

PROJET CYBERNETIC

DOXING

Etiologie des pratiques de cyberharcèlement**Cyberstalking****Arnaque au
sentiments****Chantage à
la webcam****Fraude aux
données
personnelles****Cyber-usurpation****Piratage de données
personnelles****Doxing****ARGENT**

SYNONYMES

- Doxxing
- Bulle mortifère

Définition

Concept-clé :

Le *doxing* est une pratique qui vise à rechercher et collecter depuis des sources ouvertes, des données et des informations personnelles relatives à un individu puis à les publier en ligne à son insu dans le seul but de lui nuire (intimidation, humiliation, menace, etc.).

Le doxing se déroule en deux phases. Durant la première, dite de "collecte", les auteurs rassemblent toutes les **informations disponibles sur les victimes** (adresses privées, adresses email et comptes réseaux sociaux associés, numéros de téléphone, identification des membres de la famille, photos privées et parfois données plus personnelles (bancaires, santé, professionnelles, sexualité, etc.). Aucun recours à du hacking n'est requis. Toutes ces informations personnelles sont consultables sur les réseaux sociaux, sur des sites internet (mentions légales), sur des blog et forums, des sites spécialisés en recherche de source ouverte (base de données des abonnements téléphoniques), etc.

La seconde phase consiste à **publier** largement, généralement en une seule fois, **les informations** ainsi **collectées**. Le recours à de faux profils ou à des plateformes anonymes (comme par exemple pastebin) est couramment utilisé pour diffuser largement tout en restant protégé. Les publications sont souvent accompagnées de menaces pouvant avoir des répercussions dans la vie des victimes.

Ce qu'il faut retenir...

Le **doxeur** se nourrit des nombreuses **informations publiées librement sur internet** qui dévoilent peu à peu votre intimité et votre vie privée. Il convient de limiter les informations que l'on partage sur internet.

- Évitez dès que possible d'utiliser votre **nom et prénom** sur internet. Il en est de même pour votre adresse email. Ayez recours à des pseudos.

- Évitez le recours au **processus d'inscriptions automatiques des GAFAS** (Facebook, Google, ...). Vous éviterez ainsi de communiquer à ces sites, l'entièreté de vos données personnelles collectées par ces derniers (nom, prénom, adresse, habitude, amis, ...).

- Paramétrez la **confidentialité** de vos réseaux sociaux pour éviter que tout le monde puisse avoir accès à vos publications. Créez un faux compte lambda et surveillez depuis ce dernier la visibilité de votre profil.

- Googélisez-vous régulièrement afin de contrôler ce qui est dit de vous sur internet. Mettez en place des **alertes automatiques** qui vous préviennent dès que votre nom apparaît sur un site.

- Adoptez la **double authentification** dès que possible. Renforcez vos mots de passe (12 caractères alpha-numérique, caractères spéciaux, inintelligible, unique, secret, périodique).

- Utilisez dès que possible un **VPN** pour sécuriser vos connections et rendre inintelligibles vos échanges.

“

Samuel Paty c'est l'exemple d'une violente campagne de doxing orchestrée sur les réseaux sociaux où on a traqué son nom, son numéro de portable et l'adresse de son collègue, quelques jours avant son meurtre.

Aux origines...

Révéler les informations personnelles d'une personne sans son consentement est une pratique qui n'a pas attendu l'avènement d'internet pour trouver une certaine prospérité. Cependant le mot *doxing* est apparu pour la première fois dans les **années 90**, lorsque l'anonymat était encore une notion révéérée parmi les premiers **pirates informatiques**, (considérés hors-la-loi).

A l'époque, plusieurs confrontations ont opposé des **hackers rivaux**, qui étaient uniquement connus par leurs pseudonymes ou leurs alias. Peu d'options permettaient alors de riposter, voire de se venger, si ce n'est briser cet **anonymat** sous lequel ils se dissimulaient, en révélant des "documents" les identifiant, les exposant ainsi à des actions répressives.

