© Businessman holding tablet and showing holographic - par Lunatictm

UNE MESURE STATISTIQUE DE LA CYBERCRIMINALITÉ FRAGMENTÉE

Le Service statistique ministériel de la sécurité intérieure (SSMSI) a été créé en 2014 pour que les décideurs puissent bénéficier d'une approche en conformité avec les normes de la statistique publique. Celles-ci s'appuient sur le code des bonnes pratiques de la statistique européenne et le règlement 223/2009 révisé du Parlement européen et du Conseil du 11 mars 2009 relatif à la statistique européenne. En effet, les statistiques liées à la cybercriminalité répertorient les infractions pénales tentées ou commises à l'encontre ou principalement au moyen d'un système d'information et de communication (SIC). Elles doivent pouvoir être distinguées parmi des codes de natures d'infractions existants (NATINF) ou enrichis pour accompagner l'évolution de cette délinquance spécifique. Pour mieux appréhender son périmètre, on pourrait s'appuyer sur des sources administratives mais également sur des structures qui fournissent des études sur la cybercriminalité : les sociétés offrant des services de sécurité informatique, éditeurs de logiciels antivirus, sociétés d'assurance ou les cabinets de conseil, tout en tenant compte du contexte de recueil et d'analyse de ces données externes. On peut estimer raisonnablement que la mise en œuvre de méthodes innovantes d'analyse permettront à moyen terme d'améliorer la connaissance statistique de la cybercriminalité.

Les défis de la mesure
statistique de la cybercriminalité

Par Tiaray Razafindranovona et André Moreau

La mesure de la cybercriminalité n'échappe pas aux difficultés classiques de celle de la délinquance. Pour demeurer pertinents, les outils de la statistique administrative doivent non seulement s'adapter à l'émergence de nouveaux phénomènes délinquants, comme c'est le cas avec la cybercriminalité, mais aussi se conformer aux récentes normes internationales qui permettent une production de statistiques comparables avec les pays étrangers, à l'appui notamment des actions de coopération internationale policière. Inexistante au début des années soixante-dix, la cybercriminalité constitue une adaptation de la délinquance aux récentes évolutions technologiques. La statistique de la cyberdélinquance est aujourd'hui essentiellement produite à partir des données administratives de la Police et de la Gendarmerie nationales et quelques enquêtes de victimation permettent de compléter la vision du phénomène. La mobilisation d'autres sources administratives, comme les informations saisies sur des plateformes de signalement en ligne, ainsi que la mise en œuvre de méthodes innovantes d'analyse permettront d'améliorer la connaissance statistique de la cybercriminalité.

TIARAY RAZAFINDRANOVONA

Administrateur de l'Insee. Responsable des méthodes statistiques Service statistique ministériel de la sécurité intérieure SSMSI / BPDS

ANDRÉ MOREAU

Lieutenant-colonel de gendarmerie. Adjoint au chef du Bureau de la méthodologie et des études statistiques Service statistique ministériel de la sécurité intérieure. Chargé d'études.

Mesurer la délinquance[1]

(1) Estival A., Filatriau O., La mesure statistique de la délinquance, AJ Pénal 2019.224.

Le Service central d'étude de la délinquance (SCED) de la Direction centrale de la police judiciaire (DCPJ) a mis en place en 1972 un outil de suivi statistique des seuls crimes et délits constatés par les forces de sécurité : l'état 4001, du nom du formulaire papier utilisé lors de sa création.
Les infractions y étaient classées en 107 catégories nommées index, très hétérogènes par la nature et la gravité des faits. Pour pouvoir appliquer une métrique unique, à savoir le « fait constaté », à l'ensemble des index, il est fait usage d'unités de compte spécifiques par index correspondant à la façon la plus pertinente de mesurer chaque type d'infraction (victimes, infractions, auteurs, procédure, objets). Depuis 2015 pour la Police nationale et 2016 pour la Gendarmerie nationale, les systèmes d'information centralisent toutes les infractions enregistrées par les forces de sécurité avec nettement plus de détails que ce qui figurait dans l'état 4001.

