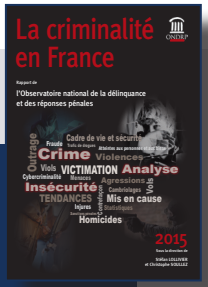

Marine VALZER
Chargée d'études criminologiques

La cybercriminalité et les infractions liées à l'utilisation frauduleuse d'internet

Éléments de mesure et d'analyse pour l'année 2014

INTRODUCTION

La cybercriminalité regroupe des infractions très diverses qui peuvent être classées en deux catégories : les infractions liées aux formes de criminalité traditionnelles qui ont pu évoluer avec les nouvelles technologies de l'information et de la communication (NTIC), et les infractions liées aux systèmes d'information et de traitement automatisé des données (STAD), qui sont apparues avec le développement des réseaux informatiques et d'internet.

La comptabilisation des infractions de la première catégorie par le biais des statistiques administratives se limite aux infractions portées à la connaissance des administrations et ne peut donc recenser exhaustivement les infractions liées à la cybercriminalité. Le dénombrement des infractions liées aux systèmes d'information ou aux STAD est en plus limité par le fait qu'il n'est pas toujours aisé pour un individu ou une entreprise de prendre conscience qu'il a été victime et donc de déposer plainte, ou de se déclarer victime lors des enquêtes de victimation.

PRINCIPAUX ENSEIGNEMENTS

En 2014, 2796 atteintes aux systèmes de traitement automatisé des données ont été recensées par la police et la gendarmerie, s'agissant essentiellement de l'accès ou du maintien frauduleux dans un STAD. 19,6% de ces atteintes consistent en des accès avec altération du fonctionnement ou modification/suppression de données. Entre 2013 et 2014, le nombre d'atteintes aux STAD constatées par la police et la gendarmerie augmente légèrement (+2,2%, *soit* +61 *faits*).

Un peu moins de 1300 infractions aux droits des personnes résultant de traitements informatiques ont également été enregistrées en 2014, soit une légère baisse de ce type d'infractions par rapport à l'année 2013 (- 2,7%, *soit* - 36 *faits*). Sur la même période, les infractions à la loi sur la presse portant atteinte aux individus et commises par l'utilisation des NTIC ont augmenté de 20,7%, dénombrant 1780 atteintes supplémentaires en 2014 pour un total de 10339 faits. S'agissant des mineurs, cible particulièrement vulnérable sur internet, le nombre d'atteintes augmente : 2940 faits sont recensés en 2014, traduisant une hausse de 26,3% par rapport à 2013 (+612 *faits*).

1 Préambule méthodologique

LA CYBERCRIMINALITÉ : DES INFRACTIONS TRÈS DIVERSES…

Dans le sens commun, la **cybercriminalité** regroupe l'ensemble des infractions susceptibles d'être commises ou facilitées par l'utilisation d'un système informatique, généralement connecté à un réseau. Ainsi définie, elle peut faire référence à des infractions très diverses. Leur étude sur le plan statistique nécessite de distinguer :

1 - **Les infractions liées aux systèmes d'information et aux systèmes de traitement automatisé des données** (accès frauduleux, altération d'un système, attaque par déni de service…), engendrées par le développement des réseaux informatiques, notamment internet ;

2 - **Les infractions liées aux formes de criminalité « traditionnelles »**, qui ont pu évoluer avec les nouvelles technologies de l'information et de la communication (NTIC) ou être facilitées par ces dernières, et donc constituer un nouveau vecteur de criminalité. Cette deuxième catégorie contient, par exemple, de nouvelles formes d'escroquerie apparues avec l'utilisation d'internet (usages frauduleux de cartes de crédit en ligne, phishing [1], etc.), des menaces et injures de toutes natures qui peuvent dorénavant être diffusées *via* les nouveaux moyens de communication électronique (messagerie, forums, réseaux sociaux…), la diffusion d'images pédo-pornographiques facilitée par les nouveaux réseaux de communication et internet, etc.

