



Le harcèlement numérique dans les relations

Rapport

Que sont les stalkerwares et les gens les reconnaissent-ils?

Table

Introduction.....	03
Que sont les stalkerwares et les gens les reconnaissent-ils?.....	04
Fractures démographiques et confusion des possibilités	05
Surveillance numérique et consentement.....	06
Abus numérique – quelle est l’ampleur du problème en France?.....	09
Personnel ou privé – quelles informations les Français partagent volontiers avec leurs partenaires?.....	10
Le problème des stalkerwares de manière générale.....	11
Comment les gens réagissent-ils aux stalkerwares?.....	12
Élimination d’un stalkerware – comment se protéger de la surveillance numérique ?.....	14
À propos de la recherche	16

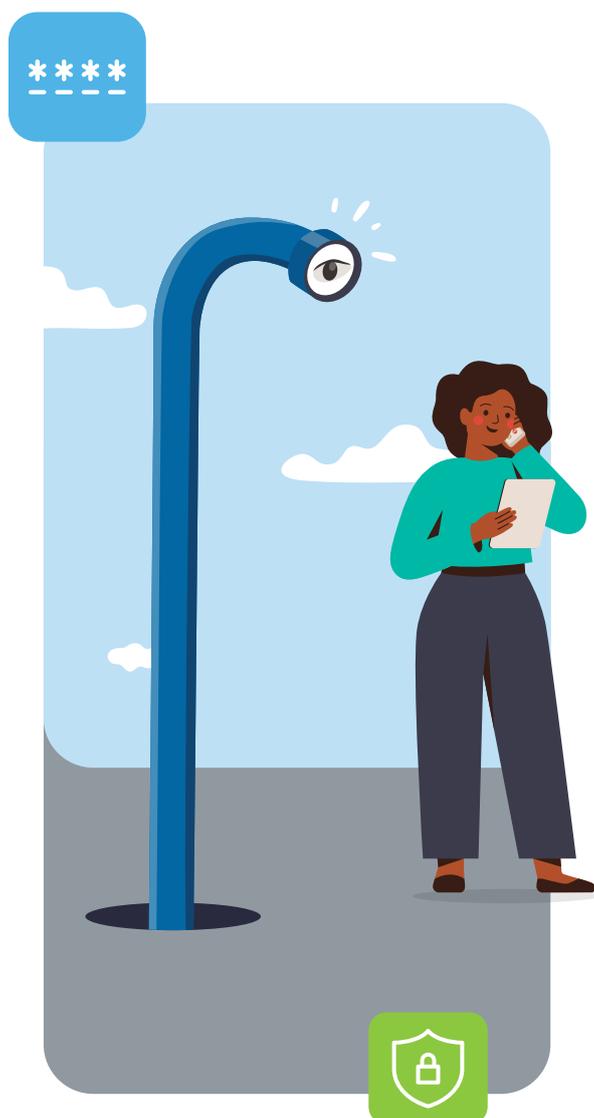


Introduction

En 2021, les utilisateurs sont plus connectés que jamais, en grande partie grâce à la prévalence de la technologie numérique et au large éventail de canaux de communication mis à disposition par les appareils intelligents. Les utilisations positives de cette technologie sont nombreuses : elle nous rapproche, elle réduit l'incidence de la distance géographique et elle facilite l'établissement de nouvelles relations, pour n'en citer que quelques-unes. Toutefois, malheureusement, la facilité d'accès à d'autres personnes et à leurs informations personnelles présente également le risque de faire l'objet d'une utilisation abusive.

Dans certaines circonstances, la technologie numérique peut être utilisée par des acteurs immoraux dans le cadre d'une campagne plus large de violence domestique. Cela peut prendre la forme, par exemple de l'utilisation au sein même d'un couple, d'applications de surveillance, d'espionnage, connues sous le nom de « stalkerware » pour suivre les allées et venues de son/sa conjoint/e, ses interactions et son utilisation d'Internet.

Ce rapport analyse les recherches entreprises par SAPIO, au nom de Kaspersky et de plusieurs ONG travaillant dans le domaine de la violence domestique, afin de mieux comprendre l'omniprésence des stalkerwares et la façon dont leur effet toxique peut être atténué de manière sûre et efficace.



Le but de l'étude a été de mesurer l'ampleur de l'utilisation des stalkerwares (ou « spouseware », comme on les appelle parfois) et de collecter des données pour aider les acteurs de la lutte contre la violence domestique à mieux comprendre le sujet et à améliorer le soutien apporté aux victimes.

Voici les objectifs:

- Comprendre combien de personnes sont conscientes de l'existence des stalkerwares et de leurs fonctionnalités
- Déterminer dans quelle mesure les gens sont prêts à surveiller leur partenaire
- Découvrir les types de données que les gens sont prêts à partager et celles qu'ils préfèrent garder secrètes
- Comprendre combien de personnes ont déjà été victimes de stalkerwares
- Savoir quels appareils sont couramment utilisés par les agresseurs pour surveiller leurs victimes

Notre recherche a démontré qu'en France, une grande partie des gens n'a pas conscience de l'existence de tels outils. 49% des Français indiquent savoir ce qu'est un stalkerware.

Que sont les stalkerwares et les gens les reconnaissent-ils?

