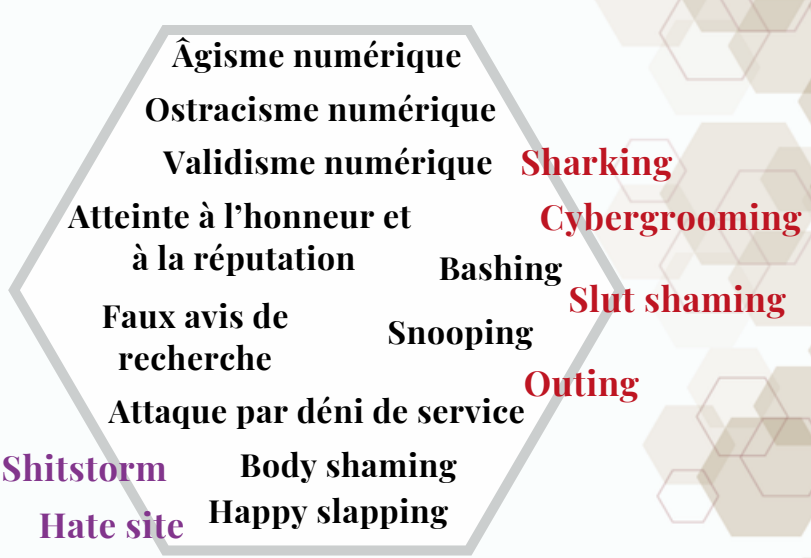
PROJET CYBERNETIC

SNOOPING

Etiologie des pratiques de cyberharcèlement



POUVOIR

SYNONYMES

- Cyber-espionnage
- Espionnage numérique

Définition

Concept-clé :

Le *snooping* désigne la pratique dissimulée et intrusive de chercher, recueillir ou surveiller en ligne des informations privées ou confidentielles sur une personne (par le biais de ses communications, de ses activités, de ses déplacements, de ses dossiers personnels, etc.), sans son consentement.

Il connaît une expansion significative dans les **relations intimes**, où la surveillance des usages et pratiques de son ou sa partenaire (ou ex), à son insu, est assimilée à une forme manifeste de **cybercontrôle**, dont l'objectif premier vise à connaître et vérifier régulièrement au moyen des outils numériques, ses **agissements** et ses **relations sociales**.

Si les dispositifs d'espionnage numérique foisonnent dans les contextes de **violences conjugales** et sont particulièrement révélateurs de mécanismes subtils d'hypercontrôle (Chatterjee, 2018), des études plus récentes mettent en évidence une tendance selon laquelle les **femmes** sont plus enclines à pratiquer le *snooping*, et ce phénomène est particulièrement répandu parmi les **jeunes adultes** (âgés de 18 à 25 ans).

Mais cette **cybersurveillance** ne se limite pas à la sphère privée et peut également s'exercer sans autorisation appropriée dans un cadre **professionnel**, que ce soit à l'encontre d'un collègue, d'un employé, d'une entreprise voire d'une entité gouvernementale.

Ce qu'il faut retenir...

Une recherche empirique menée par un collectif de scientifiques de Cornell Tech (Chatterjee, 2018) sur les **dispositifs espions et de surveillance** utilisés dans le contexte de **violences conjugales** démontrent que plusieurs procédés numériques peuvent être déployés par les agresseurs.

- **Les logiciels espions**, difficilement détectables sur un téléphone (pour certains aucune icône n'est apparente), peuvent en revanche s'installer dès lors qu'il y a un accès physique au téléphone de la victime, ce qui est facilité dans le cadre d'une relation de couple. Cette cybersurveillance à l'insu de la victime permet de prendre connaissance des appels et messages entrants/sortants, de vérifier sa présence sur les différents réseaux sociaux (WhatsApp, Facebook, Messenger, Instagram, Telegram, Tinder, etc.), d'effectuer un suivi GPS, d'avoir accès à certaines données internet tels que l'historique de navigation, les signets de sites web, les réseaux wifi, les emails, le calendar activités, des captations vidéo ou audio, etc.

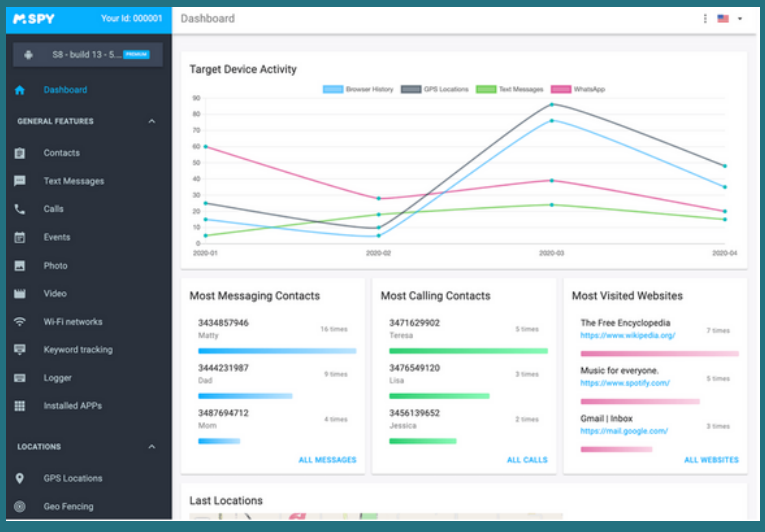
- Certains **logiciels ou applications** de type anti-vol de téléphone, antivol de clé tel que AirTag, peuvent être **détournés de leur usage** en vue de surveiller les activités du ou de la partenaire (ou ex).