Toutefois, les remontées via les logiciels de rédaction des procédures ne sont pas suffisantes pour appréhender la délinquance dans son ensemble. En effet, il est admis que l'enregistrement d'un événement dépend de la propension de la victime à porter plainte, de la priorité des forces de sécurité à la découverte de tel ou tel type d'infraction et enfin de la disposition et de la capacité des services à consigner cet événement. Pour y remédier, des enquêtes de victimation ont été mises en place : en France, l'enquête « Cadre de vie et sécurité » (CVS) est réalisée annuellement, depuis 2007, par l'Insee auprès d'environ 23 000 ménages en partenariat avec l'Observatoire national de la délinquance et des réponses pénales (ONDRP) et le service statistique ministériel de la sécurité intérieure (SSMSI créé en 2014).
Cette enquête vise à connaître les actes de délinquance dont les ménages et leurs membres ont pu être victimes.

Une décennie de polémique sur les statistiques administratives…

L'hétérogénéité des modes de mesure rend donc inappropriée l'addition des chiffres mesurés dans les différentes catégories. Pourtant un chiffre unique de la délinquance a longtemps été utilisé par les services de police et de gendarmerie pour piloter l'action publique et les politiques l'ont également mis en avant à des fins de communication[2], en particulier à partir de 2002.

(2) Mucchielli L., Robert P., Crime et sécurité. L'état des savoirs, Paris, La Découverte, 2002.

Au même moment, la mise en œuvre du management par objectifs de la délinquance, connu sous la dénomination de « politique du chiffre », a également contribué à brouiller, voire décrédibiliser les statistiques de la délinquance enregistrées par les forces de sécurité. En septembre 2012, un groupe de travail interne au ministère de l'Intérieur a été mandaté pour « rompre avec une présentation des statistiques reposant sur des indicateurs trop globaux, imprécis et hétérogènes »

et « redonner aux statistiques leur véritable vocation : être un outil au service de l'efficacité de l'action des policiers et des gendarmes ». En 2014, il a été créé le Service statistique ministériel de la sécurité intérieure (SSMSI) qui produit les statistiques sur la délinquance en toute indépendance et en s'assurant de leur fiabilité.

LE SERVICE STATISTIQUE MINISTÉRIEL DE LA SÉCURITÉ INTÉRIEURE SSMSI

Afin de produire des statistiques en conformité avec les normes de la statistique publique qui s'appuient sur le code des bonnes pratiques de la statistique européenne et le règlement 223/2009 révisé du Parlement européen et du Conseil du 11 mars 2009 relatif à la statistique européenne, la France a créé en 2014 un service statistique ministériel au sein du ministère de l'Intérieur (SSMSI). Conformément au décret n° 2014-1161 du 8 octobre 2014, il est placé sous l'autorité fonctionnelle conjointe des directeurs généraux de la police nationale (DGPN) et de la gendarmerie nationale (DGGN). Il est officiellement reconnu comme membre du service statistique public national, au sens de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, par un arrêté du 9 décembre 2014, au côté de l'Insee et des 15 autres services statistiques ministériels. La cheffe actuelle du service est la seule responsable, technique et éditoriale des informations et des données publiées par le service[3], dans le respect des règles techniques et déontologiques de fiabilité et de neutralité de la statistique publique.

(3) Le principal vecteur de diffusion de ces informations est le site internet https://www.interieur.gouv.fr/Interstats

Mesurer la cybercriminalité est encore plus complexe

Les limites évoquées sur la délinquance globale enregistrée sont encore plus marquées

Mesurer la cybercriminalité à partir des seuls évènements enregistrés dans les données du ministère de l'Intérieur conduit à une sous-estimation du phénomène.

