes de notes ou avis d'autres consommateurs cherchent le plus souvent à jouer ce rôle de garantie et sécurisation des transactions, mais offrent beaucoup moins de prise à des recours, peuvent également être l'objets de faux, difficiles à identifier.
- Une plus **grande facilité à se faire passer pour un autre**, en copiant les écrits, les logos et autres signes.
- Une **plus grande difficulté à identifier les auteurs** des forfaiteries.

Outre la numérisation à grands pas des différentes dimensions de nos vies (travail, loisirs, vie affective et relationnelle, santé, etc), **ce caractère insaisissable et démultiplié** des possibilités de malversations sur Internet explique probablement, qu'en une quinzaine d'années, les inquiétudes concernant les violences dans les espaces publics, les rues (-10 pts), à l'école ou autour des établissements scolaires (-18 points), aient cédé du terrain à celles **portant sur la criminalité sur internet (+10 points)** (Figure 1).

[1] Le système de Ponzi désigne l'obtention d'argent en promettant à des investisseurs des rendements mirobolants obtenus en réalité par les investissements de nouveaux crédules.

Figure 1 - Dans votre vie quotidienne, quels sont, parmi les faits suivants, les trois qui provoquent en vous la plus forte inquiétude ?



Source : CRÉDOC, enquêtes Conditions de vie et aspirations, 2005 et 2021.

Les escroqueries en ligne ne constituent évidement qu'une partie de ce qui est parfois appelé la « cybercriminalité », c'est-à-dire l'« ensemble des infractions pénales commises sur les réseaux de télécommunication, en particulier Internet[2] ». La cybercriminalité regroupe une diversité d'infractions telles que les cyberattaques empêchant les citoyens d'accéder à des services en ligne, la diffusion de contenus pédopornographiques, les extorsions de fonds, la fraude à la carte bancaire… Dans ce cahier de recherche, nous porterons une attention particulière aux escroqueries opérées sur Internet et par téléphone appelées également **« escroqueries en ligne et à la téléphonie »** en tentant d'apporter quelques éléments de réponse à deux problématiques :

Quelle proportion de la population française a été confrontée à ce type de malversations dans un **contexte pandémique d'accélération et de diffusion des usages numériques ?** Ce cahier de recherche propose ainsi de mettre en regard les données provenant de différentes sources statistiques afin d'approcher l'ampleur de ce phénomène en France.

Parmi les différents leviers de politiques publiques pour limiter les impacts de ce phénomène, figurent en bonne place **la prévention et l'information** des individus pour les inciter à **prendre des précautions.** Dans quelle mesure la population française a-t-elle acquis des réflexes en la matière ? Tous les groupes sociaux sont-ils aussi experts en la matière ? Les précautions aident-elles à déjouer les pièges qui leur sont tendus sur la toile ? Autrement dit : les personnes cibles des escroqueries en ligne et/ ou à la téléphonie sont-elles celles qui prennent le moins de précautions ?

Pour répondre à ces deux problématiques, nous nous appuyons sur les chiffres de la statistique administrative : l'*état 4001*, l'enquête *CVS* parue en 2019 et sur les résultats du *Rapport* de l'Observatoire des moyens de paiements publié en 2020. Les données du CRÉDOC produites pour le CGE, l'ARCEP et la mission Société Numérique dans le cadre des dernières enquêtes *Baromètre du*

[2] « Cybercriminalité » dans Dictionnaire Larousse, 2021.

Numérique élargissent le spectre de l'analyse. Elles permettent de mieux comprendre le lien qu'entretiennent les Français avec l'enjeu de la protection des données et révèlent dans quelle mesure ces derniers sont prêts à changer leurs comportements pour s'assurer de leur sécurité. Par ailleurs, les résultats de l'Eurobaromètre 499[3] apportent un éclairage complémentaire aux précédentes sources d'information, notamment sur la question de la sécurité des données personnelles et sur l'exposition des Français aux escroqueries en ligne et à la téléphonie. Enfin, les travaux de Nicolas Auray sur le spam[4] et ceux de Bilel Benbouzid et Sophie Peaucellier sur les arnaques sur Internet constituent à ce jour, les apports sociologiques principaux sur le sujet. Ce cahier de recherche repose ainsi sur une analyse croisée de données objectives et de données fondées sur l'opinion des enquêtés et contribue à étoffer nos connaissances sur un sujet majeur mais jusqu'ici, peu exploré.

[3] Commission Européenne. Spécial Eurobaromètre 499 : *Europeans' attitudes towards cyber security*, publié en janvier 2020

[4] Auray, Nicolas. « Manipulation à distance et fascination curieuse. Les pièges liés au spam », *Réseaux,* vol. 171, no. 1, 2012, pp. 103-132.

MÉTHODOLOGIE

La difficulté rencontrée est l'absence, à ce jour, d'étude statistique portant exclusivement sur ce sujet. Les quelques données dont nous disposons sur l'escroquerie en ligne et à la téléphonie proviennent de diverses sources recouvrant des champs d'analyse différents. Certaines études se concentrent sur un type d'escroquerie en ligne particulier comme la fraude bancaire quand d'autres étudient les escroqueries perpétrées en ligne, par téléphone mais également en magasin ou chez les particuliers.

Le tableau ci-dessous détaille les caractéristiques des sources statistiques utilisées dans ce cahier de recherche.

L'état 4001

L'*état 4001* révèle chaque année l'ensemble des crimes et délits enregistrés par les services de police et de gendarmerie. Ces crimes et délits sont répertoriés dans plus d'une centaine de catégories. L'escroquerie en ligne et à la téléphonie serait ainsi comptabilisée dans les deux catégories suivantes « Escroqueries et abus de confiance » et « Falsification et usage de cartes de crédit ».

Cette source administrative permet seulement de connaître **les infractions portées à la connaissance des autorités de police et de gendarmerie et qualifiées de « délits » ou de « crimes » à la suite d'une plainte.** Par conséquent, les données de *l'état 4001* sont largement sous-représentatives du phénomène.

***Les chiffres :* 255 000 victimes « d'escroqueries et abus de confiance » et 66 300 victimes de « falsifications et usages de carte de crédit » ont été enregistrées en 2019[5].**

L'enquête de victimation, dite Cadre de Vie et sécurité (CVS)

L'*enquête de victimation* dite *Cadre de Vie et sécurité (CVS)* complète les chiffres de l'*état 4001* : elle révèle les « arnaques » dont se déclarent victimes les répondants, qu'ils aient porté plainte ou non. Depuis 2009, elle intègre des questions relatives aux atteintes sur Internet et notamment sur les arnaques et les débits frauduleux. Dans cette enquête, l'escroquerie en ligne et à la téléphonie est étudiée dans deux chapitres : celui sur les « Arnaques » et celui sur les « Escroqueries bancaires ».

Les **« arnaques »** désignent toutes les escroqueries réalisées sur Internet, par téléphone, par courrier ou par contact direct à l'exception des délits frauduleux sur les comptes bancaires.

Les **« débits frauduleux » ou « escroqueries bancaires »** sont « les retraits ou paiements effectués sur le compte bancaire des victimes sans leur accord en utilisant des informations personnelles comme un numéro de carte bancaire obtenu illégalement. Ces débits frauduleux peuvent notamment avoir lieu sur Internet. Ce type d'atteinte exclut les litiges avec des créanciers, les débits résultant du vol ou de la perte d'un chèque ou d'une carte ainsi que les cas d'extorsion des données confidentielles par la violence ou la menace[6] ».

***Les chiffres :* 1,2 million de personnes déclarent avoir été victimes d'une « arnaque » et 1,3 million d'une « escroquerie bancaire » en 2018[7].**

Population étudiée : 14 ans ou plus résidant en France métropolitaine.

L'enquête *CVS* est réalisée depuis 2007 par l'Institut national de la statistique et des études économiques (Insee), en partenariat avec l'Observatoire national de la délinquance et de la réponse pénale (ONDRP) et avec le Service statistique ministériel de la sécurité intérieure. L'enquête est menée en face-à-face auprès d'un échantillon de 20 000 à 25 000 ménages « ordinaires » - c'est-à-dire hors ménages vivant en collectivité (foyers, prisons, hôpitaux…).

[5] Service statistique ministériel de la sécurité intérieure (SSMSI), bases des crimes et délits enregistrés par la police et la gendarmerie, 2019.

[6] Insee-ONDRP-SSMSI. « Escroqueries Bancaires », Enquête de victimation, *Cadre de vie et sécurité*, 2019.

[7] Insee-ONDRP-SSMSI. Enquête de victimation, *Cadre de vie et sécurité*, 2019.

Le Rapport annuel de l'Observatoire des moyens de paiement

Le *Rapport annuel de l'Observatoire des moyens de paiement* publié par la Banque de France nous livre une vision limitée de l'ampleur de l'escroquerie sur Internet et à la téléphonie en France. Elle se concentre en effet sur l'escroquerie bancaire uniquement.

L'escroquerie bancaire en ligne ou à la téléphonie correspond au **« paiement par carte à distance (par téléphone, courrier ou sur Internet)** », au **« virement »** et au **« prélèvement »** sans le consentement du détenteur du compte bancaire.

Les chiffres : En 2020, 95% des escroqueries bancaires (en volume) ont été commises via un paiement par carte et 3% par virement[8].

Les données de fraude à la carte de paiement sont collectées par l'Observatoire auprès des membres du Groupement des cartes bancaires CB, de MasterCard et de Visa Europe France et des principaux émetteurs de cartes privatives actifs en France. Les données de fraude au virement ou prélèvement sont fournies par la Banque de France et proviennent des déclarations réglementaires annuelles de fraude qui lui sont faites par les prestataires de services de paiement agréés.

Le Baromètre du numérique

Le *Baromètre du Numérique* est une enquête réalisée par le CRÉDOC depuis 2000 portant sur les pratiques numériques d'achats et leur utilisation par la population.

Les chiffres : Entre 2016 et 2020, le nombre de personnes achetant plusieurs fois par an sur Internet a augmenté de 8 points[9].

Population étudiée : 12 ans ou plus résidant en France métropolitaine.

Le *Baromètre du Numérique* présente les résultats des questions insérées dans l'enquête « Conditions de vie et Aspirations des Français » réalisée deux fois par an par le CRÉDOC (trois fois depuis 2020). Jusqu'en 2019, les résultats s'appuient sur une enquête menée en « face-à-face » : le questionnaire est administré au domicile de la personne, auprès d'un échantillon représentatif de la population française âgée de 12 ans ou plus (2 200 personnes environ). En 2020, en raison de la Covid-19, l'enquête a été menée via un recueil en mix mode : à la fois en ligne mais aussi par téléphone afin d'interroger la juste proportion de personnes ne disposant pas d'une connexion internet à leur domicile. L'échantillon ; pour l'enquête 2020, était de 4 029 individus.

L'Eurobaromètre spécial 499, Europeans' attitudes towards cyber security

L'Eurobaromètre spécial 499 porte sur le rapport qu'entretiennent les Européens avec la cybersécurité. Les résultats de l'enquête ont été publié en janvier 2020.