Le stalkerware est un logiciel de surveillance que les gens utilisent généralement pour espionner leur partenaire ou conjoint. Il est accessible facilement dans le commerce et facile à installer sur le smartphone d'autrui. Un agresseur n'a besoin d'accéder physiquement au téléphone de sa victime qu'une seule fois pour activer un stalkerware et, comme le montre ce rapport, la plupart des gens font suffisamment confiance à leur partenaire intime pour lui donner cette possibilité à un moment donné.

58% des Français indiquent d'ailleurs connaître le mot de passe du téléphone de leur conjoint. Bien qu'il soit clairement contraire à l'éthique, le stalkerware se trouve dans une zone grise juridique. Souvent, les applications de stalkerware ou de spouseware fonctionnent sous l'apparence d'applications de contrôle parental ou de solutions antiviol, ce qui leur permet également de rester accessibles via des places de marché d'applications, comme Android Apps. Cependant, dans quelle mesure le grand public est-il conscient de l'existence et de la facilité d'achat d'applications dotées de ce type de fonctionnalités ?

Nos recherches ont montré qu'à l'échelle internationale, la majorité des gens ne savent pas ce qu'est un stalkerware. 60 % des personnes interrogées dans le cadre de notre sondage ont répondu ainsi. 51% des Français ne savent pas, ou ne sont pas sûrs de savoir de quoi il s'agit. Cependant, il reste une minorité non négligeable de personnes qui savent à quoi servent ces outils. Une interprétation particulièrement pessimiste pourrait suggérer que près de la moitié de la population interrogée a personnellement été confrontée aux stalkerwares, que ce soit en tant que victime ou en tant qu'utilisateur.

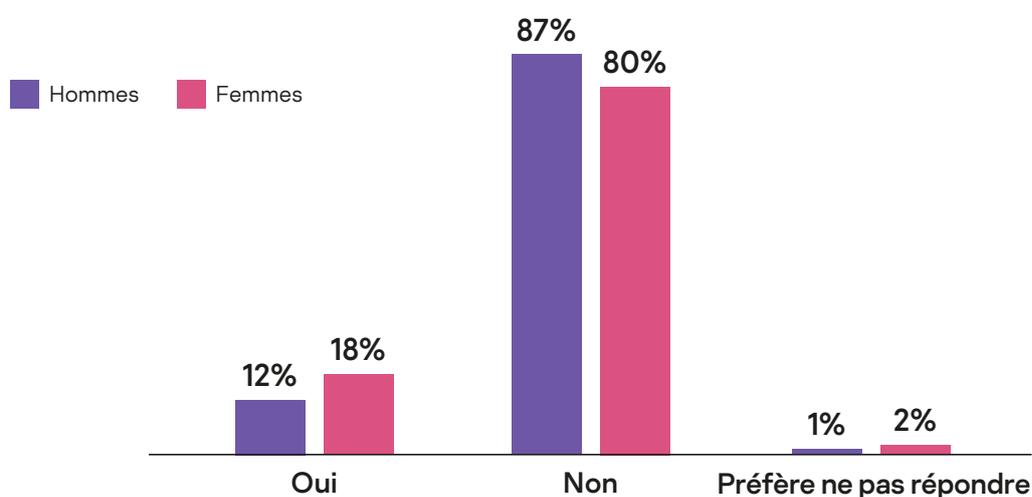
Toutefois, il n'est pas nécessaire d'avoir une expérience directe de quelque chose pour en connaître le concept. Il faut également tenir compte du fait que le nom « stalkerware » est assez explicite et que les gens peuvent déduire l'utilité des stalkerwares à partir de leur familiarité avec les logiciels espions. Cela dit, même une interprétation optimiste laisse penser que les stalkerwares sont assez répandus pour causer des atteintes à la vie privée de milliers de personnes, et doivent être pris au sérieux et contrôlés en conséquence.



Fractures démographiques et confusion des possibilités

Il existe d'importantes disparités à prendre en compte en ce qui concerne le niveau de sensibilisation aux stalkerwares. Tout d'abord, les hommes sont plus nombreux à connaître l'existence des stalkerwares que les femmes (44% contre 36% respectivement, ces chiffres montent à 56% des hommes français et 42% des femmes françaises). Deuxièmement, les jeunes sont plus susceptibles de connaître les stalkerwares que les personnes plus âgées : 46% des personnes âgées de 16 à 34 ans les reconnaîtraient, contre seulement 28% des personnes âgées de 55 ans et plus (respectivement 54% et 37% en France).

Avez-vous déjà été victime de violence ou d'abus de la part de votre partenaire?



Données françaises – panel de 1002 répondants.

Si l'on examine les données de plus près, on constate qu'il existe quelques raisons potentielles à cela. Plus d'hommes (10%) que de femmes (8 %) ont admis avoir installé un stalkerware sur le téléphone de leur partenaire. Et comme les stalkerwares fonctionnent de manière clandestine, il est logique que ceux qui les utilisent le plus fréquemment soient plus conscients de leur existence que ceux qui sont plus susceptibles d'en être victimes. En France, si les mêmes tendances se dessinent avec plus d'hommes ayant déjà installé des logiciels espions sur les téléphones de leurs conjointes que l'inverse (10% des Français contre 5% des Françaises), il est intéressant de constater que les hommes sont également plus inquiets d'être espionnés que les femmes. 15% des Français ont ainsi déjà suspecté leur conjointe d'avoir installé de tels outils, contre 11% des Françaises.