… QUI NE PEUVENT ÊTRE ÉTUDIÉES PAR LES APPROCHES HABITUELLES DE L'ONDRP

Au même titre que les phénomènes criminels traditionnellement étudiés par l'ONDRP, les formes de criminalité en lien avec l'utilisation des NTIC peuvent être abordées selon deux approches différentes : les crimes et délits portés à la connaissance des administrations et les enquêtes réalisées auprès de la population ou des entreprises.

Lorsqu'un crime ou un délit est porté à la connaissance de la police ou de la gendarmerie, l'infraction fait l'objet d'un enregistrement statistique par le biais d'un outil nommé « état 4001 », géré par le Service statistique ministériel de la sécurité intérieure (SSMSI) [2]. Celui-ci ne recense pas les crimes et délits routiers, les contraventions ou les crimes et délits constatés par d'autres administrations. Ainsi, en matière de lutte contre la cybercriminalité, la Direction générale des douanes et droits indirects (DGDDI) se préoccupe également d'infractions économiques commises sur internet (par exemple, la revente en ligne de biens contrefaits) par le biais du programme « Cyberdouane ». Si celles-ci ne font pas l'objet d'une procédure connexe par un service de police ou une unité de gendarmerie elles ne seront pas comptabilisées dans l'état 4001.

(1) Le « phishing » (ou « hameçonnage ») est une technique utilisée par les fraudeurs visant à soutirer des informations personnelles à leurs victimes en se faisant passer pour un tiers de confiance (banque, administration…).
Un exemple : http://www.caf.fr/actualites/2013/attention-aux-courriels-et-sites-internet-frauduleux

(2) *Cf. Résultats et Méthodes n°1* – Comment appréhender l'outil statistique des faits constatés par les services de police et les unités de gendarmerie.

Les faits constatés sont enregistrés selon une nomenclature composée de 103 index numérotés de 1 à 107. Cependant, à ce jour, **aucun des index de l'état 4001 ne permet une mesure directe des phénomènes liés à la cybercriminalité**. Certains index contiennent des infractions qui ont pu, en partie, être commises ou facilitées par l'utilisation des NTIC. De plus, les atteintes aux systèmes de traitement automatisé des données (STAD) ne sont pas rassemblées au sein d'un index particulier de l'état 4001, mais sont intégrées à l'index 107 « autres délits ».

Pour des infractions commises ou facilitées par les NTIC, l'utilisation de ces dernières ne constitue souvent pas l'infraction principale du fait constaté. Par exemple, dans le cas d'une atteinte sexuelle commise sur un mineur de moins de 15 ans par un majeur mis en contact avec la victime par le biais d'internet, l'infraction principale retenue sera l'atteinte sexuelle et non l'utilisation d'Internet ou le non-respect des conditions d'utilisation d'un service de discussion en ligne. Le fait sera alors classé à l'index 50 des « atteintes sexuelles ».

De plus, la dernière révision de la nomenclature de l'état 4001 a eu lieu en 1995, à une époque où l'équipement en micro-ordinateurs et l'accès à internet n'étaient pas généralisés[3]*. Par conséquent, la cybercriminalité ne constituait pas le phénomène d'ampleur qu'elle représente aujourd'hui et la lutte contre ce type d'infractions était moindre. Ce constat explique probablement l'absence d'un index particulier recensant les atteintes aux STAD ou les traitements illégaux de données nominatives informatisées.*

Néanmoins, les statistiques extraites de sources administratives comme l'état 4001 ne représentent qu'une partie du phénomène, celle qui est portée à la connaissance des administrations compétentes. Les sources administratives ne permettent pas de dénombrer précisément le nombre d'actes illicites commis sur internet ou par le biais des NTIC, mais peuvent fournir des informations qualitatives, intéressantes à des fins opérationnelles, sur les infractions et les méthodes utilisées par les « cybercriminels ».