Les situations suivantes sont présentées dans cette enquête, comme différentes formes de cybercriminalité : l'usurpation d'identité à la suite du vol des identifiants, la fraude bancaire en ligne, l'infection des appareils numérique par un logiciel malveillant (virus), le piratage d'un réseau social ou une adresse e-mail, la réception d'e-mail ou appels frauduleux, la demande d'argent en échange de la récupération du contrôle de l'appareil, l'escroquerie à l'achat d'un bien sur Internet. Dans ce cahier de recherche, nous considérons toutes ces situations comme une forme d'escroquerie en ligne ou à la téléphonie.

Les chiffres : En 2019, 77 % des Français et 66 % des Européens étaient inquiets d'être confrontés au vol de leurs identifiants ou de l'usurpation de leur identité sur Internet[10].

Population étudiée : 15 ans ou plus résidant en France métropolitaine.

L'enquête a été réalisée en France par Kantar Public France, en face-à-face auprès d'un échantillon de 1 000 personnes (passation en octobre 2019).

---

[8] Banque de France. Observatoire des moyens de paiements, *Rapport,* 2020.
[9] CRÉDOC, *Baromètre du numérique*, édition 2021.
[10] Commission Européenne. Spécial Eurobaromètre 499 : *Europeans' attitudes towards cyber security*, janvier 2020.

LÉXIQUE

COOKIES : données transmises par un site web ou une application, pour être stockées sur la machine et récupérées par le serveur à la connexion suivante. En entrant sur un site web ou une application, l'utilisateur est invité à accepter ou refuser les cookies.

DROPSHIPPING : le vendeur n'est en charge que de la commercialisation et de la vente du produit. C'est le fournisseur partenaire qui se charge de la gestion du stock et de l'expédition de la marchandise au consommateur final. Le consommateur n'a généralement pas connaissance de l'existence et du rôle incombant au fournisseur[11]. Cette dissociation des fonctions peut occasionner une difficulté pour le consommateur à faire valoir ses droits en cas de produit ou service manquant, défectueux, abusif.

HAMEÇONNAGE (*phishing* en anglais) consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance (personne, banque, administration, etc.) afin de lui soutirer des informations personnelles tels que ses données bancaires, ses identifiants et mots de passe.

INGÉNIERIE SOCIALE : « La fraude par ingénierie sociale est un terme générique qui désigne les escroqueries orchestrées par les criminels qui abusent de la confiance d'une personne afin d'obtenir de l'argent ou des informations confidentielles leur permettant de commettre une autre infraction[12] ».

RANÇONGICIEL : (*ransomware* en anglais) désigne l'utilisation d'un programme malveillant pour extorquer de l'argent. Les victimes sont tenues de donner une rançon à l'auteur de l'attaque afin de récupérer les données personnelles de son appareil).

SPAM : la CNIL défini « le *spamming* ou *spam* » comme « l'envoi massif et parfois répété, des courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière dans les espaces publics de l'Internet, forums de discussion, liste de diffusion, annuaires, sites web, etc ». Pour Nicolas Auray[13], le spam est le résultat d'une division stricte du travail entre quatre principaux acteurs. L'annonceur est la personne souhaitant vendre un produit en passant par des méthodes de prospection commerciale illégale. Elle se dirige pour cela vers un hacker qui vole une base de données commerciales ou la rachète à un autre piratage. Le promoteur rédige le message tout en assurant qu'il ne sera pas bloqué par des filtres « anti-spams ». Enfin, le coordinateur du groupe récupère et redistribue les profits générés.

[11] Dropshipping, gare aux mirages ! | economie.gouv.fr
[12] « Ingénierie sociale », INTERPOL, 2021.
[13] Auray, Nicolas. « Manipulation à distance et fascination curieuse. Les pièges liés au spam », *Réseaux,* vol. 171, no. 1, 2012, p. 109.

CHAPITRE 1 : L'ESCROQUERIE EN LIGNE ET À LA TÉLÉPHONIE : UNE PRATIQUE ILLICITE TRÈS RÉPANDUE QUI OCCASIONNE DES PERTES D'ARGENT POUR PRÈS D'UN MILLION DE PERSONNES PAR AN

Entre 1.7% et 2.3% de la population a perdu de l'argent

Comme souvent, différentes acceptions du terme « escroquerie » peuvent co-exister. Certaines sources préfèrent à la terminologie d'escroquerie, le terme « d'arnaque », d'autres celui de « fraude » quand certaines l'associent à un ensemble bien plus large qui est celui de la cybercriminalité.

Dès lors, il convient de définir strictement « l'escroquerie en ligne et à la téléphonie ». D'abord, l'escroquerie sur Internet désigne, selon les mots de Bilel Benbouzid et Sophie Peaucellier, **« toute forme de soustraction frauduleuse de bien d'autrui opérée sur ou par le web, souvent sous la forme de débits effectués sur un compte bancaire, sans l'accord de son propriétaire ou en procédant par une technique d'ingénierie sociale**[14] ». Ces escroqueries en ligne s'opèrent « par contact en ligne » ou par « courrier électronique[15] ». Dans le premier cas, l'escroquerie consiste en l'achat fictif ou défectueux d'un service, d'un bien ou d'un abonnement sur un site Internet. Dans le second cas, il s'agit de situations plus variées : une fausse demande d'aide, une fausse proposition amoureuse, une proposition d'achat d'un antivirus après avoir déclaré l'ordinateur de la victime infecté… Ensuite, l'escroquerie à la téléphonie désigne toute atteinte impliquant une perte financière ou d'informations personnelles réalisée par le biais du téléphone mobile ou fixe. Concrètement, les Français peuvent recevoir des appels ou des SMS frauduleux cherchant à récupérer leurs données personnelles, les inciter à contacter des numéros surtaxés ou bien leur vendre un abonnement ou un service fictif. L'escroquerie en ligne ou à la téléphonie prend ainsi plusieurs formes qui ne cessent de se renouveler.

D'après l'enquête *Cadre de vie et sécurité,* **1,2 million de personnes** âgées de 14 ans ou plus et résidant en France métropolitaine ont subi une « anarque » et en ont effectivement été **victimes (produit ou service non livré ou rendu, chantage, extorsion ou fausse romance, qualité ou quantité non conforme, coût supplémentaire imprévu, autres)** au cours de l'année 2018. Ce chiffre intègre uniquement les personnes qui ont subi une **arnaque leur ayant coûté de l'argent.** C'est un des **types de criminalité les plus répandus.** On dénombre par exemple, autant de personnes victimes de vol ou de tentative de vol sans menace ni violence, que de victimes d'escroquerie en ligne ou à la téléphonie[16].

72% de ces arnaques ayant touché au porte-monnaie des ménages concernent une escroquerie en ligne ou à la téléphonie (Figure 2).

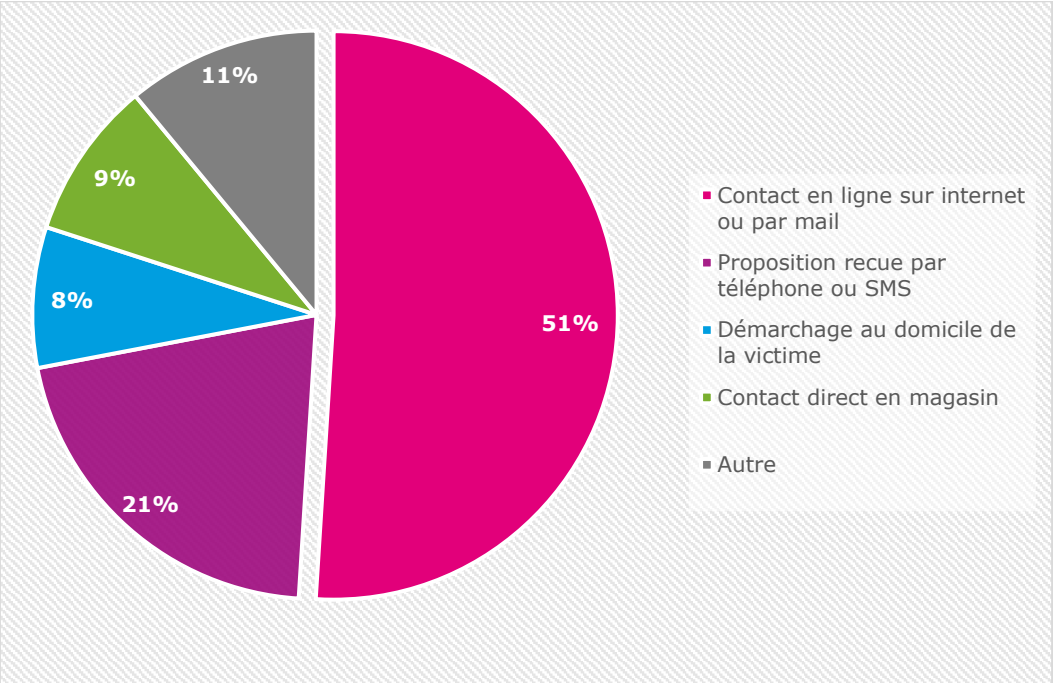
- Dans 51% des cas, la victime s'est fait tromper sur Internet, via un site en ligne ou à suite de la réception d'un mail frauduleux.
- Dans 21% des autres cas, l'auteur de l'escroquerie est entré en contact avec sa victime par téléphone ou SMS.

[14] Benbouzid, Bilel, et Sophie Peaucellier. « L'escroquerie sur Internet. La plainte et la prise de parole publique des victimes », *Réseaux*, vol. 197-198, no. 3-4, 2016, p. 139.

[15] Institut national des hautes études de la sécurité et de la justice. D'après l'enquête *Cadre de Vie et Société*, *Note de n°50 de* l'Observatoire national de la Délinquance et des réponses pénales, septembre 2020.

[16] Insee-ONDRP-SSMSI. « Vol sans menace ni violence », Enquête de victimation*, Cadre de vie et sécurité*, 2019.

Figure 2 – Type et localisation des arnaques en France



Source : Insee-ONDRP-SSMSI. « Arnaques », Enquête de victimation, *Cadre de Vie et sécurité*, 2019.
Lecture : En 2018 et en 2017, 8% des arnaques en France ont été menées au domicile de la victime.