De manière générale, les femmes sont nettement plus susceptibles que les hommes d'avoir été victimes de violences domestiques de la part de leur partenaire (30% contre 19%), même si cet écart est moins marqué en France qu'à l'échelle internationale (18% de femmes victimes de violences contre 12% d'hommes).

Erica Olsen, directrice du projet Safety Net du National Network to End Domestic Violence (NNEDV), lance un avertissement qui ne doit pas être pris à la légère:

“Une personne violente peut accroître ou intensifier son comportement violent si elle est confrontée ou lorsque le stalkerware est supprimé. Les victimes doivent faire ce qui leur semble le plus sûr sur le moment et s’adresser à un fournisseur de services aux victimes pour s’informer sur les options possibles.”

Cependant, même parmi ceux qui connaissent les stalkerwares, le niveau de sensibilisation à certaines fonctionnalités est plus élevé que d’autres. Intéressons-nous au cas de la France. 75% des Français qui connaissent l’existence des stalkerwares (moins de la moitié du panel pour rappel) sont au courant que les stalkerwares offrent des fonctionnalités comme la surveillance des activités sur Internet. 69% savent qu’ils permettent l’enregistrement de la localisation et 59% savent qu’ils permettent l’enregistrement vidéo et audio. En revanche, seul un tiers (33%) est au courant qu’un stalkerware peut informer l’auteur de l’infraction lorsqu’une victime tente de le désinstaller. Preuve en est, 42% des Français désinstalleraient immédiatement l’application s’ils venaient à la découvrir sur leur téléphone.

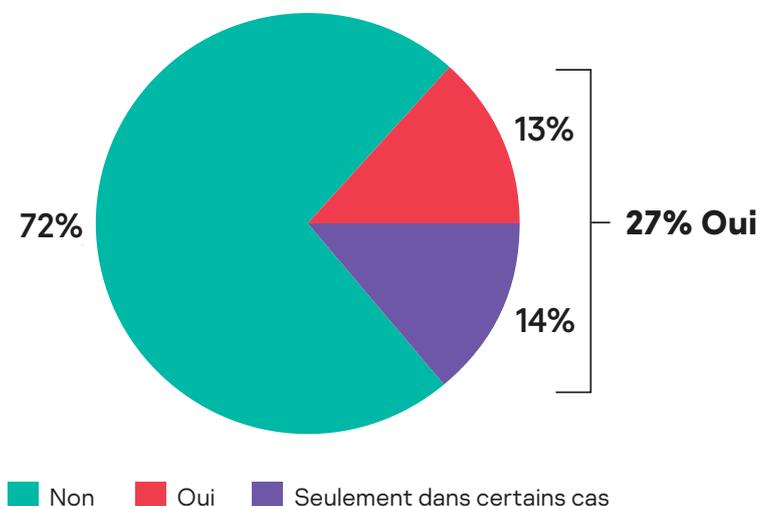
Il est donc clair qu’il y a encore du travail à faire en matière d’éducation de la population au sens large (les chiffres internationaux suivent les mêmes tendances) sur l’existence des stalkerwares et des particularités de leur fonctionnement en appliquant une approche centrée sur la victime. Par conséquent, les souhaits et les besoins des victimes sont au cœur du problème.

Surveillance numérique et consentement

Le débat sur les stalkerwares (et plus généralement sur les logiciels de surveillance) tourne autour de la question du consentement. Heureusement, la grande majorité des personnes ayant répondu à notre sondage (70%) ne pense pas qu’il soit acceptable de surveiller son partenaire sans son consentement (c’est le cas de 72% des Français). Néanmoins, il reste une minorité importante et préoccupante (30% et 27% des Français) qui pense que cette pratique est acceptable (du moins dans certaines circonstances).

Est-il acceptable de surveiller votre partenaire sans son consentement?

Données françaises – panel de 1002 répondants.





Ce chiffre est particulièrement alarmant parce qu'il suggère qu'une partie des 21% (1 personne sur 5 à l'échelle internationale, donc) de personnes interrogées qui soupçonnent un partenaire intime de les avoir espionnées à l'aide d'une application ont probablement raison. Ce nombre est également plus élevé que ce que prévoient les experts qui travaillent directement avec les victimes d'abus, notamment parmi les 13% de personnes qui pensent qu'il est acceptable de surveiller leur partenaire sans ajouter la mention « dans certaines circonstances » (14% en France). Les experts soulignent que les auteurs d'abus utilisent souvent des motifs comme des préoccupations en matière de sécurité pour justifier à tort leur harcèlement.

Le sondage nous montre que près de deux tiers des personnes qui estiment qu'il n'y a pas de mal à surveiller leur partenaire le feraient si elles pensaient qu'il est infidèle (64%), si cela était lié à leur sécurité (63%) ou si elles pensaient qu'il était impliqué dans une activité criminelle (50%). La mention des préoccupations liées à l'infidélité, en particulier, illustre la nature abusive, coercitive et contrôlante de l'utilisation des stalkerwares. Comme le souligne Berta Vall Castelló, responsable de la recherche et du développement du Réseau européen pour le travail avec les auteurs de violences (WWP EN), cette suspicion n'est pas une raison justifiable, même si un nombre inquiétant de personnes le croient.

Il existe également des défauts évidents dans la justification censée porter sur la sécurité du partenaire. Si la surveillance est véritablement due à des raisons de sécurité, l'autre partie devrait en être informée, y consentir et être en mesure de supprimer l'application comme elle le souhaite. Quant au soupçon d'activité criminelle, il existe des moyens bien plus évidents et efficaces de le combattre que d'utiliser un logiciel de surveillance.