Grâce aux nouveaux systèmes d'information déployés, en 2012, au sein de la gendarmerie nationale et, en 2014, au sein de la police nationale, et qui utilisent notamment les codes NATINF (NATures d'INFractions) du ministère de la Justice, il devrait être possible, en 2016, de disposer d'informations plus précises sur ce type de faits. Le service statistique ministériel de la sécurité intérieure a établi un projet de nomenclature composée de trois agrégats (atteintes aux systèmes d'information et de communication, infractions de diffusion de contenus illicites *via* les SIC et infractions économiques et financières ainsi que d'autres infractions commises *via* les SIC). L'ONDRP espère pouvoir exploiter ces données lors de son prochain rapport annuel.

UTILISATION DES ENQUÊTES DE VICTIMATION POUR MESURER LA CYBERCRIMINALITÉ

L'autre source statistique principale des études de l'ONDRP est l'enquête « Cadre de vie et sécurité », ou « enquête de victimation », qui est menée conjointement depuis 2007 avec l'Institut national des statistiques et des études économiques (INSEE). Chaque année, un échantillon d'environ 17000 ménages et individus représentatifs de la population française est interrogé sur les atteintes dont ils auraient pu être victimes, indépendamment de l'existence ou non d'un dépôt de plainte auprès de la police ou de la gendarmerie nationale. Les personnes qui se déclarent victimes d'une atteinte sont soumises à un ensemble de questions permettant de fournir différentes caractéristiques de la dernière atteinte subie (déroulement, préjudice subi, suites données...).

(3) En 1996, 15% des ménages français disposaient d'un micro-ordinateur à leur domicile et en 1999, 6,5% avaient accès à internet. Voir l'INSEE Première 1011 : http://www.insee.fr/fr/ffc/docs_ffc/ip1011.pdf

Outre le fait que la précision des statistiques établies dépend de la taille de l'échantillon de personnes interrogées [4], les enquêtes de victimation comportent également un biais propre à la mesure des infractions liées à la cybercriminalité. **Pour ce type d'infractions, il n'est pas toujours aisé pour un individu de prendre conscience qu'il a été victime**. Certaines formes de cybercriminalité, comme celles liées à l'altération du fonctionnement d'un système d'information (par exemple, l'introduction d'un *malware* [5] sur un ordinateur personnel), ou au vol de données ou documents dématérialisés, peuvent s'avérer totalement transparentes et n'avoir aucune conséquence « visible » pour l'utilisateur.

Par exemple, les formes d'escroqueries liées à l'ingénierie sociale, qui visent à soutirer des biens ou des informations d'une victime *via* une manipulation mentale, notamment le « *phishing* » ou les « arnaques nigérianes » [6], sont efficaces, car l'individu croit être en contact avec un interlocuteur de confiance et n'a pas conscience d'être victime.

De la même façon, un individu aura pu voir son micro-ordinateur intégré à un réseau de machines zombies, appelé « *botnet* », et utilisé à son insu pour la commission d'une infraction, telle que l'attaque par déni de service, l'utilisation de l'appareil « zombie » comme relais d'envoi de courriels indésirables [7] (« *spams* »), ou encore l'infection d'autres machines. **Il en résulte que toutes ces infractions commises dans le cyberespace sont très complexes à mesurer sur le plan statistique**, car ces « utilisations détournées » sont parfois difficiles à détecter en l'absence de connaissances avancées en sécurité informatique.

En d'autres termes, il ne peut être envisagé d'interroger une personne au sein de l'enquête « Cadre de vie et sécurité » sur le fait qu'elle ait été victime ou non de « *phishing* » ou que son ordinateur ait pu être utilisé à son insu pour la commission d'infractions, car bien souvent une victime n'aura pas eu conscience de l'infraction commise. Au contraire d'un vol « traditionnel » qui aura comme conséquence pour la victime la dépossession d'un objet physiquement matérialisé (téléphone, voiture, portefeuille…), les données ou documents numériques peuvent être aisément dupliqués, sans le moindre coût et être subtilisés de façon quasi transparente. En revanche, une escroquerie bancaire, même commise ou facilitée par internet, aura toujours pour conséquence un débit frauduleux d'argent que la victime pourra constater sur un compte bancaire.