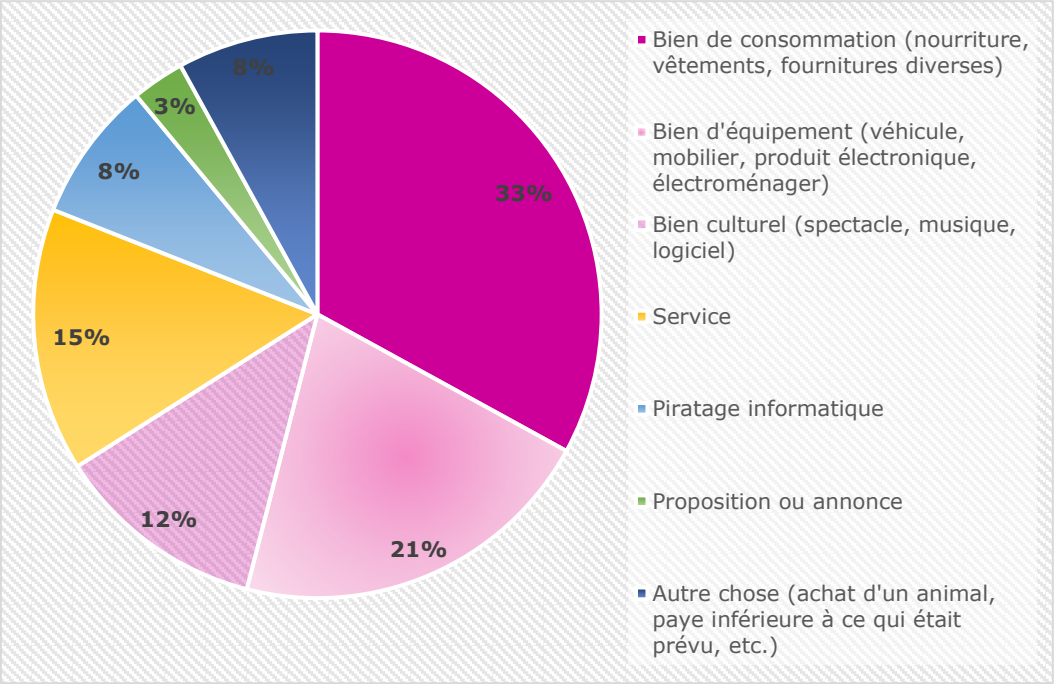
A titre de comparaison, selon la même enquête, en moyenne sur la période 2016-2019 (seuls chiffres disponibles), seules 16% des menaces en dehors du ménage et 6 % des injures en dehors du ménage sont exprimées au téléphone ou par mail, courrier, réseaux sociaux. **L'escroquerie est donc un type de criminalité qui prospère particulièrement sur le web.**

En 2018, l'escroquerie en ligne et à la téléphonie concerne à minima **864 000 victimes** (72% de 1,2 million). En rapportant ce nombre de victimes à la population métropolitaine, on établit que plus d'un habitant métropolitain sur cent a été **victime** d'une escroquerie en ligne ou à la téléphonie en 2018[17] : précisément, **1,7% de la population** résidant sur le territoire métropolitain a été victime d'une escroquerie en ligne ou à la téléphonie en 2018.

Sur Internet, les escroqueries (hors débit frauduleux) couronnées de succès portent trois fois sur quatre, sur **l'achat d'un bien ou d'un service** qui peut être non conforme, plus cher qu'initialement prévu ou tout simplement non délivré. Dans 33% de ces situations, l'escroquerie a pour objet un bien de consommation (Figure 3). En 2020, la mode et l'habillement représentent 53,9% des produits les plus achetés sur Internet en France[18] Par conséquent, les auteurs d'escroquerie semblent concentrer leurs efforts sur les biens qui attirent le plus les internautes.

[17] Le nombre de personnes vivant sur le territoire métropolitain âgées de 14 ans ou plus en 2018 était de 52 063 798 selon l'Insee : voir Bilan démographique 2018 - *La fécondité se stabilise en France* -, janvier 2019.
[18] Fevad, *Etude Bilan e-commerce,* 2020.

Figure 3 – Lorsqu'une victime se fait escroquer lors de l'achat d'un produit ou d'un service sur Internet, celui-ci concerne :



Source : Institut national des hautes études de la sécurité et de la justice. D'après l'enquête *Cadre de Vie et Société*, *Note de n°50* de l'Observatoire national de la Délinquance et des réponses pénales, septembre 2020.
Lecture : En 2017 et en 2018, 21% des escroqueries à l'achat sur Internet portaient sur un bien d'équipement.

La plupart du temps (53%), le préjudice est inférieur à 100 euros. Mais il peut atteindre (11% des cas) un montant de plus de 1000 euros.

Outre ces types d'arnaques ; l'enquête *CVS* révèle que **858 000 personnes ont subi un débit frauduleux sur Internet** ; soit sous forme d'un achat par carte bancaire sur un site de commerce en ligne, soit sous forme de virement. C'est donc 1,6% de la population qui est concernée. L'enquête mesure que 79% des victimes de ces méfaits (qu'ils aient ou non été commis sur Internet) déclarent avoir été remboursé au moment de l'étude. Au total, si on part de l'hypothèse que ce taux est le même que l'escroquerie ait eu lieu en ligne ou non, ce serait donc 257 400 personnes qui ont perdu de l'argent à la suite de débits frauduleux, soit 0.5% de la population.

Les publications de l'enquête ne nous permettent pas de savoir si les victimes de débits frauduleux en ligne ont également subi une ou plusieurs autres formes d'arnaque sur Internet ou par téléphone. Au total, la proportion de personnes ayant été victime avérée d'une escroquerie est donc comprise entre **1.7% et 2.2%.**

Un nombre de dépôts de plainte parmi les plus bas

En 2018, seulement 7% des victimes d'escroquerie sur Internet ont porté plainte et 2% ont déposé une main courante[19]. Ce taux de dépôt de plainte est très bas. A titre de comparaison, en moyenne entre 2011 et 2018, 92% des personnes victimes d'un vol de voiture ont porté plainte[20]. Par

[19] Insee-ONDRP-SSMSI. « Arnaques », Enquête de victimation, *Cadre de vie et sécurité*, 2019.
[20] Insee-ONDRP-SSMSI. « Vol de voiture », Enquête de victimation, *Cadre de vie et sécurité*, 2019

ailleurs, parmi les ménages victimes de cambriolage entre 2016 et 2018, 71 % en moyenne ont déposé plainte.[21]

Bilel Benbouzid et Sophie Peaucellier[22] ont montré que les caractéristiques socio-économiques des ménages ne constituent pas un des déterminants de la déclaration aux autorités publiques de l'escroquerie en ligne dont ils ont été victimes. Autrement dit, aucun groupe de la population ne porte plainte plus souvent qu'un autre à la suite d'une escroquerie sur Internet. En revanche, le **montant du préjudice** peut être un élément favorisant le dépôt de plainte. **Plus la somme d'argent dérobée est importante, plus la propension à porter plainte augmente.** On sait par exemple, que les victimes de chantage ou de piège sur Internet déposent plainte plus souvent (22%) - 15 points de plus que la moyenne[23]. Or, le montant du préjudice pour ce type d'escroquerie figure parmi les plus élevés : 500 euros ou plus dans 26% des cas. Il est par exemple plus conséquent que le montant d'un préjudice lié à une escroquerie à l'achat qui s'élève à moins de 100 euros dans presque 70% des situations[24].

Le dépôt de plainte semble refléter un ratio entre les efforts à faire pour porter plainte (se déplacer, justifier de différentes pièces) et la projection d'une faible probabilité de réparation liée à la difficulté à identifier les auteurs de fraude. En effet, en 2017 et en 2018, **94% des victimes d'escroquerie sur Internet n'ont jamais rencontré physiquement l'auteur, 20% ne savent pas dans quel pays il se situe** et 38% pensent qu'il provient d'un pays étranger ; la Chine étant le premier pays cité (38%)[25]. Sans pouvoir communiquer des informations sur l'auteur du méfait (nom, adresse postale ou adresse électronique), il est peu probable que les autorités puissent retrouver ce dernier.

L'absence de bénéfices personnels anticipés, cumulé au **manque de communication des institutions sur l'existence de dispositifs** explique probablement le faible usage des plateformes recensant les cybercrimes en France. D'après l'Eurobaromètre spécial 499, en 2019, 82% des Français métropolitains âgés de 15 ans ou plus n'étaient pas informés de l'existence dans leur pays, d'un site internet, d'une adresse électronique, d'une plateforme en ligne ou d'un numéro de téléphone auquel ils pouvaient rapporter l'existence d'un cybercrime. Seuls 17% connaissaient l'existence d'un tel support[26].

Les plateformes de signalement en France

Pour signaler une escroquerie : contactez la plateforme téléphonique « Info Escroquerie ». Composée de policiers et de gendarmes, la plate-forme « Info Escroqueries » est chargée d'informer, de conseiller et d'orienter les personnes victimes d'une escroquerie.
Contact : du lundi au vendredi de 9H à 18H30 au 0 805 805 817 (appel gratuit depuis la France).

Pour signaler un contenu ou un comportement illicite rencontré sur Internet : déposez un signalement sur la plateforme internet PHAROS, la Plate-forme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements.

Internet-signalement.gouv.fr

Pour signaler un spam sms ou un spam vocal : contactez le 33700 ou rendez-vous sur la plateforme internet signal-spam.fr

[21] Insee-ONDRP-SSMSI « Cambriolage et tentatives », Enquête de victimation*, Cadre de vie et sécurité*, 2019

[22]Benbouzid, Bilel, et Sophie Peaucellier. *art cité*, p. 146.

[23] Institut national des hautes études de la sécurité et de la justice. D'après l'enquête *Cadre de Vie et Société*, *Note de n°50 de* l'Observatoire national de la Délinquance et des réponses pénales, septembre 2020

[24] *Ibid.*

[25] *Ibid.*

[26] Commission Européenne. Spécial Eurobaromètre 499 : *Europeans' attitudes towards cyber security*, publié en janvier 2020.

Le taux de plainte diffère selon **la forme** que prend l'escroquerie en ligne ou à la téléphonie. En effet, 23% des victimes d' « escroquerie bancaire » - orchestrées sur et en dehors d'Internet - ont porté plainte en 2017 et en 2018[27]. Or, plus de la moitié de ces « escroqueries bancaires » a lieu sur Internet. On en déduit que **l'escroquerie bancaire en ligne détient un taux de plainte plus élevé** que celui des autres types d'escroqueries en ligne ou à la téléphonie (qui, pour mémoire, s'élève à 7%). Bilel Benbouzid et Sophie Peaucellier expliquent ce taux relativement élevé de **dépôt de plaintes pour l'« escroquerie bancaire »** par l'attitude des banques à l'égard de leurs clients victimes[28]. En effet, depuis 2009, les titulaires de carte bancaire dont les données ont été frauduleusement utilisées ne sont plus contraints de porter plainte afin d'être remboursés par leur banque du montant détourné[29]. Il en est de même pour les personnes atteintes par le biais de l'hameçonnage depuis 2011. Autrement dit, toute banque en France est tenue de rembourser son client si ses données bancaires sont utilisées à son insu par un tiers et sans son consentement. Pourtant, les avocats rencontrés dans le cadre des travaux de ces chercheurs rapportent que rares sont les banques qui remboursent automatiquement les clients à la suite d'une escroquerie bancaire. **Le dépôt de plainte constitue ainsi une sorte d'étape** pour les banques, leur permettant de trier les clients les plus déterminés à se faire rembourser. D'ailleurs, 79% des répondants de l'enquête *CVS* déclarent avoir été remboursé au moment de l'étude, et non 100% d'entre eux.

Si de façon générale les victimes d'escroquerie à la téléphonie et en ligne rapportent peu leur atteinte aux services de police et de gendarmerie, cela ne signifie pas pour autant qu'elles ne communiquent pas sur l'escroquerie dont elles ont été victimes. Par exemple, il n'est pas rare que les victimes d'escroquerie sur Internet dénoncent l'atteinte qu'elles ont subi sur **d'autres canaux alternatifs**[30]. En analysant les données du web, Bilel Benbouzid et Sophie Peaucellier ont découvert qu'Internet et notamment les forums, constituent **un espace de dénonciation** pour les victimes[31]. Par ailleurs, une minorité de forums concentrent la majorité des publications relatives aux escroqueries. *Lesarnaques.com* est à ce titre, l'un des forums contentant le plus de discussions à ce sujet et se présente comme un **site « d'entraide et de médiation ».** L'absence de dépôt de plainte ou de signalement sur les plateformes ne semble donc pas être reliée à un manque de civisme mais plutôt au symptôme des **nouvelles régulations numériques entre pairs.** En signalant les déboires à leurs pairs directement, les victimes d'escroquerie ont le sentiment de protéger plus efficacement leurs congénères, et de limiter le potentiel de nuisance des structures ou individus qui les ont piégés.