En effet, certaines victimes d'infractions « cyber » peuvent considérer que le préjudice subi ne justifie pas la démarche de déposer une plainte (banalisation des faits, anonymat des auteurs) ou, du moins, que cette démarche n'est pas indispensable : par exemple, le remboursement par la banque d'un débit frauduleux sur compte bancaire peut s'effectuer sans dépôt préalable de plainte. De plus, les victimes, en particulier les personnes morales (entreprises, administrations, …), peuvent choisir de ne pas déposer de plainte pour des questions d'image ou de réputation[4].

(4) Protéger les internautes – Rapport sur la cybercriminalité (Groupe de travail interministériel sur la cybercriminalité).

Plus en amont encore du dépôt de plainte, une spécificité de la cybercriminalité est la transparence de certaines infractions : les victimes ne sont pas forcément conscientes qu'elles subissent une atteinte. Par exemple, il est difficile pour une per-

sonne non avertie de repérer une utilisation clandestine, par un tiers, de son ordinateur transformé en « machine zombie » pour par exemple miner de la cryptomonnaie (*cryptojacking*) ou encore lancer des attaques par déni de service.

Une absence de définition juridique unique

La mesure de la cybercriminalité se heurte à l'absence de définition juridique unique : ses contours peuvent alors apparaître comme flous. La cybercriminalité ne renvoie pas ainsi à une liste de natures d'infractions (Natinf[5]) bien déterminées ni à un index spécifique puisqu'elle couvre une bonne partie de l'ensemble du champ infractionnel.

(5) Il s'agit d'une nomenclature du ministère de la Justice qui repose sur les différents textes de loi s'appliquant en France.

En 2014, un groupe de travail « Cybercriminalité », piloté par le SSMSI, a été mis en place avec des représentants du ministère de la Justice, du ministère de l'Intérieur, du ministère de l'Économie et des Finances et du ministère de l'Économie Numérique pour établir une définition de ce concept : la cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou principalement au moyen d'un système d'information et de communication (SIC), à savoir : les infractions spécifiques à l'encontre des SIC et de leurs données, les infractions relatives à la diffusion de contenus illicites via les SIC et les autres infractions tentées ou commises principalement au moyen des SIC.

Par ailleurs, une autre spécificité de la cybercriminalité, compliquant sa mesure ou sa connaissance statistique dans un cadre national standard, est son caractère largement transnational : les atteintes subies par la victime sur le territoire national peuvent provenir d'attaques opérées depuis l'étranger, des fonds peuvent être détournés vers l'étranger et les données techniques nécessaires à l'enquête peuvent être hébergées à l'étranger.

Une production fragmentée de données statistiques sur la cybercriminalité

Une multitude d'acteurs fournit des chiffres sur la cybercriminalité. La plupart d'entre eux ne sont pas labellisés au sens de la statistique publique mais peuvent néanmoins être abondamment commentés dans le débat public.

Ainsi, un grand nombre de sociétés privées fournissent des statistiques ou des études sur la cybercriminalité : les sociétés offrant des services de sécurité informatique (comme les éditeurs de logiciels antivirus), les sociétés d'assurance ou encore les cabinets de conseil. Ces données peuvent être d'un grand intérêt pour appréhender les nouvelles formes de cyberdélinquance. Cependant, ces acteurs privés ont des intérêts propres et la méthodologie utilisée n'est pas forcément transparente :

les chiffres doivent être pris avec un certain recul et l'interprétation en termes statistiques doit être prudente.

La fragmentation[6] de la production de données renvoie dans une certaine mesure à l'hétérogénéité conceptuelle de la cybercriminalité. Le rôle de la statistique publique et du SSMSI est de diffuser des résultats à la fois garants d'une qualité statistique certaine et dont l'homogénéité facilite l'interprétation.

(6) Côté A.-M., Bérubé M., Dupont B., *Statistiques et menaces numériques* – Comment les organisations de sécurité quantifient la cybercriminalité, Réseaux 2016/3.