En anglais, ces "documents" ont opéré un glissement sémantique en "docs", puis en "dox", contracté au verbe "to drop" pour appuyer la notion de "révélation".

Un exemple concret :

```
"linkedin.com/[redacted]5",
"linkedin_username":"charlie-[redacted]5","linkedin_id":"2[redacted]
"facebook_url":"facebook.com/v[redacted]",
"facebook_username":"v[redacted]",
"facebook_id":"1[redacted]5",
"work_email":"c[redacted].com",
"mobile_phone":"+15[redacted]8",
"industry":"biotechnology",
"location_name":"cambridge, massachusetts, united states",
"location_metro":"boston, massachusetts"
"location_geo":"42.37,-71.10","location_last_updated":"2020-12-0
"linkedin_connections":120,"inferred_salary":"[redacted]",
"inferred_years_experience":5,
"summary":"I am a moti[redacted]
"full_name":"mehari [redacted]"
"linkedin_url":"linkedin.com/[redacted]",
```

Que dit le cadre légal...

Le **10 février 2021**, l'assemblée nationale a voté la création d'un **délit de mise en danger de la vie d'autrui par la diffusion d'informations relatives à la vie privée**. Il s'agit de l'**article 36 dit "Samuel Paty"** (qui vient combler un vide juridique) dans le cadre de la loi du séparatisme :

"Le fait de révéler, de diffuser ou de transmettre, par quelque moyen que ce soit, des informations relatives à la vie privée, familiale ou professionnelle d'une personne permettant de l'identifier ou de la localiser aux fins de l'exposer, le ou les membres de sa famille, à un risque direct d'atteinte à la personne ou aux biens que l'auteur ne pouvait ignorer".

Ce délit est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

La peine de prison encourue est de 5 ans lorsque le délit est commis à l'encontre :

- d'une personne dépositaire de l'autorité publique ou chargée d'une mission de service public ;
- du titulaire d'un mandat électif ;
- d'une personne mineure.

A noter que la sanction punit "**l'intention de nuire**" et non pas "**l'intention d'informer**".

Avant ce vide juridique et suivant les cas saisis, le *doxing* pouvait relever du code pénal et être considéré comme une atteinte à la vie privée, une dénonciation calomnieuse, une violation du secret des correspondances, une atteinte au système de traitement automatisé de donnée, une collecte, traitement et divulgation de données personnelles sans le consentement ou autorisation.

Pour aller un peu plus loin...

Quelques références scientifiques :

CHANDLER Daniel, MUNDAY Rod, *Doxing, A dictionary of Social Media*, Oxford University Press, 2016, 320 pages.

CHEN Mengtong, CHEUNG Anne Shann Yue, CHAN Ko Ling, *Doxing : What Adolescents Look for and Their Intentions*, *International journal of environmental research and public health*, 2019, Volume 16, n° 2, pp. 218-230.

JOMNI Adel, *Le Darknet est-il une zone de non droit ?*, *Sécurité globale*, Volume 15, n° 3, 2018, pp. 17-23.

LI Lisa B., *Data Privacy in the Cyber Age : Recommendations for Regulating Doxing and Swatting*, *Federal communications law journal*, The George Washington University Law School, 2018, Volume 70, n° 3, pp. 317-328.

MARION Nancy E., TWEDE Jason, *Cybercrime: An Encyclopedia of Digital Crime*, ABC-CLIO, 2020, 520 pages.

NORRIS Ingrid, *Mitigating the Effects of Doxing*, Utica College, 2012, URL: https://concordia.ab.ca/wp-content/uploads/2017/04/Roney_Mathews.pdf?x60138.

TROTTIER Daniel, *Denunciation and doxing : towards a conceptual model of digital vigilantism*, *Global crime*, Routledge, 2020, Volume 21, n° 3-4, pp. 196-212.