Les auteurs observent également une différence de comportement sur le web entre les victimes de fraude bancaire en ligne et les victimes d'escroquerie à l'achat de produit ou service. Tandis que les premières expriment leur besoin de conseil et d'information pour obtenir réparation auprès de leur banque, les secondes utilisent cet espace en ligne pour **« faire scandale » et générer de la « mauvaise publicité ».** Ces personnes utilisent le forum pour faire la preuve de leur victimation et se déresponsabiliser, une tentative qui peut s'avérer plus ou moins fructueuse. L'analyse des caractéristiques socio-économiques des auteurs de messages sur ces forums mériterait d'être étudiée. En effet, selon Dominique Pasquier[32], la participation à des forums en ligne suppose la production de messages de qualité soignée et formelle, une compétence attribuée aux catégories diplômées. Il serait intéressant de savoir si les victimes rapportant sur le web, l'escroquerie en ligne ou à la téléphonie dont elles ont été victimes appartiennent davantage aux catégories diplômées ou non.

---

[27] Insee-ONDRP-SSMSI « Escroqueries bancaires », Enquête de victimation*, Cadre de vie et sécurité*, 2019.

[28] Benbouzid, Bilel, et Sophie Peaucellier. « L'escroquerie bancaire en France métropolitaine : profils de victimes et décisions de renvoi à la police », *Questions pénales*, XXIX, 1. 2016

[29] Article L133-19 du Code Monétaire et financier, paragraphe II, en application de la directive européenne SEPA (Single Euro Payments Area).

[30] Benbouzid, Bilel, et Daniel Ventre. « Pour une sociologie du crime en ligne. Hackers malveillants, cybervictimations, traces du web et reconfigurations du *policing* », *Réseaux*, vol. 197-198, no. 3-4, 2016, p. 16.

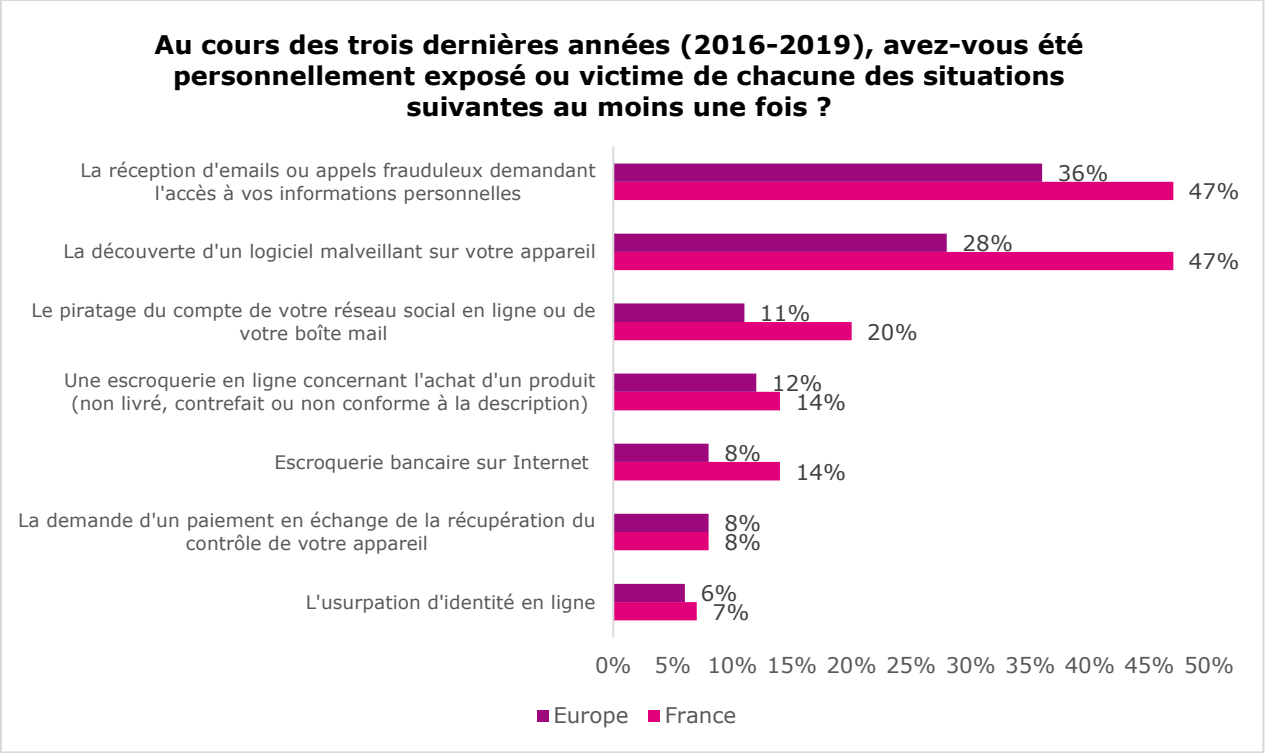
[31] Benbouzid, Bilel, et Sophie Peaucellier. *art cité,* p. 153.

[32] Pasquier, Dominique. « Classes populaires en ligne : des « oubliés » de la recherche ? », Réseaux, vol. 208-209, no. 2-3, 2018, p. 15.

Une personne sur deux exposée

L'enquête *CVS*, par construction, met en avant seulement les **victimes** d'escroquerie, ayant laissé des plumes dans l'affaire, occultant ainsi toutes les personnes qui ont été **exposées** à cette pratique illicite sans pour autant s'être fait soustraire leurs données personnelles ou leur argent. Par exemple, l'enquête ne tient pas compte de l'ensemble des personnes ayant reçu des SMS ou des appels frauduleux, mais seulement celles s'étant faites escroquées à la suite de leur réception. En effet, d'après *l'Eurobaromètre spécial 499*[33], 47 % des Français ont reçu au moins une fois un e-mail ou un appel frauduleux entre 2016 et 2019 leur demandant des informations personnelles (mot de passe de l'ordinateur, identifiants, informations bancaires…). La même proportion déclare avoir découvert un logiciel malveillant sur son appareil et 20% affirment s'être fait pirater son réseau social ou son adresse électronique.

Figure 4 – Le niveau de victimation des Français souvent supérieur à la moyenne européenne



Source : Commission Européenne. Spécial Eurobaromètre 499 : *Europeans' attitudes towards cyber security*, janvier 2020.

Lecture : En 2019, 20% des Français et 11% des Européens se sont fait pirater le compte de leur réseau social ou leur boîte mail au moins une fois au cours des trois années précédentes.

D'après ces déclarations, on constate que les Français se disent beaucoup plus souvent victimes d'escroquerie en ligne ou à la téléphonie que la moyenne des Européens. L'écart est particulièrement sensible s'agissant des emails ou appels frauduleux destinés à accéder aux données personnelles des victimes (47% en France, + 11 points par rapport à la moyenne européenne) ou à la découverte d'un logiciel malveillant sur un appareil (47%, + 19 points). Le piratage d'une boite mail ou d'un compte de réseau social serait deux fois plus souvent fréquent en France (20%) que dans l'Europe en moyenne (11%). Cette différence reflète-t-elle des attaques plus souvent présentes dans l'Hexagone ? Ou est-ce une conséquence d'une vigilance accrue ? En effet, depuis quarante ans,

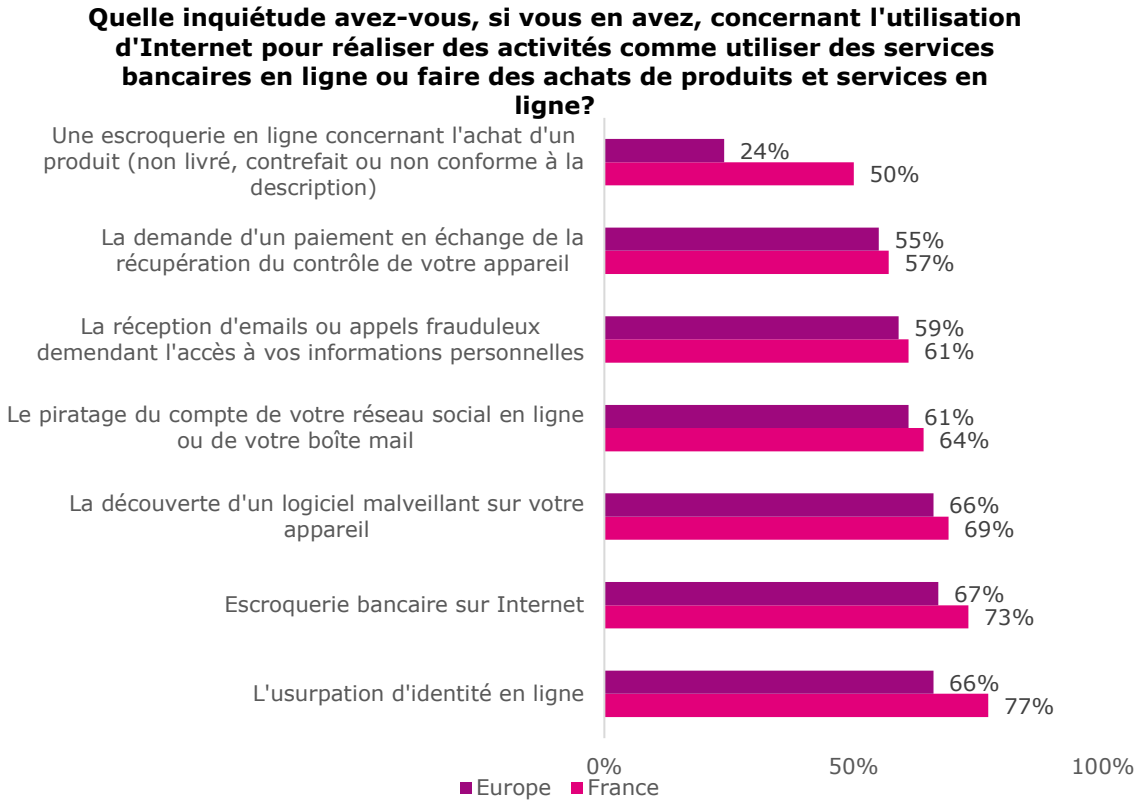
[33] Commission Européenne. Spécial Eurobaromètre 499 : *Europeans' attitudes towards cyber security*, janvier 2020.

l'enquête Européenne sur les valeurs montre que la France appartient aux pays d'Europe du Sud où la confiance est rare, et nos compatriotes ont tendance à se montrer très circonspects et prudents, alors que le Nord de l'Europe, particulièrement les pays scandinaves, se caractérise par une très forte confiance interpersonnelle[34]. Rappelons également que la France est un territoire où dès les années 70, la question de la protection des données personnelles a mobilisé l'opinion, entrainant la création de la CNIL, premier organe au monde à se saisir de ces questions.

Des inquiétudes fortes, notamment concernant l'identité numérique

Nombreuses sont les formes d'escroqueries en ligne qui inquiètent les Français. **L'usurpation de l'identité en ligne** (77%, +11 points par rapport à la moyenne européenne), la **fraude bancaire en ligne** (73%, +6 pts par rapport à la moyenne) et l'infection de leur appareil par **un logiciel malveillant** ou un virus (69%, +3 pts)[35] constituent le tryptique de tête des sources d'anxiété numérique les plus répandues dans l'Hexagone.

