# Sécurité en ligne

- Le nombre de dossiers de fraude dans lesquels les enquêteurs de l'*Internet Referral Unit* (i2-IRU) sont intervenus a fortement augmenté.
- L'année 2020 a également été particulière pour la Federal Computer Crime Unit (FCCU). La pandémie de Covid-19 a eu un grand impact, notamment sur le fonctionnement international, les dossiers d'appui et les formations.
- Sous l'égide de l'Académie européenne de police CEPOL, les experts de la FCCU ont développé un nouveau module de formation de pointe concernant le *dark web* destiné aux services de police européens.

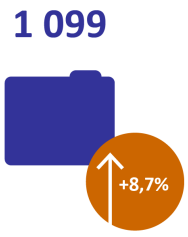
## Recherche sur Internet

La section i2-IRU (Internet Referral Unit) de la Direction de la lutte contre la criminalité grave et organisée (DGJ/DJSOC) assure différentes missions :

- la recherche sur Internet ;
- le blocage de sites et/ou de contenus (en collaboration avec les fournisseurs d'accès et les plates-formes Internet) ;
- la communication en matière de prévention ;
- la formation, l'information et le partage d'expertise ;
- la participation aux actions d'Europol.

Pour les dossiers Terro (propagande terroriste et activités extrémistes violentes apparentées sur Internet), l'i2-IRU travaille avec l'Internet Referral Unit créée par Europol (IRU EU). Europol dispose d'un outil automatisé pour rendre inaccessible la propagande une fois détectée. Les dossiers liés à la Belgique sont ensuite traités par l'i2-IRU.

En 2020, l'i2-IRU a fourni un appui aux unités dans 1 099 dossiers. Cela représente une augmentation de 88 dossiers par rapport à 2019 (1 011). La forte augmentation observée pour certains phénomènes est due au Covid-19 : la vente illégale de produits (fraude), l'appel à la désobéissance (ordre public) et les *fake news* concernant les vaccins et les prétendus remèdes au Covid-19.




*dossiers*

| Phénomènes | 2019 | 2020 |
|---|---|---|
| Terrorisme | 314 | 244 |
| Information | 132 | 151 |
| Fraudes | 118 | 194 |
| Vols | 91 | 32 |
| Tentatives de suicide | 66 | 69 |

| Phénomènes | 2019 | 2020 |
|---|---|---|
| Abus sexuels sur mineurs | 54 | 53 |
| Traite des êtres humains | 47 | 35 |
| Stupéfiants | 40 | 57 |
| Ordre public | 40 | 97 |
| Haine en ligne | 37 | 47 |
| Cybercriminalité | 31 | 37 |
| Armes | 26 | 20 |
| Disparitions | / | 23 |
| Hormones | 13 | 15 |
| Meurtres | 2 | 16 |
| Patrimoine | / | 6 |
| Fake news | / | 2 |
| Revenge porn | / | 1 |
| **Total** | **1 011** | **1 099** |

## Federal Computer Crime Unit

La Federal Computer Crime Unit (FCCU) a pour mission de lutter contre les formes complexes et organisées de cybercriminalité, en particulier lorsque celles-ci ont un impact sur les infrastructures critiques ou les fournisseurs de services essentiels. Parallèlement, la FCCU a développé une expertise dans certaines matières de haute technologie et elle fournit un appui spécialisé aux services d'enquête centraux et aux services d'inspection (AIG/Comité P) pour analyser des supports de données digitaux. Enfin, la FCCU collabore avec la Direction de la communication (CGC) pour informer et sensibiliser la population au sujet de la cybersécurité, des tendances digitales actuelles et de la sécurité en ligne, notamment via les canaux de la Police Fédérale sur les médias sociaux.

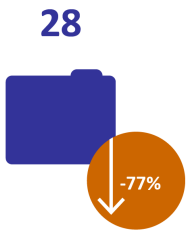
2020 a été une année particulière ; la pandémie de Covid-19 a eu un grand impact, notamment sur le fonctionnement international, les dossiers d'appui et les formations.

Cela n'a pas empêché la **capacité effective** de la FCCU d'augmenter de 22 % en 2020 (passant de 23 à 28 collaborateurs). Il s'agit d'un fait assez remarquable, dans la mesure où les spécialistes ICT sont très prisés sur le marché du travail. Les efforts se concentrent essentiellement sur l'amélioration des processus internes et du service rendu à nos partenaires.