Ainsi, pour la première fois en 2010, un ensemble de questions traitant des escroqueries bancaires a été intégré au sein de l'enquête de victimation. Il permet d'estimer l'ampleur du phénomène et de décrire les différentes caractéristiques de ces atteintes, notamment le rôle des NTIC et d'internet dans leur commission, ou l'utilisation des données bancaires frauduleusement obtenues. Ces questions ont fait l'objet d'une étude de l'Observatoire, publiée en juillet 2015 [8].

Cette étude révèle que, lors des enquêtes « Cadre de vie et sécurité » menées entre 2011 et 2014, 6 ménages victimes d'escroqueries bancaires sur 10 ont déclaré que l'auteur a utilisé leurs coordonnées bancaires dans le but d'effectuer un achat réglé avec une carte bancaire. Un peu plus de 12 % des débits constatés serait la conséquence d'un retrait opéré à partir d'un distributeur automatique de billets (DAB) tandis que 7 % des escroqueries auraient pris la forme d'un virement bancaire. Enfin 17,2 % affirment que l'auteur a eu recours à un autre type d'opération bancaire pour accomplir son méfait comme, par exemple, un rechargement de crédit téléphonique.

(4) Voir la présentation méthodologique de l'enquête de victimation au sein de ce rapport annuel.

(5) Un logiciel malveillant (ou « malware ») désigne un programme développé dans le but de nuire à un système informatique et de le détourner de son fonctionnement habituel, sans le consentement de l'utilisateur.

(6) Les arnaques nigérianes (ou « scam ») désignent une forme d'escroquerie en ligne basée sur l'envoi d'un courriel à la victime l'incitant à effectuer un transfert d'argent à une personne censée posséder une quantité importante d'argent, ou suite à une victoire (non réelle) à un jeu de hasard.

(7) Par exemple : http://www.01net.com/editorial/530844/la-chute-du-botnet-rustock-a-diminue-d-un-tiers-le-volume-de-spams/

(8) http://www.inhesj.fr/fr/ondrp/les-publications/reperes/30

© juillet 2015 - INHESJ/ONDRP – Rapport annuel 2015

Parmi les ménages victimes d'achats frauduleux réglés avec une carte bancaire (volée, piratée, contrefaite) ou grâce à des services de paiement en ligne, près de 79% précisent que l'achat effectué par l'auteur a été réalisé via le commerce en ligne sur internet. Les 21% restant ayant été commis et enregistrés dans un commerce dit traditionnel.

« COMMERCIAL VICTIMISATION SURVEY » COMME EXEMPLE

Les atteintes aux systèmes de traitement automatisé des données pourraient, en revanche, être étudiées par le biais de questions spécifiques sur la victimation intégrées à une enquête soumise aux entreprises, qui disposent généralement des moyens nécessaires pour prévenir et détecter ces atteintes.

Une enquête de victimation auprès des entreprises marchandes a ainsi été réalisée en **Angleterre** et au **Pays de Galles** au cours de l'année 2012. La « ***Commercial Victimisation Survey*** » et ses principaux résultats ont fait l'objet d'une publication au début de l'année 2013, puis une suivante en 2014[9]. Un ensemble de questions posées permettait de savoir si les entreprises interrogées avaient été victimes de *hacking* (accès non autorisé à leur système d'information), de *phishing*, de vol en ligne d'argent ou d'information, d'altération de leur site internet, ou si l'une de leurs machines avait été infectée par un virus ou un programme conçu pour nuire à l'entreprise.