Figure 5 – De fortes inquiétudes concernant les escroqueries en ligne



Source : Commission Européenne. Spécial Eurobaromètre 499 : Europeans' attitudes towards cyber security, publié en janvier 2020.
Lecture : En 2019, 50% des Français sont inquiets d'être victime d'une escroquerie à l'achat sur Internet contre seulement 24% des Européens.

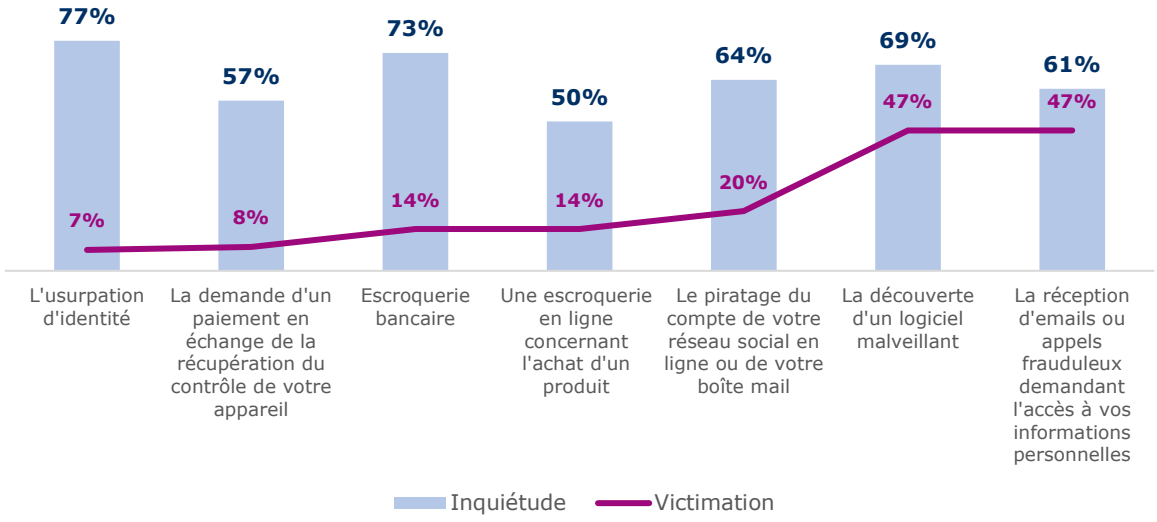
[34] ARVAL – Un site utilisant WordPress (valeurs-france.fr) Ainsi en 2018, date de la dernière mesure, seuls 27% de nos concitoyens déclarent que l'on peut faire confiance à la plupart des gens (plutôt que « on n'est jamais assez prudents »), contre 36% en moyenne et par exemple 72% en Finlande et 67% en Suède.

[35] Spécial Eurobaromètre 499 : *Europeans' attitudes towards cyber security*, publié en janvier 2020.

Deux des situations étudiées - **l'escroquerie à l'achat d'un produit (26 points d'écart) et l'usurpation d'identité (11 points d'écart)** - suscitent une plus forte inquiétude dans le pays au drapeau tricolore.
Lorsque l'on rapproche les données de victimation du sentiment d'inquiétude ressenti vis-à-vis de cette même situation (Figure 6) on peut distinguer **2 groupes de fraudes** :

- Des escroqueries où le sentiment d'inquiétude semble relié à la fréquence de survenue effective des événements :
    - La découverte de logiciels malveillants ou la réception d'emails demandant l'accès à des informations personnelles sont relativement répandues et suscitent mécaniquement une inquiétude plus partagée.
    - Dans la même veine, la demande de paiement en échange de la récupération du contrôle de l'appareil, ou les escroqueries concernant l'achat d'un produit sont moins souvent signalées, et inquiètent, logiquement, moins.
- Des malversations signalées assez rarement mais générant de fortes inquiétudes : l'usurpation d'identité et l'escroquerie bancaire ou le piratage de son réseau social. Ces trois types d'action ont pour caractéristique de toucher à **l'identité numérique,** avec de potentielles conséquences risquant de **s'étaler dans le temps**, à la fois car les escrocs peuvent multiplier les effractions le temps que ces identités falsifiées puissent être arrêtées, et parce que la toile conserve une **longue mémoire** dont les traces sont souvent quasi impossibles à effacer.

Figure 6 – L'usurpation d'identité en ligne : la situation la moins fréquente, mais la plus anxiogène



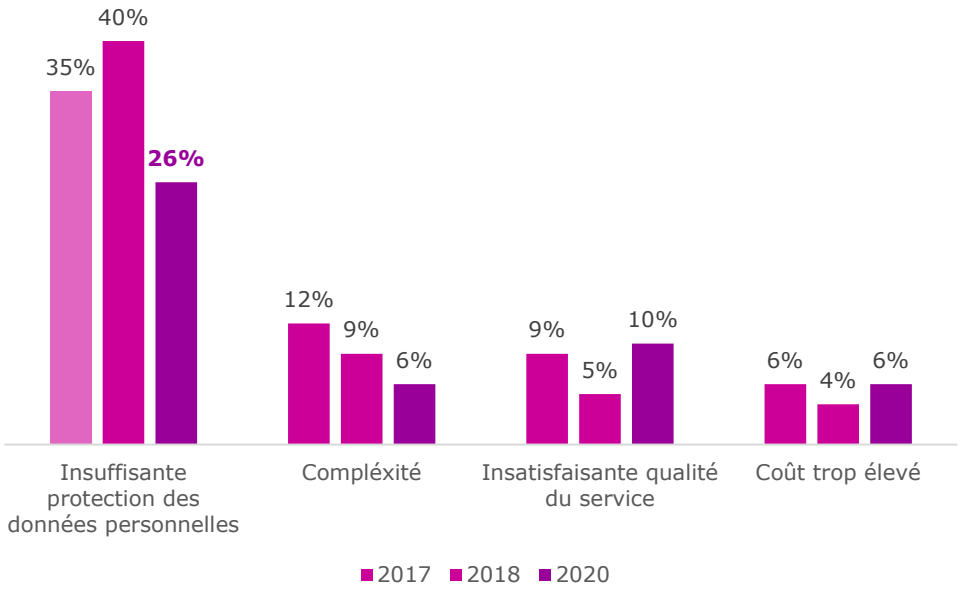
Source : Commission Européenne. Spécial Eurobaromètre 499 : Europeans' attitudes towards cyber security, publié en janvier 2020.
Lecture : En 2019, 77% des Français sont inquiets d'être victime d'une usurpation d'identité en ligne, alors que 7% seulement en auraient été victimes.

Les inquiétudes de la population vis-à-vis de l'escroquerie en ligne ou à la téléphonie s'inscrivent dans un contexte plus général **d'un manque de confiance vis-à-vis de la protection et l'utilisation de leurs données personnelles**. La majorité des Français (76%) ont peu confiance dans la capacité des sites Internet à protéger leurs données personnelles. Lorsqu'elle utilise Internet, 49% de la population craint qu'un tiers récupère ses données et les utilise à de mauvaises fins et 43% est

inquiète à l'idée de réaliser un paiement en ligne sur un site non-sécurisé[36]. Par ailleurs, 8 personnes sur 10 sont convaincues que des logiciels installés sur leur téléphone mobile peuvent transmettre leurs informations personnelles sans les avertir.[37] L'insuffisante protection des données personnelles représente d'après la population, le principal frein à l'utilisation d'Internet en 2020 (**Erreur ! Source du renvoi introuvable.** 7). Cette crainte demeure le principal frein évoqué par les Français, loin devant sa complexité d'utilisation ou son coût trop élevé. Toutefois elle a tendance à s'estomper. Ils étaient en effet 35% à l'évoquer en 2017 contre 26% en 2020.[38] Cette diminution de l'inquiétude peut être l'effet de la mise en œuvre du **Règlement Général de Protection des Données** et de la systématisation des demandes d'autorisation sur les usages des données personnelles par les sites et applications, communément appelés cookies.
La **sécurité des moyens de paiement** représente quant à elle, la principale raison faisant hésiter les Français à réaliser un achat sur Internet (29%), juste devant l'impossibilité de toucher ou de voir en réel le produit acheté (28%). Il faut dire que, effectivement, le taux d'escroquerie au paiement à distance est dix-neuf fois plus élevé en volume que le taux de fraude des paiements de proximité et sur automate. Toutefois depuis 2016, la sécurité des moyens de paiement **inquiète moins les Français** (Figure 8).

Est-ce un effet de l'amélioration continue de la sécurisation des transactions (avec les empreintes digitales par exemple, ou la vérification par sms) le développement d'identités numériques officielles avec France Connect) ? Ou l'appropriation des mesures de protections ? Un signe d'une forme de relâchement de la vigilance liée à la généralisation des pratiques ? Les Français sont de plus en plus à l'aise avec l'idée d'effectuer des transactions marchandes sur Internet.

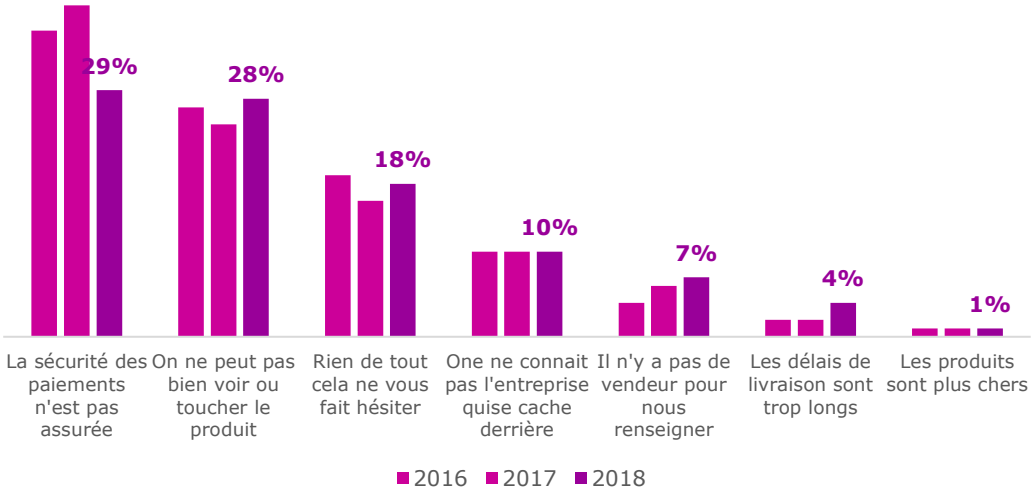
Figure 7 – Le manque de protection des données personnelles est le principal frein à l'utilisation d'Internet



Source : CRÉDOC. *Baromètre du Numérique*, éditions 2017, 2018, 2021.
Lecture : En 2020, 38% de la population âgée de 15 ans ou plus résidant en France métropolitaine ne voit aucun frein à l'utilisation d'Internet.

[36] Spécial Eurobaromètre 499 : *Europeans' attitudes towards cyber security*, publié en janvier 2020.
[37] CRÉDOC. *Baromètre du Numérique*, édition 2019.
[39] Commission Européenne. Spécial Eurobaromètre 480 : *Europeans' attitudes towards Internet security*, publié en mars 2019.

Figure 8 – La sécurité des paiements reste le principal frein à l'achat en ligne



Source : CRÉDOC. *Baromètre du Numérique*, éditions 2016, 2017, 2018.

