Cybercriminalité : risques et conséquences pour les données personnelles

26 novembre 2025

La CNIL a commandé un sondage sur la perception des Français vis-à-vis de l'utilisation de leurs données personnelles et du consentement à la publicité en ligne. Ce dernier volet d'une série de trois publications évoque les préjudices matériels pour les victimes de violations de données personnelles.

Le cybercrime lié aux données personnelles (par exemple une fuite ou un vol de données) est un phénomène largement connu et discuté, mais son impact pour les individus restent difficiles à mesurer.

Les estimations de son coût pour la société varient fortement selon les sources. Par exemple, en France Statista l'évalue à 119 milliards d'euros pour les organisations en 2024, tandis que le cabinet Asterès l'estime à 2 milliards pour l'année 2022. Face à ces écarts considérables, la CNIL a entrepris de mieux quantifier les coûts des différents **préjudices pour les personnes** (perte financière, changement de comportement) associés à l'utilisation frauduleuse de données personnelles. Elle s'est aussi attachée à analyser comment la nature des préjudices du cybercrime est susceptible d'induire **des biais comportementaux poussant à des attitudes risquées.**

Ces travaux font également écho à un thème déjà abordé dans le cadre d'une autre publication identifiant le sous-investissement dans la cybersécurité comme un problème structurel au sein des entreprises. La nouvelle enquête montre que **la nature même du risque cyber génère des biais comportementaux chez les individus, qui freinent la constitution d'un écosystème résilient face au cybercrime.**

Ces questions ont été étudiées par la CNIL, dans le cadre d'un sondage de Harris Interactive réalisé en ligne du 18 au 23 décembre 2024, sur un échantillon représentatif de 2 082 Français âgés de 15 ans et plus. Les répondants ont été interrogés pour savoir s'ils avaient subi une utilisation frauduleuse ou non contrôlée de leurs données personnelles, ainsi que sur les préjudices matériels ou immatériels qui en ont découlé.

Fréquence et gravité des cybercrimes liés aux données personnelles

Les résultats de ce sondage montrent que les incidents liés à l'utilisation non autorisée des données personnelles sont fréquents. **41 % des répondants ont déjà subi une utilisation frauduleuse de leurs données personnelles.** Parmi eux, **21 % ont subi un préjudice financier.**

Tous cas confondus, le préjudice financier moyen déclaré est de **740 euros.** L'atteinte menant au préjudice financier moyen le plus élevé est la **fraude à l'identité** (915 euros).

Des **données personnelles mal protégées** conduisent donc à des **préjudices réels**, bien évalués par les individus, et ayant pour eux un coût élevé, notamment pour les plus modestes.

UTILISATION FRAUDULEUSE DES DONNÉES PERSONNELLES	PRÉVALENCE	PART MENANT À UN PRÉJUDICE	PART MENANT À UN PRÉJUDICE MORAL (STRESS, ANXIÉTÉ)	PART MENANT À UN PRÉJUDICE FINANCIER	PRÉJUDIC FINANCIE MOYEN
Une fraude à l'identité	16 %	70 %	28 %	24 %	915 €
Un démarchage non sollicité	24 %	35 %	15 %	29 %	691 €
Une fraude ou tentative de fraude financière	5 %	65 %	26 %	75 %	592 €
Divulgation d'informations « compromettantes »	7 %	76 %	27 %	18 %	609 €
Du chantage ou du harcèlement	4 %	71 %	19 %	13 %	450 €

Utilisations frauduleuses des données personnelles perçues lors des trois dernières années par les répondants

Parmi les victimes de ces atteintes, 30 % les signalent à une autorité publique (police, CNIL, etc.). La réaction la plus fréquente consiste en **un changement de comportement visant à réduire le risque perçu, cité par 67 % des répondants.**

Ces incidents ont également un impact durable sur la confiance des individus : ils entraînent une défiance accrue ainsi qu'un renoncement à l'utilisation de certains services numériques, notamment les achats en ligne. Ainsi, **57 % des personnes ayant subi un préjudice au cours des trois dernières années**

ont renoncé à un service numérique par crainte d'un usage détourné de leurs données personnelles, contre 35 % dans la population générale.

Au-delà des pertes financières directes, **le cybercrime installe ainsi un climat de méfiance** envers l'économie numérique, qui freine les échanges commerciaux en ligne et amplifie son impact global tant pour les personnes que pour les entreprises. Il s'agit de **dommages indirects de cybercrimes**, une notion que la CNIL a déjà évoquée.