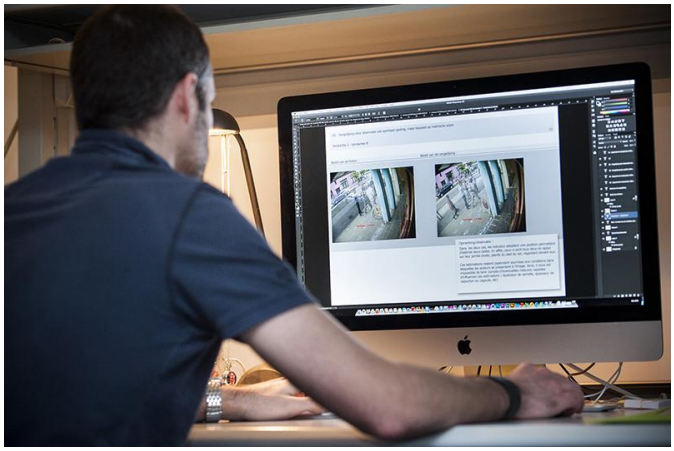
**En matière de coopération internationale**, la FCCU assure toujours le pilotage d'un projet EMPACT consistant à élaborer un module de formation de pointe au sujet du *dark web*. La précédente mouture de la formation avait déjà été accueillie très favorablement.

En 2020, la FCCU a :

- traité 28 dossiers propres (contre 121 en 2019, y compris les missions d'appui au profit d'autres unités) ;
- reçu 50 signalements via l'application web de lutte contre le *ransomware* (contre 171 en 2019). Ce recul est toutefois dû pour l'essentiel à un déficit de signalement (aussi bien en interne qu'à l'extérieur), car les *ransomwares* continuent de faire des ravages.
  Les auteurs de ce type de criminalité informatique installent frauduleusement un virus sur un appareil, à l'insu de son propriétaire. Le logiciel malveillant prend alors "en otage" l'appareil et les fichiers (en les cryptant) et une rançon est réclamée pour les débloquer.




*dossiers de cybercriminalité*



Success Story

## Des condamnations dans un vaste dossier d'abus sur mineurs

Cinq prévenus ont été condamnés à des peines de prison par le tribunal correctionnel de Flandre orientale, division de Termonde, le 31 mars 2020, dans l'un des plus grands dossiers d'abus sur mineurs jamais vus dans notre pays. Mais l'enquête ne s'est pas arrêtée là. La quantité d'images saisies était inédite et a permis l'identification de dizaines de victimes et d'auteurs dans le monde entier. Le dossier est un bel exemple de coopération entre la Police Fédérale, la Police Locale, Europol et Interpol.

Tout a commencé en 2015, lorsqu'un homme prenant des photos d'enfants jouant nus sur la plage a été arrêté. La zone de police VLAS (Courtrai/Kuurne/Lendelede) a ouvert une enquête et a découvert des images digitales d'abus sur mineurs. Les enquêteurs ont également constaté que l'individu était en contact avec un habitant de Wetteren, en Flandre orientale, avec lequel il échangeait des images. Le parquet et la Police Judiciaire Fédérale (PJF) de Flandre orientale ont ouvert une enquête sur cet individu. Sur mandat du juge d'instruction de Termonde, une perquisition a été effectuée et a conduit à la saisie d'environ 15 térabytes (TB) d'images ! La suite des investigations a permis d'identifier trois autres suspects.

Étant donné l'énorme quantité de fichiers et les nombreux contacts en milieu fermé passant par le *dark web*, il a fallu renforcer l'équipe d'enquête et s'engager dans une coopération internationale. La Computer Crime Unit, le service central Child Abuse de la Police Fédérale, la PJF de Flandre occidentale et la zone de police VLAS ont fourni un appui. Au niveau international, Europol a participé à l'analyse des données. Interpol a aidé à transmettre les messages aux collègues de pays non européens.

Cette collaboration intensive entre l'équipe d'enquête et Europol a permis d'identifier plus de 110 victimes et 90 suspects dans le monde entier. Les informations ont entraîné l'ouverture d'enquêtes ou ont pu être liées à des dossiers existants dans plus de 40 pays. Des arrestations et des condamnations ont eu lieu aux quatre coins de la planète. De nombreuses enquêtes sont toujours en cours.

toujours en cours.