Lecture : Entre 2018, 29% de la population âgée de 15 ou plus résidant en France métropolitaine cite « le manque de sécurisation du paiement » comme le principal élément les faisant hésiter pour effectuer un achat sur Internet.

Les plateformes ressources pour se prémunir de l'escroquerie en ligne et à la téléphonie en France

L'escroquerie à la fausse commande - Conseils pour repérer et se prémunir de ce type d'arnaque. Cybermalveillance.gouv.fr, 2 novembre 2021.

Les arnaques aux faux RIB (relevé d'identité bancaire) se multiplient. Lafinancepourtous.com prodigue des conseils pour se protéger de ce type d'escroquerie. 18 octobre 2021.

Paiement en ligne : 7 conseils pour éviter les risques de piratage. economie.gouv.fr, 8 octobre 2021

L'AMF appelle à la vigilance des consommateurs concernant des acteurs proposant des investissements sans y être autorisés. 29 septembre 2021.

La page Infos du site Internet de la DGCCRF aide les internautes à identifier les pratiques commerciales abusives, mensongères et trompeuses.

L'ACPR (Autorité de contrôle prudentiel et de résolution) et l'AMF (Autorité des marchés financiers) publient et mettent à jour régulièrement, sur le site abe-infoservice.fr, cinq listes noires de sites ou entités non autorisés à proposer des produits bancaires, d'assurance ou financiers en France.

La CNIL propose plusieurs articles sur son site Internet sur l'hameçonnage, le spam et les arnaques en ligne.

Progression des escroqueries en ligne avec la digitalisation de la société et son amplification liée à la pandémie

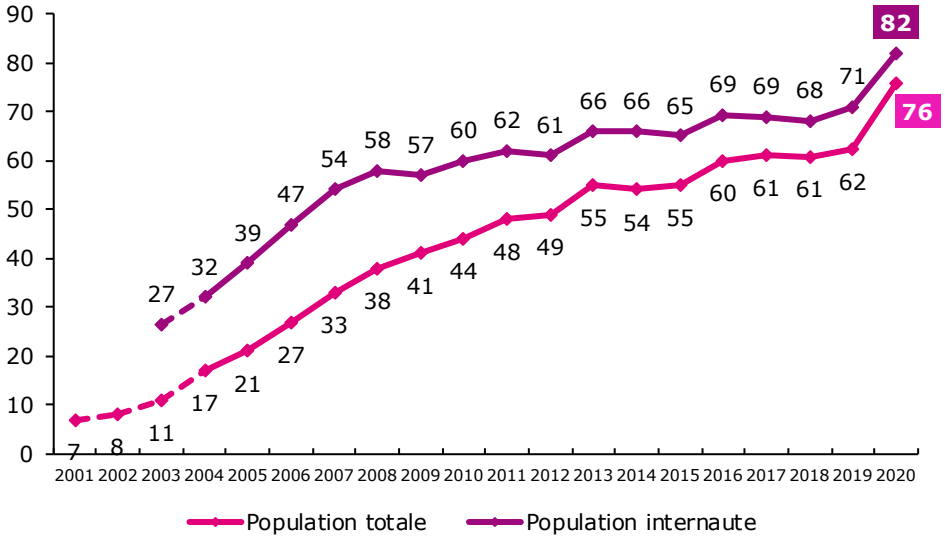
En 2019, 82% des Français pensent que le risque d'être victime d'un cybercrime, dont l'escroquerie en ligne et à la téléphonie, est en train d'augmenter contre 79% des Européens.[39]

Nous ne sommes pas en mesure de connaître dans quelle proportion exacte l'escroquerie en ligne et à la téléphonie a augmenté ces dernières années, mais nous pouvons affirmer que la population est davantage touchée en liaison avec différentes données.

Tout d'abord rappelons le formidable essor des pratiques et équipements numériques dans la société dans de nombreuses dimensions : démarches administratives, bancaires, achats de produits et services, etc. Ces pratiques ont progressé en nombre mais touchent aussi **une part de la population de plus en plus grande,** avec de nouveaux adeptes chaque année depuis que nous suivons ces questions. Les mesures prises par le gouvernement pour enrayer la propagation du virus (confinement, couvre-feu, fermeture de certains lieux…) ont accéléré la numérisation de nombre d'activités : consultations médicales en ligne, recours accru à l'administration en ligne, augmentation des opérations bancaires réalisées en ligne, visio-conférences[40]… En **particulier, les achats en ligne ont connu un coup d'accélérateur très net** (+11 points en un an). Les différentes mesures prises par le gouvernement ont en effet modifié les habitudes d'achat des consommateurs et les pratiques commerciales des commerçants qui ont développé la vente en ligne et notamment le *click and collect*.

Figure 9 - Proportion d'individus ayant effectué dans les 12 derniers mois, des achats par Internet

- Champ : ensemble de la population de 12 ans et plus, en % -



Source : CREDOC, Baromètres du numérique.

Note : la courbe en pointillés porte sur les 18 ans et plus ; à partir de 2003, la courbe porte sur les 12 ans et plus.

[39] Commission Européenne. Spécial Eurobaromètre 480 : *Europeans' attitudes towards Internet security*, publié en mars 2019.

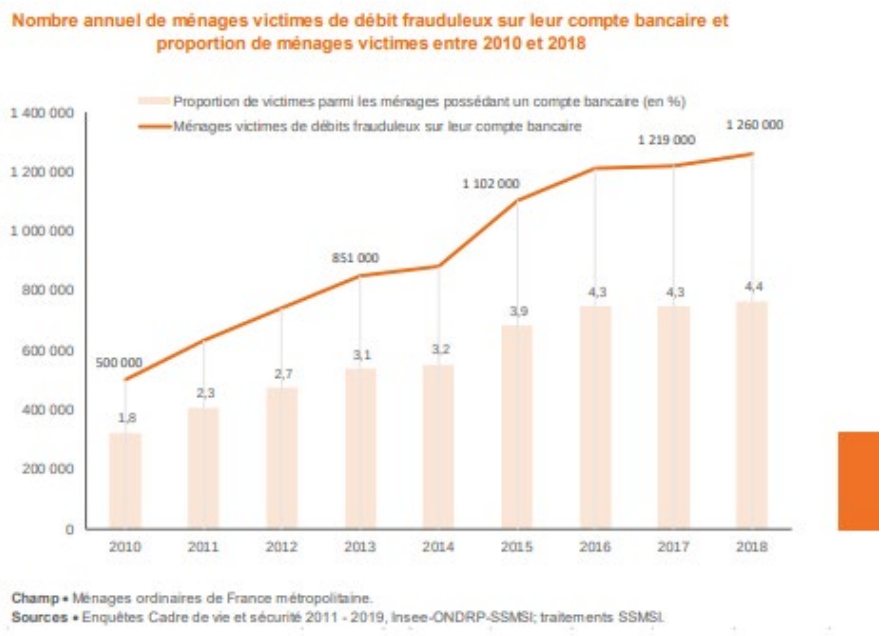
[40] Baromètre du numérique, op.cit.

La population a davantage acheté sur Internet et donc, procédé à des paiements à distance au cours de l'année 2020 : +13,5% en valeur par rapport à 2019[41]. En valeur, l'**escroquerie au paiement à distance** (opéré par téléphone, courrier ou sur Internet) a progressé de **plus 16,4% par rapport à 2019**[42]. **Toutefois, son taux est toutefois resté relativement stable,** passant de 0.0170% en 2019 à 0.0174% en 2020.

La fraude au virement quant à elle, progresse de manière significative en 2020 (+65% en valeur et +125% en volume par rapport à 2019). Les fraudeurs ont profité de la perte de repères des organisations engendrée par la Covid-19[43] pour justifier la réalisation de virements en urgence. La fraude au virement a toutefois surtout touché les administrations publiques et les entreprises privées, moins les ménages.

La panique liée à la période et la découverte soudaine de pratiques numériques sans alternatives possibles pour des publics peu familiers, n'est pas seule en cause. La progression des escroqueries en ligne suit la **numérisation de la société**, les fraudeurs reportent leurs agissements en ligne. Les attaques au *phishing*[44] et de logiciels malveillants se sont multipliées pour récupérer les données bancaires des victimes. D'après l'enquête *CVS,* en 2010, 500 000 ménages déclaraient avoir été victimes **d'un débit frauduleux** (sur et en dehors d'Internet) contre 1,3 million en 2018. Leur nombre a plus que doublé en huit années. L'augmentation n'est pas seulement visible en volume mais également en proportion de ménages puisque c'est 4.4% des ménages qui ont été victimes de débits frauduleux en 2019 contre 1.8% en 2010.

Figure 10 : Victimes d'escroquerie bancaire sur et en dehors d'Internet



Au total, *l'état 4001* enregistre **une augmentation moyenne de 7% par an** du nombre « d'escroqueries et abus de confiance » réalisés en France **entre 2012 et 2019**.

[41] Ibid.
[42] Banque de France. Observatoire des moyens de paiements, *Rapport,* 2020.
[43] *Ibid.*
[44] Le *phishing* ou *hameçonnage* est une forme d'escroquerie sur internet qui consiste à récupérer les données personnelles des consommateurs par la tromperie, puis à les utiliser de manière malveillante, par exemple pour faire des achats.

CHAPITRE 2 : LES MÉNAGES LES PLUS PRÉCAUTIONNEUX SONT AUSSI LES PLUS TOUCHÉS PAR L'ESCROQUERIE EN LIGNE ET À LA TÉLÉPHONIE

Protection des données et restriction des possibilités numériques : un dilemme qui penche en défaveur de la sécurité des utilisateurs

La **protection des données personnelles** est au cœur de la lutte contre l'escroquerie en ligne et à la téléphonie. Cette opération illicite se déroulant par nature à distance, les auteurs d'escroquerie ont besoin d'accéder aux données bancaires ou personnelles de leurs victimes pour arriver à leurs fins. Par exemple, les données personnelles des victimes telles que leur identifiant et mot de passe permettant l'accès à leur espace bancaire en ligne, sont nécessaires pour procéder à un virement bancaire. Payer avec la carte bleue d'un tiers sur Internet nécessite de connaitre les numéros inscrits sur la carte, le nom du détenteur et le cryptogramme au dos. Ces données bancaires ou personnelles sont récupérées de façon illégale par les auteurs d'escroquerie soit pour dérober directement une somme d'argent à la victime, soit pour entrer en contact avec celle-ci dans le but de lui soustraire une somme d'argent. Dès lors, **la protection des données apparaît comme un moyen permettant la diminution de l'exposition des citoyens à cette forme de criminalité**. Pourtant, tous ne sont pas prêts à renoncer aux services et libertés proposés par les GAFAM en échange de la non-utilisation de leurs données personnelles. En 2018, 82% de la population **refusait d'utiliser un site internet ou un réseau social payant en échange de la garantie** de la non-utilisation de ses données personnelles. De plus, 60% des internautes refusaient de voir leur accès à un service en ligne limité, en échange de la garantie que leurs données personnelles ne soient pas utilisées. Ces opinions révèlent l'ambivalente position dans laquelle se trouvent les internautes aujourd'hui. Bien qu'inquiète quant à la détention et l'utilisation de ses données personnelles et du risque d'être potentiellement victime d'une escroquerie en ligne ou à la téléphonie, la majorité de la population n'est pas prête à renoncer à la gratuité des services sur le web ou à leur pleine accessibilité pour mieux protéger ses données personnelles. Ces résultats appuient la démonstration de Mark Poster[45] selon laquelle les internautes contribuent activement à la collecte d'informations personnelles les concernant.