41 % des répondants **ont subi au moins une utilisation frauduleuse de leurs données personnelles** au cours des trois dernières années.

Plus d'1 personne sur 2 ayant subi un préjudice au cours des trois dernières années **ont renoncé à utiliser un service numérique par la suite.**

Préjudices : des conséquences financières inégalement réparties

La CNIL constate une **forte concentration des préjudices financiers** sur un nombre limité de répondants. Les 2 082 personnes interrogées ont déclaré un total de **131 614 euros de pertes**, soit 63 euros de perte moyenne par répondant. Cependant, cette moyenne masque une **forte disparité** : à elle seule, une personne a déclaré environ 20 000 euros de préjudices.

La moitié des individus subissant un préjudice financier subissent un préjudice inférieur à 200 euros, mais 14 % subissent un dommage supérieur à 1 000 euros, ce qui met en évidence la distribution très inégale des dommages du cybercrime.

Les incidents les plus graves apparaissent donc comme **des événements à la fois rares mais particulièrement sévères.**

Le graphique ci-dessous illustre ce phénomène en montrant la distribution des préjudices financiers dans la population.

Distribution des préjudices du cybercrime

Aide à lecture du graphique : le pic à gauche représente la majorité des individus qui ne subissent qu'un préjudice financier autour des 100 euros. Cependant, une minorité est touchée par des montants bien plus élevés, ce qui allonge fortement la queue de la distribution (à droite).

Ces chiffres illustrent par ailleurs la **pertinence et l'intérêt** – non seulement pour les entreprises, mais aussi pour les particuliers – **du développement des offres de cyberassurance** proposées par certains assureurs et courtiers, et peuvent contribuer aux réflexions de la statistique en la matière.

Comprendre les biais comportementaux liés au cybercrime pour ne pas en être victime

En économie expérimentale, il est fréquent de considérer que les individus ont tendance à relativiser la fréquence des évènements rares et à réduire les prises de risque lorsqu'ils font face à des pertes potentielles (Kahneman & Tversky, 1979). Sachant cela, on pourrait s'attendre à ce que les individus soient particulièrement préparés au risque de cybercrime.

Cependant, ce comportement ne s'applique que lorsque les probabilités des différents évènements sont explicitées aux individus (par exemple, les prévisions météorologiques). Or, pour de nombreux évènements, les individus estiment les probabilités à partir de leurs expériences passées. Dans ce cadre, a contrario, **la probabilité des évènements rares est sous-estimée**, c'est ce qu'on appelle la « disparité expérience-description » (« *description-experience gap* ») (Hertwig et al., 2004, Hertwig & Erev, 2009).

Dans le domaine de la cybersécurité, la probabilité d'un incident n'est jamais clairement observable, sauf via des enquêtes ayant, entre autres, comme objectif d'estimer celle-ci. **Les individus estiment donc le risque en fonction de leur propre expérience**, **ce qui crée une tendance à sous-estimer celui-ci.** Ainsi, de nombreux répondants au sondage de la CNIL ont indiqué que leur perception du risque s'était accrue après une **violation de données**. **La faible perception du risque avant l'incident biaise l'analyse bénéfice/risque des personnes et rend plus difficile l'incitation à recourir des mesures de protection adaptées.**

Au travers de cette étude et de ses publications régulières sur ce sujet, la CNIL souhaite **alerter les personnes sur la réalité de cette menace** pour adopter les comportements adaptés. Cette mission de sensibilisation complète les autres actions de la CNIL en matière de contrôle et de sanction des organismes ne protégeant pas suffisamment les données personnelles.

Le saviez-vous ?

Sur 1 000 lecteurs de cette publication, environ 13 subiront une utilisation frauduleuse de leurs données dans les trois prochaines années pour un préjudice financier supérieur à 1 000 euros.

Pour limiter la probabilité d'être victime et les conséquences négatives (financières, psychologiques…), adoptez dès à présent les réflexes essentiels pour vous protéger.

En savoir plus : Ma sécurité numérique

Articles en relation

- [1/3] Les Français sont-ils prêts à payer pour des services en ligne sans publicité ciblée ?
- [2/3] Monétisation des données personnelles : combien valent nos données ?

Pour approfondir

- Cybersécurité : les bénéfices économiques du RGPD
- Toutes les ressources de la CNIL sur la cybersécurité