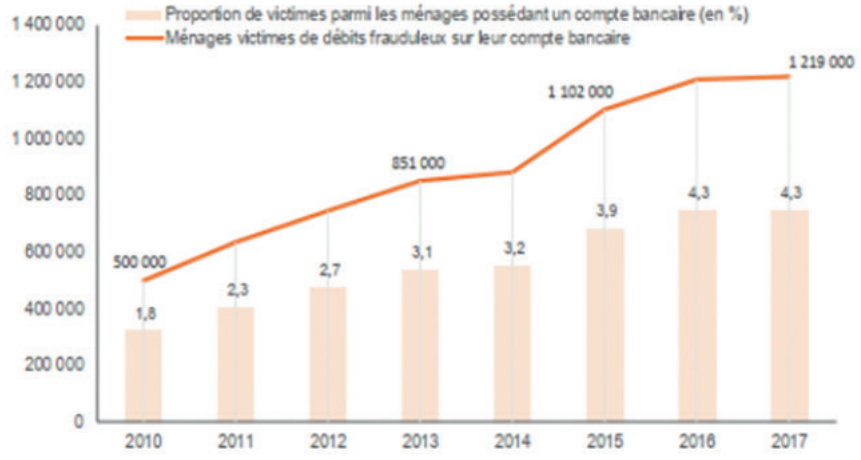
Sources et résultats de la statistique publique sur la mesure de la cybercriminalité

Appréhender la cybercriminalité par les enquêtes sur échantillons représentatifs

Les données d'enquêtes sur échantillons représentatifs de ménages ou d'entreprises peuvent être mobilisées pour appréhender et quantifier certains aspects de la cybercriminalité par le prisme des victimes.

Depuis 2011, le questionnaire de l'enquête « Cadre de Vie et Sécurité » comprend

Nombre annuel de ménages victimes de débit frauduleux sur leur compte bancaire et proportion de ménages victimes entre 2010 et 2017



Champ • Ménages ordinaires de France métropolitaine.
Source • Enquêtes Cadre de vie et sécurité 2011 - 2018, Insee-ONDRP-SSMSI.

un module spécifique sur les escroqueries bancaires qui sont en forte progression : la proportion de ménages qui déclarent avoir été victimes de débit frauduleux sur leur compte bancaire a plus que doublé entre 2010 et 2017[7], passant de 1,8 % à 4,3 %.

(7) Rapport d'enquête « cadre de vie et sécurité » 2018 (SSMSI).

Ces atteintes ont une large composante « cyber » : en moyenne entre 2015 et 2017, 56 % des ménages victimes indiquent que le débit frauduleux a été effectué sous la forme d'un achat en ligne réglé par carte bancaire. En 2018, le questionnaire s'est également enrichi d'un module spécifique sur les arnaques. Là aussi, la composante « cyber » de ces infractions est très marquée : en 2017, pour un ménage victime d'une arnaque sur deux, le contact se réalise via Internet, que ce soit par un site en ligne ou par un courriel.

L'enquête sur l'utilisation des technologies de l'information et de la communication (TIC) et le commerce électronique dans les entreprises, réalisée annuellement par l'Insee auprès d'environ 13 000 sociétés, comporte en 2010 et 2015 un module spécifique de questions sur la sécurité des TIC. La part de sociétés victimes d'incidents liés aux TIC est en progression. En particulier, 7 % des sociétés déclarent avoir subi en 2015 une destruction ou une altération de données due à l'attaque d'un programme malveillant ou à un accès non autorisé, alors qu'elles étaient 4 % en 2010[8].

(8) Demoly E., Vacher T., Sécurité numérique et médias sociaux dans les entreprises en 2015, Insee Première n°1594.

Une quantification de la cybercriminalité par les données administratives de la délinquance enregistrée

La quantification de la cybercriminalité couvrant un spectre d'infractions plus large s'effectue à partir des données administratives de la délinquance enregistrée.