« Ces résultats mettent en évidence un idéal de l'amour romantique, particulièrement fort chez les adolescents, où les partenaires n'ont pas droit à l'intimité, et où tout partager avec son partenaire est une façon de présenter son amour ainsi que sa confiance », commente Berta Vall Castelló, responsable de la recherche et du développement du WWP EN.

L'utilisation non consensuelle de stalkerwares est un problème beaucoup plus répandu dans certains pays que dans d'autres. L'Inde (45%), la Malaisie (31%) et la Chine (27%) sont les pays où les personnes ont le plus tendance à penser qu'il est acceptable de surveiller ses partenaires intimes à leur insu. En France, 14% des répondants indiquent que c'est acceptable de surveiller son partenaire à son insu, et 13% pensent que c'est acceptable dans certaines circonstances. Les citoyens du Portugal et de la Colombie (7%), de l'Espagne, de la République tchèque, du Mexique et du Pérou (6%) ainsi que de l'Argentine (5%) ont tendance à être moins d'accord avec cette affirmation. Ce résultat pourrait être dû en partie aux perceptions culturelles du droit à la vie privée. En effet, moins d'une personne interrogée sur quatre en Inde (24%) pense que tout le monde a droit à la vie privée, contre 65% en Espagne et au Mexique.

Lorsque le consentement est introduit dans la conversation, on constate une augmentation correspondante du nombre de personnes ouvertes à la surveillance de leur partenaire. Près de la moitié d'entre elles (48%, et 44% en France) seraient théoriquement prêtes à surveiller leur partenaire de manière consensuelle : 25% dans l'intérêt d'une « transparence totale » dans la relation (18% en France) et 24% dans certaines circonstances (s'il s'agit de sécurité physique ou si la surveillance est mutuelle).

Abus numérique – quelle est l'ampleur du problème en France?

En bref, l'abus numérique est un problème massif et répandu en France. 15% des Français indiquent avoir vécu une forme de violence de la part de son partenaire, bien que les hommes soient moins susceptibles d'avoir subi des abus (12%) que les femmes (18%). Les disparités de genre sont moins marquées en France qu'à l'échelle mondiale où 19% des hommes estiment avoir été victimes d'abus et violences au sein du couple contre 30% des femmes. En ce qui concerne les types de violence perpétrée, la violence psychologique est la forme la plus courante vécue par les Français (66%), suivie par la violence physique (52%), la violence économique (27%) et la violence sexuelle (24%).

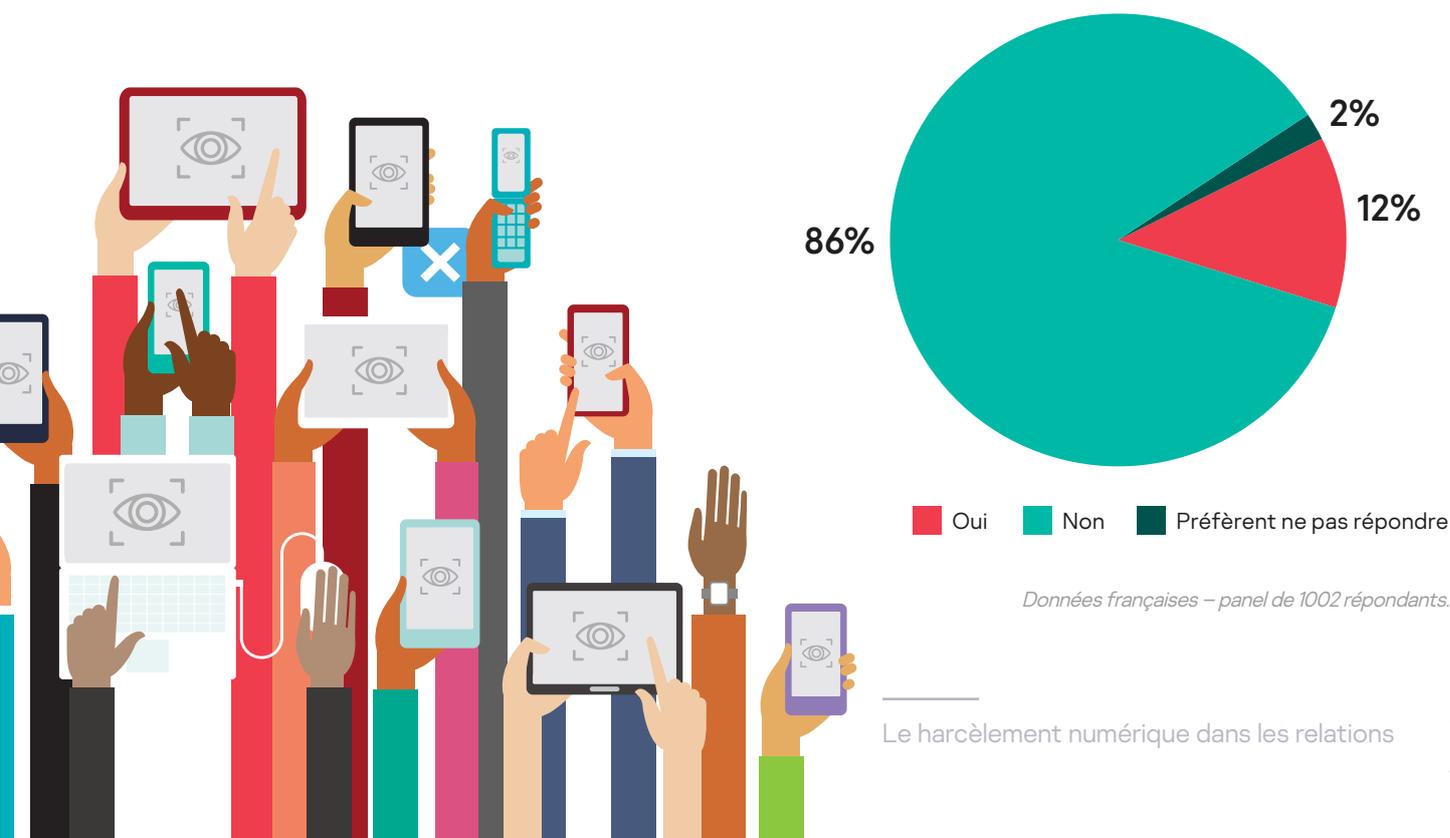
Les différences entre les hommes et les femmes sont intéressantes à observer, en France. Dans la plupart des cas, les femmes sont plus susceptibles d'être victimes de formes de violence ou d'abus. Elles sont 78% à indiquer avoir subi des violences psychologiques contre 47% pour les hommes, 58% victimes de violences physiques contre 43% pour les hommes, 26% à avoir subi des violences sexuelles contre 22% chez les hommes. En revanche, en ce qui concerne les violences économiques la tendance s'inverse et 34% des hommes victimes de violences ont subi des abus ou violences économiques contre 21% des femmes.