Elle évaluait à 356000 le nombre d'infractions de ce type entre 2012 et 2013, en Angleterre ou au Pays de Galles, essentiellement des virus (*302000 infractions*). 86% des victimes déclaraient que leur système avait été infiltré ou infecté à distance (en général par email ou *hacking*). Seuls **11% de ces infractions ont fait l'objet d'une plainte auprès de la police**. Environ 41% des entreprises victimes n'ont pas déposé plainte car elles considéraient que l'incident n'était pas assez grave. 27% ne l'ont pas fait, car elles préféraient régler ce problème en interne, par leurs propres moyens.

AUTRE MOYEN DE LUTTE CONTRE LA CYBERCRIMINALITÉ

Le dossier thématique du rapport annuel 2011 de l'ONDRP présente également la plateforme PHAROS[10] (plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements) mise en place par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), qui permet aux internautes de « signaler les contenus ou comportements présumés illicites au regard du droit pénal, quel que soit le type d'infraction ». Au même titre que l'état 4001, cette plateforme ne vise pas à dénombrer de manière exhaustive les infractions commises sur internet. Elle est limitée, d'une part, à ce que les internautes auront identifié comme infraction pénale au cours de leur navigation sur internet, et d'autre part, au fait que ces derniers aient pris l'initiative de porter ces infractions à la connaissance des autorités par le biais de la plateforme, ce qui peut être lié aux opérations de communications menées pour promouvoir le dispositif.

En 2015 ou 2016 une nouvelle analyse des données PHAROS est envisagée par l'ONDRP.

(9) https://www.gov.uk/government/publications/crime-against-businesses-headline-findings-from-the-2013-commercial-victimisation-survey/crime-against-businesses-headline-findings-from-the-2013-commercial-victimisation-survey

(10) http://www.inhesj.fr/sites/default/files/rapport_2011_0.pdf

2 Les atteintes aux systèmes de traitement automatisé des données enregistrées par la police et la gendarmerie entre 2013 et 2014

AVERTISSEMENT

Les données présentées au sein de ce paragraphe ne sont pas extraites de l'état 4001, mais des systèmes d'information opérationnels des services de police et des unités de gendarmerie. **Pour cette année, le déploiement en cours du nouveau système d'information de la police nationale a nécessité, pour des raisons de continuité statistique, de restreindre la période d'étude aux années 2013 et 2014**. Pour la gendarmerie, les données sont extraites de la base Pulsar-MIS (*Messages d'information statistique*).

Ces sources de données permettent d'identifier certaines catégories d'infractions liées à la cybercriminalité, notamment les atteintes aux systèmes de traitement automatisé des données (STAD) et, pour certaines autres catégories d'infraction, celles qui ont été commises sur ou par le biais d'internet.

Outre les limites des statistiques administratives, présentées précédemment, les sources exploitées ici sont principalement utilisées à des fins opérationnelles. Elles ne visent pas à être exhaustives ou à fournir des tendances sur le nombre ou la nature des infractions qui sont commises ou facilitées par l'utilisation d'internet, mais à **décrire l'activité d'enregistrement des services de police et unités de gendarmerie dans le domaine de la cybercriminalité**.

LÉGÈRE HAUSSE ENTRE 2013 ET 2014 DES ATTEINTES AUX SYSTÈMES DE TRAITEMENT AUTOMATISÉ DES DONNÉES (STAD)

La loi pour la confiance dans l'économie numérique [11] réprime l'accès ou le maintien frauduleux dans un système automatisé de données (STAD) et aggrave la sanction lorsque l'accès ou le maintien a provoqué l'altération du système ou des données.

En 2014, 2 796 atteintes aux systèmes de traitement automatisé des données (STAD) ont été enregistrées par les services de police et unités de la gendarmerie nationale (*tableau 1*). Ces atteintes se caractérisent essentiellement par des accès ou maintiens frauduleux dans un STAD, avec 2 793 faits constatés en 2014.