La population se protège face à l'escroquerie en ligne et à la téléphonie

Pour protéger leurs données personnelles en ligne, les internautes et possesseurs de téléphone mobile peuvent adopter certaines précautions. En 2020, la première d'entre elles est le refus de la géolocalisation proposée lors de l'ouverture d'une page web ou d'une application. Ensuite, les répondants sont 67% à déclarer avoir déjà renoncé à un achat en ligne lorsqu'ils considéraient le paiement insuffisamment sécurisé. Enfin, la troisième précaution la plus adoptée par la population est le renoncement à l'installation d'une application. Par rapport à 2017, la plupart des précautions adoptées sont citées **plus souvent**. Seul le renoncement à publier ou la suppression d'un message sur un réseau social (-3 points) et le renoncement d'installer une application pour des raisons de sécurité (-5 points) ont légèrement reculé.

[45] Poster Mark. *The Mode of Information: Poststructuralism and Social Context*, Chicago, University of Chicago Press, 1990.

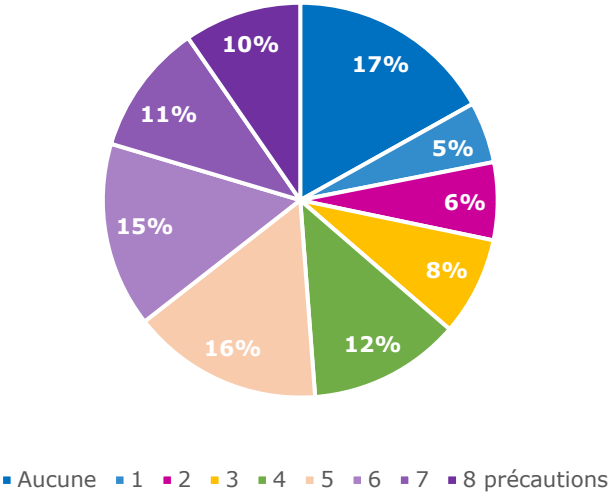
Figure 11 : Précautions prises par les internautes lorsqu'ils utilisent Internet

Il est possible de prendre certaines précautions ou d'adopter certains comportements quand on utilise Internet. Vous, personnellement, avez-vous déjà…?

Source : CRÉDOC. *Baromètre du numérique,* éditions 2017 et 2021.
Champ : individus internautes ou possesseurs d'un téléphone mobile, en %.

En prenant en compte l'ensemble des précautions déclarées, on constate que la population adopte des comportements très différenciés : 17% des personnes interrogées n'ont jamais pris aucune des précautions évoquées alors qu'à l'inverse, 10% les ont déjà toutes prises. Par rapport à 2017, l'évolution la plus notable concerne la proportion de personnes ayant pris l'ensemble des précautions évoquées, dont la proportion passe de 4 à 10% (+6 points).

Figure 12 – Répartition de la population en fonction du nombre de précautions prises



Source : CRÉDOC. *Baromètre du numérique,* édition 2021.
Lecture : 16 % des internautes et possesseurs de téléphone portable prennent cinq précautions simultanément lorsqu'ils utilisent Internet.

Les caractéristiques sociales des internautes et des détenteurs de téléphone déterminent le type de précaution prise par ces derniers. Le recours à telle ou telle précaution dépend notamment de l'âge et du niveau de diplôme.
Les **jeunes (18-24 ans) et les diplômés du supérieur** adoptent des précautions similaires : ils sont les plus nombreux à refuser la géolocalisation (79% et 76%), à prendre des dispositions pour ne pas laisser de traces sur Internet (64% et 61%), à renoncer à publier ou supprimer un message sur leur réseau social (57% et 51%).
Les personnes âgées (60-69 ans) disent plus souvent que la moyenne arrêter leur navigation sur un site jugé pas assez sécurisé (66%) et renoncer à l'installation d'une application pour protéger leurs données personnelles (71%).

En revanche, le fait d'éteindre son téléphone portable pour éviter d'être tracé est une précaution prise **de façon homogène** par l'ensemble de la population. Il en est de même pour le renoncement à un achat par manque de confiance au moment du paiement. Les 18-24 ans l'adoptent autant que les 60-69 ans (70%). Seuls les très jeunes et les très âgés y ont moins eu recours. Or, l'on sait que ces groupes de personnes sont ceux qui pratiquent le moins l'achat en ligne. En 2020, 43% des 12-17 ans et 45% des 70 et ans ou plus ont déclaré n'avoir effectué aucun achat sur Internet au cours des douze derniers mois, soit beaucoup plus que la moyenne (23%)[46].
Enfin, on observe que le revenu n'influence quasiment pas le choix des précautions adoptées. En effet, les bas revenus et les hauts revenus disent recourir dans des proportions très proches aux précautions suivantes : éteindre son téléphone pour éviter d'être tracé, prendre des dispositions pour ne pas laisser de traces sur Internet, renoncer à un achat par manque de confiance au moment du paiement, souscrire à un service de sécurisation en ligne, renoncer à publier ou supprimer un message en ligne.

[46] CRÉDOC, *Baromètre du numérique,* édition 2021.

Qui sont les personnes prenant le plus de précautions ?

À partir des résultats des enquêtes *Baromètre du numérique*, ce cahier de recherche permet de dresser le portrait des utilisateurs les plus et les moins précautionneux sur Internet. Le nombre de précautions adoptées sur Internet est notamment corrélé à l'âge et au niveau de diplôme, au temps passé en ligne, au nombre d'activités réalisées sur Internet, à la compétence auto-déclarée à utiliser un ordinateur et à la fréquence de son utilisation.

- **Les plus précautionneux : les utilisateurs prenant entre six et huit précautions (36% de l'ensemble)**

Ce sont en majorité des jeunes (18-24 ans), les diplômés du supérieur et des actifs appartenant aux catégories socio-professionnelles des indépendants (agriculteur, artisan, commerçant, chef d'entreprise) et supérieures (cadre, profession intellectuelle supérieure et profession intermédiaire). Ce sont des personnes qui ont recours à Internet pour plusieurs et divers usages (acheter en ligne, utiliser les réseaux sociaux, effectuer une démarche administrative, vendre un bien ou un service, téléphoner en visioconférence, télécharger des applications…) et qui y passent entre 20 et 25 heures par semaine. Les plus précautionneux se considèrent comme assez, voire, très compétents pour utiliser un ordinateur. D'ailleurs, ce sont également les personnes qui utilisent le plus fréquemment ce type d'appareil numérique.

44% des 18-24 ans

41% des diplômés du supérieur

49% des cadres et professions intellectuelles supérieures

45% des personnes très compétentes pour utiliser un ordinateur

38% des personnes qui utilisent tous les jours un ordinateur

Ils passent en moyenne 23H sur internet par semaine

Source : CRÉDOC. *Baromètre du numérique,* édition 2021.
Lecture : 44 % des 18-24 ans sont des utilisateurs prenant de 6 à 8 précautions, contre 36% de l'ensemble de la population concernée en moyenne.

- **Les moins précautionneux (ne prenant aucune ou une seule précaution - 22% de l'ensemble)**

Il s'agit à la fois de personnes âgées de 70 ans ou plus ou de très jeunes (12-17 ans). Ce sont souvent des personnes habitant seules, non diplômées et en retrait du marché de l'emploi (soit parce qu'elles sont inactives, soit parce qu'elles sont retraitées). Ce sont des personnes qui passent peu de temps sur internet. Les moins précautionneux sont aussi ceux qui se déclarent comme les moins compétents pour utiliser un ordinateur et qui ne l'utilisent rarement, voire jamais.

36% des 70 ans ou plus

28% des 12-17 ans

46% des non diplômés

31% des retraités

22% des inactifs

92% de personnes qui n'utilisent jamais ou rarement un ordinateur

32% des personnes vivant seules

75% des personnes pas du tout compétente pour utiliser un ordinateur

Ils passent 14,5 heures par semaine sur Internet

Source : CRÉDOC. *Baromètre du numérique,* édition 2021.
Lecture : 36% des 70 ans et plus sont des utilisateurs prenant une ou aucune précaution, contre 22% de l'ensemble de la population concernée en moyenne.

Les profils précautionneux davantage victimes d'escroquerie en ligne et à la téléphonie ?

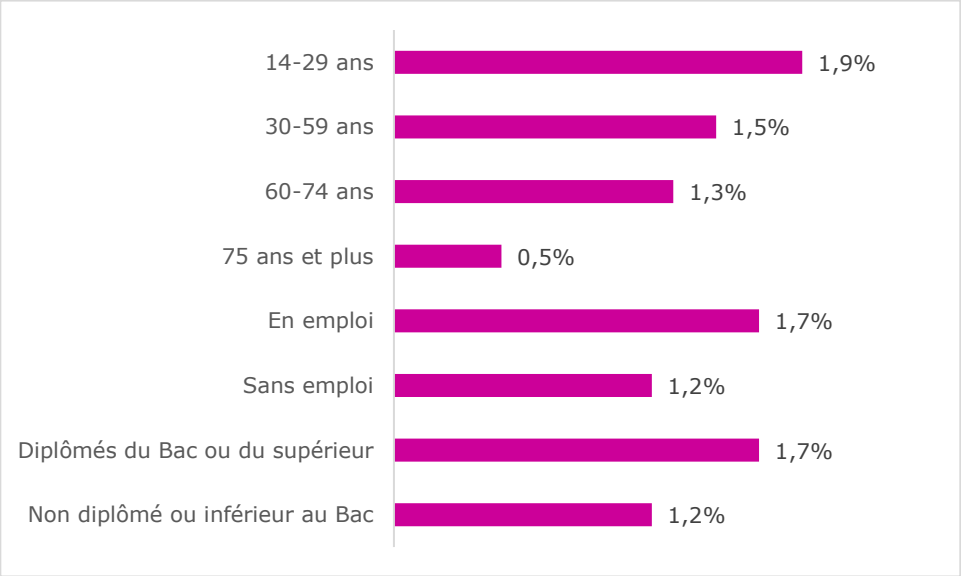
- **Qui sont les victimes de l'escroquerie sur Internet ?**

Les publics les plus victimes de l'escroquerie en ligne sont les personnes en emploi, les **diplômés** et les **plus jeunes**. La victimation plus conséquente des jeunes s'explique structurellement par une plus grande présence que leurs aînés sur Internet[47]. En effet, en 2020, 99% des 12-17 ans utilisaient Internet contre 71% des 70 ans ou plus. De la même façon, les diplômés du supérieur sont davantage internautes (98%) que les non diplômés (66%)[48].

Par ailleurs, d'après l'Observatoire national de la délinquance et des réponses pénales, **l'objet de l'escroquerie diffère en fonction de l'âge** : 57% des personnes âgées de 75 ans et plus atteintes d'une escroquerie en ligne ont été victimes **d'un chantage ou d'un piège**[49]. Parmi les autres catégories d'âge, l'escroquerie la plus fréquente concerne l'achat fictif ou frauduleux d'un bien ou d'un service. Les différences d'usages d'Internet selon les âges contribuent à expliquer ces résultats. En effet, en 2020, 42% des 25-39 ans achètent tous les mois sur un site de e-commerce. Ils ne sont que 24% chez les 70 ans ou plus à l'avoir fait[50].