L'abus numérique par le biais de stalkerwares pourrait être un facteur clé de la violence psychologique. Si « seuls » 12% des Français estiment avoir été surveillés par le biais de la technologie, un Français sur 5 (21%) craint que son partenaire ne viole sa vie privée numérique.

La plupart des inquiétudes concernant la manière dont une telle atteinte à la vie privée pourrait se manifester portent sur les informations accessibles via un smartphone, et donc exposées au risque d'un stalkerware. Les informations numériques auxquelles les Français interrogés s'inquiètent le plus de voir leurs partenaires accéder sont les SMS (53%), les réseaux sociaux (46%) et les emails (35%).

C'est particulièrement déconcertant quand on constate que 34% des Français ayant déjà été espionnés l'ont été par le biais d'une application sur leur téléphone (50% à l'échelle du monde).

Avez-vous déjà été surveillé par le biais de technologies?



Personnel ou privé – quelles informations les Français partagent volontiers avec leurs partenaires?

La protection de la vie privée est une question complexe, car chaque personne a ses propres limites quant aux informations qu'elle est prête à divulguer à son partenaire ou auxquelles elle est d'accord de lui donner accès. Par exemple, plus de 6 Français sur 10 ont partagé le mot de passe de leur téléphone avec leur partenaire, et une proportion similaire (58%) connaît le mot de passe du téléphone de leur partenaire. Pour plus de la moitié des répondants (53%) il est également normal de partager les données de connexion aux services iCloud ou Google au sein de leur famille. Ces chiffres suggèrent que de nombreuses personnes sont d'accord que leur partenaire intime et/ou leur famille proche ait accès à leur vie numérique.



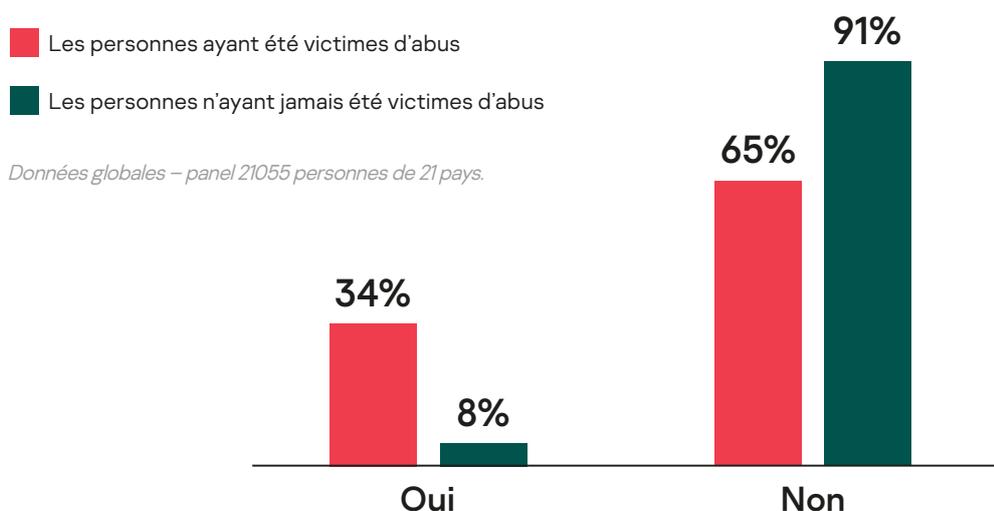
Mais encore une fois, il s'agit de circonstances consensuelles où la situation est mutuelle plutôt qu'unilatérale, et donc indicative d'une relation saine plutôt que d'une relation abusive. En outre, même en disposant d'un mot de passe, un partenaire devrait avoir un accès physique à un appareil pour consulter les informations qu'il contient. Dans une relation saine, cet accès pourrait être refusé, ou le mot de passe pourrait être mis à jour si le propriétaire de l'appareil changeait d'avis à tout moment.