(11) http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=54C38267FF98279B44344E20FD29E6DE.tpdila19v_2?cidTexte=JORFTEXT000000801164&dateTexte=20150526

548 accès ou maintiens frauduleux dans un STAD, soit environ 19,6% de l'ensemble des faits constatés d'atteintes aux STAD, ont engendré l'altération du fonctionnement du système ou l'introduction, la modification ou la suppression de données. Le nombre d'infractions liées à la fourniture de moyen matériel ou informatique permettant l'accès frauduleux ou l'entrave à un système informatique demeure peu élevé (*3 faits constatés en 2014, 4 en 2013*).

L'année précédente, 2735 atteintes aux STAD étaient enregistrées par la police et la gendarmerie. Entre 2013 et 2014, ce sont donc 61 faits de plus qui ont été enregistrés, soit une hausse d'environ 2,2%. Le nombre de faits constatés d'atteintes aux STAD avec altération du fonctionnement ou introduction/suppression/modification de données connaît une hausse d'ampleur plus importante (*+25,8%, soit 191 faits supplémentaires*).

Tableau 1

Nombres et variations annuelles des atteintes aux systèmes de traitement automatisé des données enregistrées par la police et la gendarmerie entre 2013 et 2014.

Nature d'infractions	2013	2014
Atteintes aux systèmes de traitement automatisé des données	**2 735**	**2 796**
Variations en volume	-	*+ 61*
Variations en %	-	*+ 2,2*
Accès ou maintien frauduleux dans un STAD	**2 731**	**2 793**
Variations en volume	-	*+ 62*
Variations en %	-	*+ 2,3*
dont Accès ou maintien frauduleux dans un STAD avec altération ou suppression/modification de données	739	548
Variations en volume	-	*- 191*
Variations en %	-	*- 25,8*
Fourniture de moyen matériel ou informatique d'entrave ou d'accès frauduleux à un système informatique	**4**	**3**
Variations en volume	-	*- 1*
Variations en %	-	*ns.*

Source : STIC-BN, DCPJ –Puls@r-MIS, DGGN - Traitement ONDRP

3 Éléments supplémentaires concernant certaines catégories d'infractions commises ou facilitées par internet

INFRACTIONS SPÉCIFIQUES AUX NTIC

En 2014, 1 290 infractions aux droits des personnes résultant des traitements informatiques ont été constatées par la police et la gendarmerie (*tableau 2*). Cette catégorie d'infractions comporte les atteintes aux personnes spécifiquement liées aux technologies de l'information et de la communication telles que la collecte, le traitement non autorisé ou la divulgation des données personnelles. Ces infractions sont sanctionnées par la loi Informatique et liberté [12]. S'ajoutent à ces atteintes, les violations de correspondances électroniques [13] qui représentent 60,3 % du total des infractions aux droits des personnes résultant des traitements informatiques en 2014, soit 778 faits.

Le nombre des infractions aux droits des personnes résultant des NTIC diminue entre 2013 et 2014 : - 2,7 %, soit 36 faits constatés en moins. Cette baisse résulte aussi bien des violations de correspondances électroniques (*- 2,5 %, soit - 20 faits constatés*) que des infractions à la loi Informatique et libertés (*- 3 %, soit - 16 faits constatés entre 2013 et 2014*).

Tableau 2

Nombres et variations annuelles des infractions aux droits des personnes résultant des traitements informatiques enregistrées par la police et la gendarmerie entre 2013 et 2014.