Cette mesure repose sur les logiciels de rédaction des procédures de la police (LRPPN) et de la gendarmerie (LRPGN), en s'appuyant sur une

Modalités de la prise de contact pour les arnaques

Modalité de la prise de contact	%
Internet, contact en ligne, site, courriel	51
Par téléphone	23
À domicile	7
En magasin, sur un marché, salon ou foire	7
Par courrier papier	ND
Autres	10

ND : non diffusable, l'effectif de victimes ayant répondu étant inférieur à 30.
Champ : France métropolitaine, individus âgés de 14 ans et plus victimes d'arnaque en 2017. Arnaque la plus récente.
Source : Enquête Cadre de vie et sécurité 2018, Insee-ONDRP-SSMSI ; traitements SSMSI.

liste, définie par le groupe de travail mentionné supra, de Natinf, dites « spécifiques », relevant explicitement de la cybercriminalité. Elles sont au nombre de 97 et 59 d'entre elles décrivent des atteintes aux systèmes de traitement automatisé des données.

Les systèmes d'information permettent aussi le comptage d'infractions « cyber » au sein d'autres Natinf, dites « génériques », qui n'identifient pas explicitement des actes de cybercriminalité mais qui peuvent relever de la cybercriminalité dès lors qu'elles ont été commises sur internet ou dans le cadre d'un SIC. Le repérage de ces infractions s'effectue sur le mode opératoire, le contexte de la procédure et la nature de lieu de l'infraction pour la police (LRPPN) ou par une coche « cyber » déclenchée au moment de la rédaction du message d'information statistique pour la gendarmerie (LRPGN).

Après expertise de la qualité des données recueillies, le SSMSI estime qu'il ne peut diffuser pour l'instant, auprès du grand public, que les évolutions des atteintes aux systèmes de traitement automatisé des données[9]. En effet, il considère que les autres NATINF spécifiques ne sont pas toujours suffisamment utilisées lors de l'enregistrement et que les variables annexes servant au repérage des infractions « cyber » ne sont pas toujours bien renseignées.

(9) État de la menace liée au numérique en 2019 (Ministère de l'Intérieur).

Une mesure de la cybercriminalité enregistrée permettant de mieux apprécier son ampleur et son évolution temporelle est néanmoins envisageable dans un futur proche. À cette fin, des travaux sont en cours au SSMSI en collaboration avec le SSP Lab de l'Insee, pour mieux identifier, à partir de la description sur la manière d'opérer, les infractions qui relèvent de la cybercriminalité en combinant l'utilisation de techniques innovantes d'analyse textuelle et de machine learning. De plus, l'analyse des données issues des plateformes de signalement en ligne (Percev@l pour les fraudes à la carte bancaire, Pharos pour les contenus illicites sur Internet) viendra compléter le panorama sur la cybercriminalité au-delà de la seule délinquance enregistrée.

L'AUTEUR

Diplômé de l'Ensae et du master APE de l'École d'Économie de Paris, Tiaray Razafindranovona est responsable des méthodes statistiques au Service statistique ministériel de la sécurité intérieure.

Sa dernière contribution aux publications Interstats du SSMSI porte sur l'analyse conjoncturelle de la délinquance enregistrée : Interstats Conjoncture n° 49 – octobre 2019. [https://www.interieur.gouv.fr/Interstats/Actualites].

L'AUTEUR

Docteur en sciences de gestion, André Moreau étudie les statistiques de la délinquance. Officier de liaison pour la Gendarmerie nationale auprès du Service statistique ministériel de la sécurité intérieure, ses travaux portent sur les phénomènes émergeants comme la cybercriminalité.

Sa dernière contribution aux publications Interstats du SSMSI traite des arnaques : Plus de la moitié des arnaques passent par internet - Interstats analyse n° 21 – juillet 2019. [https://www.interieur.gouv.fr/Interstats/Actualites].