Même dans les relations où l'un des partenaires ou les deux sont disposés à partager leurs informations numériques, certains types de données sont communiqués plus librement que d'autres. Plus d'un quart des Français ne partageraient jamais les enregistrements d'appels téléphoniques (28%) et 23% ne partageraient pas leur historique de navigation. En revanche, à peine 10% d'entre eux ne seraient pas disposés à partager des photos et 16% seulement seraient réticents à divulguer leur activité sur les réseaux sociaux ou l'accès à leur appareil photo. 36% des Français répondent d'ailleurs qu'ils ne « cachent » absolument aucune information numérique à leur conjoint.

Le problème des stalkerwares de manière générale

Les stalkerwares se développent particulièrement dans des circonstances où il existe une disparité entre le niveau d'accès aux informations qu'un partenaire souhaite obtenir et celui que l'autre souhaite divulguer : 15% des personnes dans le monde ont été invitées par leur partenaire à installer une application de surveillance, mais ce chiffre est disproportionnellement plus élevé chez les répondants qui ont subi des abus (34%) que chez ceux qui n'en ont pas subi (8%). Il s'agit peut-être de l'indication la plus claire du lien direct entre stalkerware et violence que notre recherche démontre.

Est-ce qu'un partenaire intime vous a déjà demandé d'installer une application de surveillance?



Les jeunes (entre 18 et 34 ans) sont également beaucoup plus susceptibles (21%) que les personnes âgées de 55 ans et plus (5%) d'avoir reçu une telle demande de la part d'un partenaire. Il s'agit là d'un autre élément clé à retenir : les stalkerwares sont liés aux abus, et les jeunes sont beaucoup plus vulnérables à leurs effets néfastes.

Une personne sur dix (9%, et 8% en France) admet avoir installé des applications de surveillance sur le téléphone de son partenaire

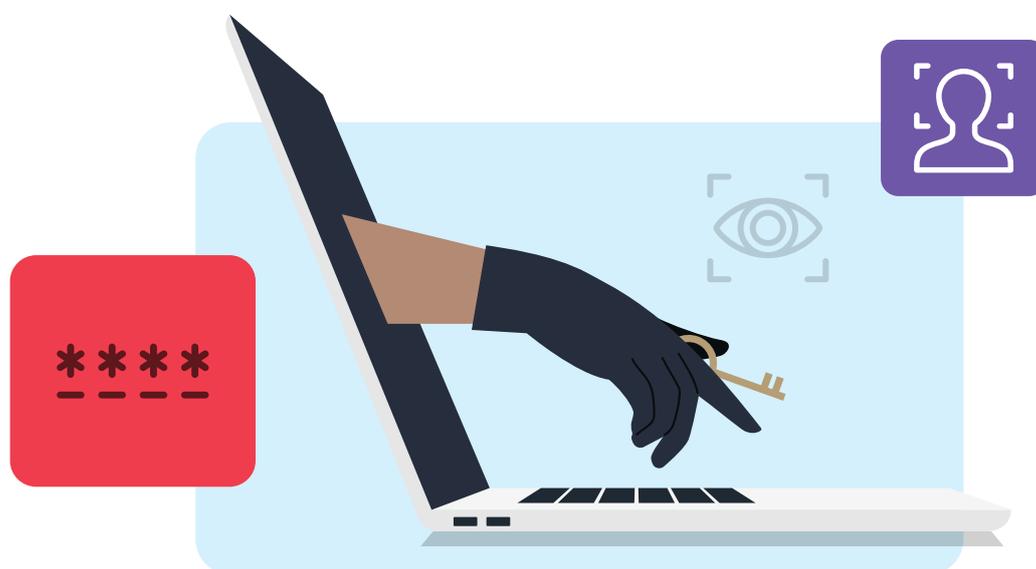
La plupart des personnes interrogées dans le cadre de notre sondage (84%) n'autorisent pas volontairement leur partenaire à installer ni à paramétrer leur téléphone. Toutefois, il existe des disparités géographiques considérables à cet égard. Par exemple, plus d'un tiers des personnes interrogées en Inde (38%) affirment que leur partenaire installe ou définit des paramètres pour leur téléphone, alors que seulement 7% des personnes interrogées en Australie sont du même avis (14% en France).

La proportion de personnes qui franchissent les limites et tentent quand même d'accéder à ces informations (ou ne posent pas la question au départ) est assez déconcertante: une personne sur dix (9%, et 8% en France) admet avoir installé des applications de surveillance sur le téléphone de son partenaire et 9% des personnes (8% des Français) ont utilisé des fonctionnalités de smart home pour surveiller leur partenaire sans son consentement.

Comment les gens réagissent-ils aux stalkerwares?

Quand on pose la question à nos répondants de leur réaction s'ils découvraient un logiciel espion dans leur téléphone, on obtient des réponses très variables. Ce résultat n'est pas surprenant, car il reflète l'énorme variation des circonstances personnelles dans lesquelles se trouvent les personnes du point de vue de leur niveau de stabilité et de vulnérabilité, et des réseaux de soutien dont elles disposent, ainsi que le contexte plus large des attitudes culturelles à l'égard de la violence et du comportement dans les relations.