Nature d'infractions	2013	2014
Infractions aux droits des personnes résultant des traitements informatiques	**1 326**	**1 290**
Variations en volume	-	*- 36*
Variations en %	-	*- 2,7*
Infractions à la loi informatique et libertés	**528**	**512**
Variations en volume	-	*- 16*
Variations en %	-	*- 3,0*
Violations de correspondances électroniques	**798**	**778**
Variations en volume	-	*- 20*
Variations en %	-	*- 2,5*

Source : STIC-BN, DCPJ –Puls@r-MIS, DGGN - Traitement ONDRP

(12) http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460
(13) http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000173519&dateTexte=&categorieLien=id

INFRACTIONS DE DIFFUSION DE CONTENU ILLICITE

La loi du 29 juillet 1881 sur la liberté de la presse[14] prévoit la répression des infractions dites «de presse» pouvant être commises par les professionnels de la presse, mais aussi par tout particulier, dès lors qu'il a agi publiquement. Les infractions de presse concernent tous faits d'injure, de diffamation, de provocation à la haine ou provocation à la discrimination en public, et notamment par un moyen de communication électronique (messagerie, réseaux sociaux, etc.).

10 399 infractions de presse, commises par le biais d'internet ou des NTIC, ont été constatées par la police et la gendarmerie nationales en 2014 (*tableau 3*). Entre 2013 et 2014, 1 780 faits supplémentaires ont été enregistrés, ce qui représente une hausse en proportion de +20,7%.

10,7% de ces atteintes constituent des injures, diffamations ou provocations à la haine ou la discrimination ayant un caractère racial ou religieux, soit 1 110 faits constatés en 2014. Leur nombre a augmenté de 12,3% par rapport à 2013 (*+122 faits constatés*).

Tableau 3

Nombres et variations annuelles des infractions à la loi sur la presse commises par le biais d'internet et enregistrées par la police et la gendarmerie entre 2013 et 2014.

Nature d'infractions	2013	2014
Infractions de presse	**8 619**	**10 399**
Variations en volume	-	*+ 1 780*
Variations en %	-	*+ 20,7*
dont Injure, diffamation, provocation à la discrimination à caractère racial ou religieux	988	1110
Variations en volume	-	*+ 122*
Variations en %	-	*+ 12,3*
dont Injure, diffamation, provocation à la discrimination en raison du sexe ou de l'orientation sexuelle	194	230
Variations en volume	-	*+ 36*
Variations en %	-	*+ 18,6*

Source : STIC-BN, DCPJ –Puls@r-MIS, DGGN - Traitement ONDRP

INFRACTIONS À L'ENCONTRE DES MINEURS

Les atteintes portées aux personnes mineures sont de natures diverses et regroupent principalement des infractions liées à la pédopornographie en ligne, de corruption, de proxénétisme, de racolage ou exhibition sexuelle. Au nombre des infractions liées à la pédopornographie sur internet, on retrouve principalement l'enregistrement, la diffusion et la détention d'images à caractère

(14) http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000877119

pornographique d'un mineur, qui représentent une part importante de toutes les atteintes portées aux mineurs *via* internet. En 2014, 2 165 faits relatifs à l'enregistrement, la diffusion ou la détention de ces images ont été enregistrés, soit 73,6% du total des atteintes aux mineurs.

En 2014, 2 940 faits d'atteintes à l'encontre des mineurs par le biais d'internet ont été constatés par les services de police et les unités de la gendarmerie nationale (*tableau 4*). En 2013, 2 328 faits d'atteintes commis par le biais d'internet avaient été constatés. Ils ont augmenté de 26,3% entre 2013 et 2014, soit +612 faits constatés.

Tableau 4

Nombres et variations annuelles des infractions à l'encontre des mineurs commises par le biais d'internet enregistrées par la police et la gendarmerie entre 2013 et 2014.

Nature d'infractions	2013	2014
Infractions liées à la pédopornographie et mises en péril des mineurs	**2 328**	**2 940**
Variations en volume	-	*+ 612*
Variations en %	-	*+ 26,3*
dont Diffusion ou détention de l'image à caractère pornographique d'un mineur	1798	2 165
Variations en volume	-	*+ 367*
Variations en %	-	*+ 20,4*

Source : STIC-BN, DCPJ –Puls@r-MIS, DGGN - Traitement ONDRP

* * *