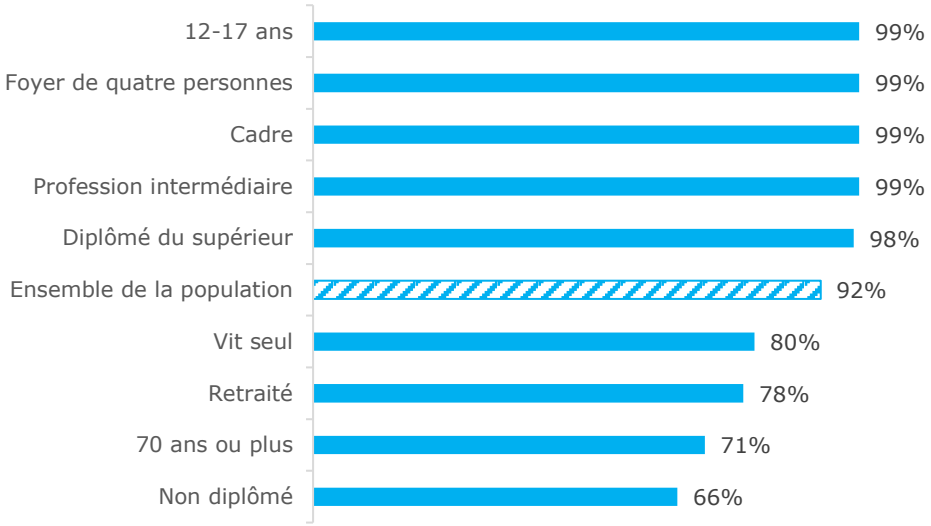
[47] Institut national des hautes études de la sécurité et de la justice. D'après l'enquête *Cadre de Vie et Société*, *Note de n°50* de l'Observatoire national de la Délinquance et des réponses pénales, septembre 2020.
[48] CRÉDOC, *Baromètre du numérique*, édition 2021.
[49] Institut national des hautes études de la sécurité et de la justice. D'après l'enquête *Cadre de Vie et Société*, *Note de n°50 de* l'Observatoire national de la Délinquance et des réponses pénales, septembre 2020.
[50] CRÉDOC, *Baromètre du numérique*, édition 2021.

Figure 13 – La victimation d'escroquerie sur Internet dans différentes catégories sociales



Source : Insee-ONDRP-SSMSI, Enquête de victimation, *Cadre de vie et sécurité*, 2018-2019.
Lecture : En 2017 et 2018, 1,9% des individus âgés de 14 à 29 ans ont été victime d'une escroquerie sur Internet.

Figure 14 – Les groupes de population les plus et les moins internautes en 2020



Source : CRÉDOC, *Baromètre du numérique*, édition 2021.
Lecture : En 2020, 99% des cadres utilisaient Internet.

- **Qui sont les plus exposés au risque d'escroquerie à la téléphonie ?**

D'après l'enquête *Baromètre du Numérique* de 2010, les jeunes adultes et les plus diplômés rapportent plus souvent avoir reçu un appel ou un SMS frauduleux : 57% des 18-24 ans et 54% des diplômés du supérieur (soit respectivement + 11 points et + 8 points par rapport à la moyenne). Les cadres (52%), employés (53%) et membres des professions intermédiaires (54%) se disent également

plus souvent concernés que l'ensemble des personnes équipées d'un téléphone mobile en moyenne[51]. On ne note, en revanche, aucun écart en fonction du genre, des revenus ou de la taille d'agglomération de résidence. Il est possible que les catégories plus jeunes et diplômées **aient davantage su repérer les escroqueries auxquelles elles ont été soumises**, alors que d'autres groupes, plus âgés et moins informés en ont été victimes à leur insu. Toutefois, l'exposition supérieure des jeunes au risque d'escroquerie à la téléphonie s'explique également par une **utilisation plus assidue du téléphone mobile ou smartphone** que les plus âgés. Ainsi, en 2020, 87% des 12-17 ans et 86% des 18-24 ans utilisent un smartphone ou un téléphone portable de façon régulière, contre 56% des 70 ans ou plus et 74% des 60-69 ans[52]. On peut imaginer que dix ans auparavant, les écarts sur l'intensité d'usage étaient au moins aussi importants. De la même façon, les non-diplômés utilisent moins le téléphone mobile au quotidien (54%) que les diplômés du supérieur (83%). Enfin, les personnes appartenant aux catégories sociales supérieures sont davantage utilisatrices de cet appareil numérique (85% des cadres et 89% des professions intermédiaires) que les personnes éloignées de l'emploi (62% des retraités et 74% des personnes au foyer).

On observe ainsi **des similitudes entre le profil des internautes les plus précautionneux et le profil des personnes exposées ou victimes d'escroquerie sur Internet et à la téléphonie**. Ce sont en effet les jeunes (18-29 ans), les individus les plus diplômés (diplômés du supérieur) et ceux issus des catégories socio-professionnelles dites supérieures (cadres, profession intellectuelle supérieure, profession intermédiaire) qui sont à la fois les plus précautionneux et les plus victimes ou concernées par ce type d'escroquerie. Par conséquent, un nombre de précautions adoptées élevé ne permet pas de réduire le risque d'exposition ou de victimation. La multiplication des usages d'Internet et l'utilisation fréquente de ce dernier et plus largement, des TIC, augmente le risque d'être concerné ou bien victime d'une escroquerie en ligne ou à la téléphonie. Les jeunes, les diplômés du supérieurs et les catégories professionnelles supérieures sont aussi les individus les plus compétents en matière numérique. On peut ainsi émettre l'hypothèse selon laquelle la compétence numérique permet de détecter plus facilement le risque d'escroquerie auquel un ménage est exposé et donc de se déclarer « victime ». Certains groupes de la population peuvent ainsi être victimes de ce type d'escroquerie sans en avoir toujours conscience.

[51] CRÉDOC. *Baromètre du numérique,* édition 2010.
[52] CRÉDOC. *Baromètre du numérique*, édition 2021.

CONCLUSION

Ce cahier de recherche avait pour enjeu principal de mesurer et de présenter l'ampleur de l'escroquerie en ligne et à la téléphonie en France. Il n'existe aujourd'hui, aucun chiffre permettant de couvrir une telle réalité. En revanche, l'analyse croisée des différentes sources officielles sur la criminalité que sont *l'état 4001,* l'enquête *Cadre de vie et sécurité* et le *Rapport* annuel de l'Observatoire des moyens de paiement avec les enquêtes du CRÉDOC et de la Commission Européenne a permis de mieux appréhender le phénomène. Nous savons désormais qu'au moins une personne sur cent est victime d'escroquerie sur Internet ou par téléphone en France chaque année et près de la moitié de la population est exposée à ces pratiques illicites. Cette analyse croisée des sources administratives et publiques révèle également qu'Internet est devenu le lieu privilégié des escroqueries en général et notamment des escroqueries bancaires. Il s'avère que peu de victimes portent plainte. La population semble considérer les pouvoirs publics comme incapables de réparer le préjudice auquel elle fait face et peut **préférer chercher le soutien** des internautes sur le web.

Le second enjeu de ce cahier de recherche était l'analyse du lien entre les précautions adoptées par les internautes pour protéger leurs données personnelles et la victimation. Dans un contexte où la majeure partie de la population est amenée à utiliser Internet, on comprend que l'escroquerie en ligne et à la téléphonie n'est pas l'affaire de quelques-uns, mais bien l'affaire de tous. Les données du *Baromètre du Numérique* ont révélé qu'un nombre élevé de précautions adoptées sur Internet ne permet pas systématiquement d'être moins exposé ou victime d'une situation d'escroquerie en ligne ou à la téléphonie. Les plus précautionneux se déclarent également les plus compétents, les mieux équipés et les plus utilisateurs du web. Mécaniquement, ils sont davantage exposés et victimes de ce type de criminalité que des personnes moins compétentes, moins équipées et moins utilisatrices. Et les précautions prises n'arrivent pas à empêcher les incidents. Par ailleurs, l'enquête révèle une **attitude ambivalente** des internautes vis-à-vis de la protection de leurs données personnelles. Même si l'inquiétude est grande d'être confronté à des situations d'escroqueries sur Internet ou par le biais de leur téléphone, **la grande majorité de la population n'est en effet pas prête à renoncer à des services en ligne aujourd'hui gratuits** ou à restreindre leur utilisation pour protéger ses données personnelles, justement utilisées par les auteurs d'escroquerie pour les tromper.

Avec la poursuite de la dématérialisation des démarches administratives, du recours croissant des entreprises aux outils numériques et l'augmentation des achats en ligne, on peut s'attendre à une **progression** du nombre de tentatives d'escroquerie sur Internet. L'approfondissement de la recherche sur l'escroquerie en ligne et à la téléphonie apparaît comme essentielle afin d'établir **une mesure plus précise** de l'ampleur de ce type de criminalité. L'enjeu est en effet de fournir aux pouvoirs publics une expertise solide afin de les soutenir dans leur mission de protection de la population. L'augmentation de l'exposition des Français à ce type de criminalité soulève aussi la question de la **responsabilité des différents acteurs.** Les politiques publiques s'appuient en effet aujourd'hui sur des politiques de prévention et d'information, qui font porter le poids du risque sur les individus. Ceux-ci ont beau être, nous l'avons vu, de plus en plus experts et précautionneux à mesure qu'ils s'emparent de nouveaux usages, cela n'enraye pas réellement la dynamique. A côté de la nécessaire sensibilisation et formation des consommateurs aux bonnes pratiques, l'accélération de la numérisation de notre société pose la question de **la responsabilisation légale de tous les acteurs de la chaine : des plateformes et sites internet en passant par les opérateurs télécom et les fabricants de matériel.** La multiplication de mini arnaques portant sur des montants très faibles, mais touchant de très nombreuses victimes, invite également à **réfléchir des modalités d'appui juridiques accessibles, mutualisées** via – par exemple - des recours collectifs ? - facilités par la puissance publique.

BIBLIOGRAPHIE

Auray, Nicolas. « Manipulation à distance et fascination curieuse. Les pièges liés au spam », *Réseaux,* vol. 171, no. 1, 2012, pp. 103-132.

Benbouzid, Bilel, et Sophie Peaucellier. « L'escroquerie sur Internet. La plainte et la prise de parole publique des victimes », *Réseaux*, vol. 197-198, no. 3-4, 2016, pp. 137-171.

Benbouzid, Bilel, et Sophie Peaucellier. « L'escroquerie bancaire en France métropolitaine : profils de victimes et décisions de renvoi à la police », *Questions pénales*, XXIX, 1. 2016

Benbouzid, Bilel, et Daniel Ventre. « Pour une sociologie du crime en ligne. Hackers malveillants, cybervictimations, traces du web et reconfigurations du *policing* », *Réseaux*, vol. 197-198, no. 3-4, 2016, pp. 9-30.

Bianquis, Gaspard. « La protection juridique des données personnelles », *Regards croisés sur l'économie*, vol. 23, no. 2, 2018, pp. 156-160.

Pasquier, Dominique. « Classes populaires en ligne : des « oubliés » de la recherche ? », Réseaux, vol. 208-209, no. 2-3, 2018, pp. 9-23.