Environ la moitié (50%) des personnes enquêteraient si elles découvraient une application de surveillance sur leur appareil et affronteraient la personne qui l'a installée (c'est le cas pour 48% des Français). La plupart des répondants à notre enquête (83%, mais seulement 76% en France) en parleraient avec leur partenaire s'ils découvraient qu'une application de surveillance a été installée sur leur téléphone sans leur consentement. Cependant, le fait de tenir tête à un partenaire dans cette situation ne fera qu'accroître le risque auquel la victime de stalkerware est confrontée, ce que les experts des organisations de lutte contre les violences domestiques déconseillent fortement. Cela met en évidence le travail nécessaire pour former, éduquer et soutenir les gens face à des problèmes complexes relatifs aux stalkerwares.



Seuls 17% des répondants appelleraient une ligne d'assistance ou se rendraient dans un centre de soutien dans cette situation. En France, ce chiffre n'est que de 14%. Parmi les raisons possibles, on peut citer la faible reconnaissance des stalkerwares comme un véritable problème lié à la violence entre partenaires intimes ou à un manque de compréhension du type de soutien que ces services peuvent offrir.

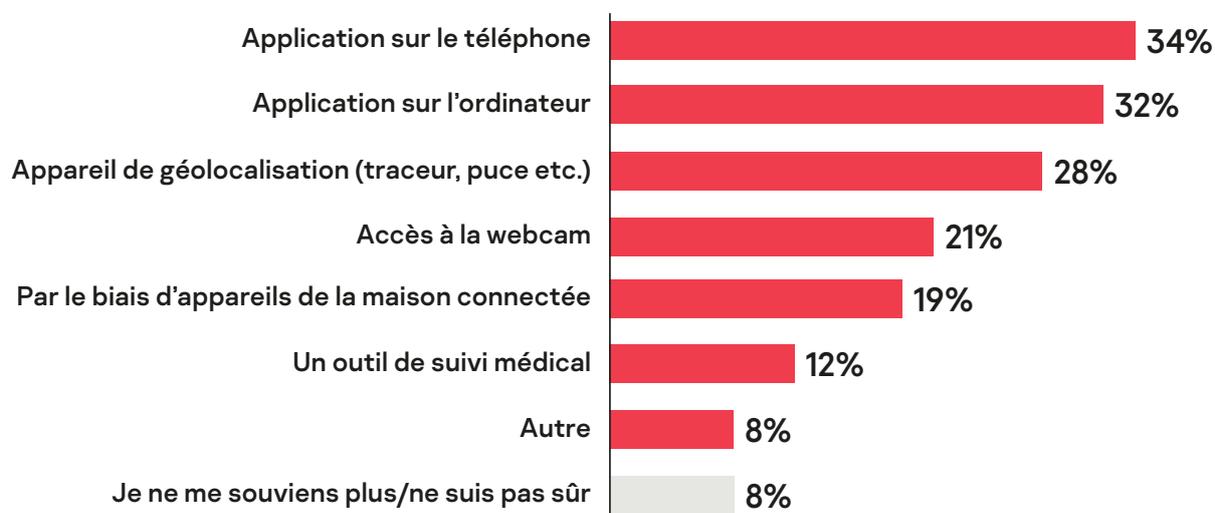
« Les victimes de violences domestiques qui affrontent leur partenaire après avoir trouvé un stalkerware sur leur téléphone peuvent aggraver le risque et s'exposer à des dommages graves. Le faible nombre de répondants qui appelleraient une ligne d'assistance ou visiteraient un centre de soutien est inquiétant. Dans les cas de contrôle coercitif par un partenaire, il est crucial d'obtenir le soutien des services d'aide aux victimes, afin de procéder selon un plan de sécurité élaboré avec des professionnels », conseille Berta Vall Castelló du WWP EN.



Parmi les personnes interrogées qui n'affronteraient pas leur partenaire si elles découvraient une application de surveillance sur leur smartphone, un quart explique que discuter de la situation ne servirait à rien (26%, et 33% en France), qu'elles n'auraient aucun moyen de prouver que leur partenaire est responsable (24% et 23% en France) ou qu'elles préféreraient une autre stratégie de sortie (24% et 15% en France). Ces raisons sont préoccupantes et indiquent une relation malsaine, avec une forte possibilité de pratiques abusives plus larges.

Si l'un des partenaires ne se sent pas capable de discuter d'un sujet qui dépasse ses limites personnelles avec son partenaire, il est probable qu'il craigne les conséquences d'une telle discussion. Même si ces personnes estiment que le fait d'en discuter ne changerait rien, leur relation n'est manifestement pas une relation où leur autonomie et leurs préférences sont valorisées. Préférer une stratégie de sortie différente est une réaction recommandée, et certainement une réaction très sensée lorsqu'une personne craint pour sa sécurité. Mais comment ces personnes peuvent-elles s'y prendre exactement?

Par quelles technologies avez-vous été espionnés?



Données françaises, panel de répondants ayant indiqué avoir déjà été surveillés par la technologie.