- Des applications déjà installées sur le téléphone qui activent la géolocalisation (Google maps par exemple) et dont l'historique peut être consulté à distance peuvent être instrumentalisées pour permettre également de surveiller les déplacements de la victime. Seul un accès au mot de passe du cloud de sa ou son conjoint est nécessaire.

- L**a commande à distance d'appareils connectés** peut également être activée, tels que les caméras de surveillance des entrées et de sorties d'un immeuble, les appareils d'assistance personnelle domestiques (Alexa d'Amazon) pour écouter les conversations, etc.

« Je ne me suis rendue compte de rien. Plus de 4 mois qu'il violait mon intimité en lisant tous mes mails et textos grâce à un logiciel espion ! »

Un exemple concret :



Aux origines...

L'émergence des nouvelles technologies a souvent été pointée du doigt comme principale responsable de la surveillance massive dans notre société moderne. Mais les ***surveillance studies*** ont largement rappelé que ces pratiques étaient déjà présentes dans différents contextes, tels que la religion, la politique et la société, bien avant l'introduction et le déploiement des avancées numériques. Pour plusieurs auteurs, la **religion** et ses préceptes ont joué un rôle significatif dans la préparation des populations à accepter et tolérer la surveillance massive que nous connaissons aujourd'hui. Les croyances religieuses ont souvent enseigné que **Dieu** était **omniscient** et **omniprésent**, observant les actions de chacun et prononçant un jugement ultime. Cette idée d'une **surveillance divine** a inculqué dans les esprits une notion de surveillance constante et d'obligation morale de se conformer aux normes établies.

Avec l'évolution de la société et la **sécularisation** progressive, la religion a cédé la place à d'autres formes de surveillance, notamment la **surveillance sociale et institutionnelle**. Les valeurs morales de la société ont remplacé les dogmes religieux en justifiant la mise en place de mécanismes de surveillance pour maintenir l'ordre public et assurer une police et une justice efficaces.

Depuis les *surveillance studies* s'attachent à mettre en évidence de nouvelles pratiques qui ne cessent de favoriser des injustices, des exclusions, des discriminations, et dénoncent dans le même temps des **réactions sociales** relativement limitées face à leur développement qui menacent et entravent pourtant les libertés individuelles.

Que dit le cadre légal...

La violation de l'intimité numérique consiste à prendre connaissance, à détourner, à enregistrer, à transmettre, toute donnée collectée par la technologie sans le consentement de leur auteur. Si elle est extrêmement rarement poursuivie de manière isolée, elle est souvent associée à d'autres infractions, notamment dans des contextes de violences conjugales.

Ces agissements sont condamnés par :

- L'article 226-1 du Code Pénal qui dispose qu'est "*puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui, en captant, enregistrant ou transmettant, sans le consentement de leur auteur*" telles que des **paroles**, des **images** prises dans un lieu privé ou encore la **localisation** en temps réel ou en différé d'une personne.

- Ces mêmes peines sont applicables d'après **l'article 226-15 du Code pénal** pour des faits "*commis de mauvaise foi" qui visent à "intercepter, détourner, utiliser ou divulguer des* ***correspondances*** *émises, transmises ou reçues par la* ***voie électronique***" ou de "*procéder à l'****installation d'appareils***" conçus à cette fin.

- Les l**ogiciels destinés à modifier les systèmes informatiques à l'insu de l'utilisateur** afin de capter des données personnelles peuvent également être réprimés par **l'article 323-1 du Code Pénal** de trois ans d'emprisonnement et 100 000 euros d'amende, pour le fait "*d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé*".

Pour aller un peu plus loin...

Quelques références scientifiques :

CHATTERJEE Rahul et al., *The spyware used in intimate partner violence*, 2018 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 2018, pp. 441-458.

CHAULK Kasey, JONES Tim, Online obsessive relational intrusion: Further concerns about Facebook, *Journal of Family Violence*, Volume 26, Issue 4, 2011, pp. 245-254.

DOUGLAS Heather, HARRIS Bridget A., DRAGIEWICZ Molly, Technology-facilitated domestic and family violence: Women's experiences, *British Journal of Criminology*, Volume 59, Issue 3, 2019, pp. 551-570.

HENRY Nicola, FLYNN Asher, POWELL Anastasia, Technology-Facilitated Domestic and Sexual Violence: A Review, *Violence against women*, Volume 26, Issue 15-16, 2020, pp. 1828-1854.

JOHNSON Michael P., *A Typology of Domestic Violence. Intimate Terrorism, Violent Resistance, and Situational Couple Violence*, Northeastern University Press, 2010, 168 pages.

LANGHINRICHSEN-ROHLING Jennifer, Controversies involving gender and intimate partner violence in the United States, *Sex Roles*, Volume 62, Issue 3, 2010, pp.179-193.

RAMIREZ karli, To Catch a Snooping Spouse: Reevaluating the Roots of the Spousal Wiretap Exception in the Digital Age, *University of Pennsylvania law review*, Volume 170, Issue 4, 2022, pp. 1093-1125.

REED Lauren A., TOLMAN Richard M., WARD Monique L., Snooping and Sexting: Digital Media as a Context for Dating Aggression and Abuse Among College Students, *Violence against women*, Volume 22, Issue 13, 2016, pp. 1556-1576.

TOLMAN Richard M., The validation of the Psychological Maltreatment of Women Inventory, *Violence and Victims*, Volume 14, Issue 1, 1999, pp. 25-37.