« Lorsque le stalkerware est utilisé dans le cadre d'abus domestiques ou de violence entre partenaires intimes, il peut indiquer que l'agresseur est très autoritaire et, ce qui est inquiétant, cela peut indiquer que la violence peut s'aggraver. J'invite instamment toute personne victime de harcèlement, que ce soit dans la vie réelle ou par le biais d'un stalkerware, et qui estime qu'il ne serait pas sûr ou qu'il serait dangereux d'affronter son agresseur, à s'adresser à une organisation de lutte contre la violence domestique pour obtenir des conseils ainsi qu'un soutien », déclare **Karen Bentley, PDG de WESNET et experte en sécurité technologique.** « Le projet [The Safety Net](#) mené par NNEDV aux États-Unis ainsi que [WESNET](#) en Australie proposent également des boîtes à outils sur la sécurité en ligne et la protection de la vie privée qui donnent des conseils aux victimes sur l'utilisation abusive des technologies dans le cadre de la violence domestique », ajoute-t-elle.



Élimination d'un stalkerware – comment se protéger de la surveillance numérique?

Les résultats de la recherche présentent sans aucun doute que les stalkerwares représentent un problème désagréable et pernicieux. Alors, quels sont les principaux indicateurs qui montrent que votre appareil peut être surveillé ? Bien que les applications d'espionnage tentent de se dissimuler, la plupart révèlent leur présence d'une manière ou d'une autre. Les données mobiles s'épuisent plus vite que prévu ou l'appareil se décharge tout aussi rapidement sont deux avertissements. Si vous remarquez l'un ou l'autre de ces problèmes, soyez sur vos gardes et vérifiez quelles applications consomment les ressources de votre téléphone.

De même, regardez quelles sont les applications qui accèdent à votre localisation. Si vous ne trouvez rien sur votre téléphone Android, mais que vous soupçonnez toujours quelqu'un de vous espionner, vérifiez quelles applications ont accès à l'accessibilité (Paramètres -> Accessibilité).

L'accessibilité permet aux applications de fouiller dans d'autres programmes, de modifier les paramètres et de faire de nombreuses autres actions en agissant comme l'utilisateur. Cette autorisation est donc très utile pour les stalkerwares. L'accessibilité est l'une des autorisations les plus dangereuses d'Android. Nous vous recommandons de ne donner ce type d'accès qu'à votre utilitaire antivirus et à rien d'autre.

Protégez votre téléphone par un mot de passe fort que vous ne partagez jamais avec votre partenaire, vos amis, ni vos collègues.



D'autres méthodes de détection consistent à utiliser une solution de cybersécurité pour vos appareils mobiles, comme Kaspersky Internet Security for Android ou TinyCheck (sous la supervision d'un organisme de service), comme indiqué [ici](#). Si l'une des méthodes ci-dessus détecte un logiciel espion sur votre smartphone, réfléchissez-y à deux fois avant de le supprimer. La personne qui l'a installé le remarquera, et cela pourrait aggraver la situation. La désinstallation du programme pourrait également effacer des preuves dont vous pourriez avoir besoin plus tard.

Comme pour toutes les questions de sécurité, prenez d'abord des mesures de protection. Par exemple, si un partenaire potentiellement violent vous surveille, avant de faire quoi que ce soit avec le stalkerware, contactez un centre d'aide aux victimes de violences domestiques (pour en savoir plus, cliquez [ici](#)).

Dans certains cas, il est plus facile de remplacer complètement votre smartphone et de vous assurer que personne ne pourra installer d'applications d'espionnage sur le nouvel appareil. Pour éviter d'être victime d'un stalkerware, Kaspersky recommande ce qui suit:

- Protégez votre téléphone par un mot de passe fort que vous ne partagez jamais avec votre partenaire, vos amis, ni vos collègues.
- Modifiez les mots de passe de tous vos comptes et ne les partagez pas non plus avec qui que ce soit.
- Téléchargez des applications uniquement à partir de sources officielles, comme Google Play ou la boutique App Store.
- Installez immédiatement une [solution de sécurité fiable](#) et procédez régulièrement à une analyse de l'appareil. Toutefois, cette étape ne doit être réalisée qu'après avoir évalué le risque pour la victime, car l'auteur de l'infraction peut remarquer l'utilisation d'une solution de cybersécurité.
- Ne vous précipitez pas pour supprimer un stalkerware s'il est détecté sur l'appareil, car l'agresseur pourrait le remarquer. Il est très important de prendre en compte le fait que l'agresseur peut représenter un risque pour la sécurité. Dans certains cas, la personne peut intensifier ses comportements abusifs en guise de réponse.
- Pour obtenir de l'aide et planifier votre sécurité, contactez les autorités locales ainsi que les organisations de services qui soutiennent les victimes de violence domestique. Une liste des organisations concernées dans plusieurs pays est disponible sur le site www.stopstalkerware.org.

Pour en savoir plus à propos des stalkerwares et de la manière d'y faire face, consultez le site de la [Coalition Against Stalkerware](#), qui réunit des organisations de lutte contre les violences domestiques et la communauté de la sécurité pour lutter contre cette menace.

À propos de la recherche

Le sondage a été réalisé auprès de 21 055 personnes de 21 pays qui sont actuellement en couple ou l'ont été dans le passé. Les données françaises proviennent d'un panel de 1002 personnes.

Au niveau mondial, les résultats sont précis à $\pm 0,7\%$ avec des limites de confiance de 95%, en supposant un résultat de 50%.

Les entretiens ont été réalisés en ligne par Sapio Research en septembre 2021 à l'aide d'une invitation par courriel et d'un sondage en ligne.



Audience | Brand | Content Research



Le harcèlement numérique dans les relations

Rapport

kaspersky

BRING ON
THE FUTURE