Les marketplaces du Darkweb

Matthieu Audibert

Les *marketplaces* du *darkweb*

Par Matthieu AUDIBERT
Officier de gendarmerie et doctorant en droit privé et sciences criminelles,
Université Paris Nanterre – CDPC – EA 3982

Le *darkweb* ou l'Internet sombre fait beaucoup fantasmer. Initialement créé dans le but de contourner les restrictions ou la censure sur Internet, ses fonctionnalités en matière d'anonymat sont devenues prisées des cybercriminels. Plusieurs écosystèmes cybercriminels se sont développés : le plus important est constitué des *marketplaces*. Plateformes de commerce en ligne portant sur des biens ou services illicites, elles génèrent d'importants flux financiers sous la forme d'actifs numériques. Les acteurs étatiques ont pris en compte ces activités cybercriminelles cachées depuis plusieurs années et perfectionnent leurs moyens d'investigation pour identifier les auteurs de ces infractions. Dans le même temps, le droit évolue pour mieux prendre en compte ces évolutions technologiques, notamment en ciblant directement les administrateurs de ces plateformes illégales.

Avertissement : l'auteur s'exprime à titre personnel et dans le cadre de ses travaux universitaires. Ses propos, thèses ou opinions n'engagent en aucune façon la gendarmerie nationale.

« Les *marketplaces* du *darkweb* », voici un sujet d'actualité.

En effet, les médias évoquent régulièrement le démantèlement de telle ou telle plateforme d'échanges cybercriminelle sur le *darkweb*. De même, le *darkweb* ou le *darknet* sont des termes largement répandus dans les médias depuis plusieurs années. Désignant une sorte de zone sombre d'Internet, ce serait le repaire de malfaiteurs, de cybercriminels mais de quoi s'agit-il exactement ? Il convient donc de poser quelques définitions.

Internet est un réseau mondial et immatériel de communications électroniques entre différents supports numériques. Le World Wide Web (WWW) est un sous-ensemble d'Internet communément appelé « le *web*, la toile ». Le World Wide Web est composé de pages *web* hébergées sur des serveurs qui répondent aux utilisateurs par le biais de protocoles de communications électroniques (http ou https). Pour y accéder, les utilisateurs emploient un navigateur Internet (Chrome, Firefox, Safari, etc.).

Au sein du *web*, on trouve trois grands ensembles : le *clear web*, le *deepweb* et le *darkweb* :

- le *clear web* désigne l'ensemble des pages *web* accessibles par un navigateur et référencées par les moteurs de recherche en ligne (Google, Bing…) ;
- le *deep web* désigne l'ensemble des pages *web* accessibles par un navigateur mais non référencées par les moteurs de recherche en ligne. Ces pages *web* sont accessibles uniquement en connaissant le lien qui y mène. Il s'agit enfin de tous les espaces du *web* qui sont accessibles après une authentification des utilisateurs. C'est par exemple le cas des bases de données en ligne ou encore des espaces privés virtuels (*cloud*) ;
- le *darkweb* désigne un ensemble de sous-espaces numériques (les *darknets*) utilisant des protocoles de communication différents du *clearweb* et du *deepweb*. Ces espaces intègrent des fonctions d'anonymisation des communications électroniques ; toute-

fois les informations sont consultables de la même façon que le *web*, il faut juste utiliser des logiciels spécifiques pour y accéder. Les principaux sont Tor, Freenet, I2P, ZeroNet, IPZN ou encore GNU:NET. Il y a donc un *darkweb* composé de plusieurs réseaux *darknets*.

Historiquement créés pour partager des informations de manière sécurisée et anonyme, les *darknets* permettent notamment de contourner la censure d'Internet mise en œuvre par certains États peu respectueux des standards démocratiques. Dès lors, il est un outil de choix pour les journalistes, les universitaires, plus largement les défenseurs de la liberté d'expression sur Internet. Comme toute technologie, le *darkweb* a été dévoyé par les délinquants, notamment les cybercriminels. En effet, ceux-ci ont très rapidement identifiés les potentialités criminelles de ces outils : anonymat garanti lors de la commission d'activités frauduleuses, partage d'informations à caractère illicite, diffusion de contenus illicites (pédocriminalité), trafics en tout genre.

Pour faciliter la mise en relation des auteurs de ces activités illicites, certains ont développé des places de marché ou *marketplaces* au sein desquelles un certain nombre de produits ou services sont illégaux.

De ce fait, quel est l'écosystème de ces *marketplaces* sur le *darkweb* et comment les acteurs étatiques luttent-ils contre ces activités illicites ?

Pour répondre à ces différentes questions, nous étudierons successivement les opportunités cybercriminelles sur le *darkweb* proposées par les *marketplaces* puis l'appréhension des *marketplaces* sur le *darkweb* par les acteurs étatiques.

Les opportunités cybercriminelles offertes sur le *darkweb* par les *marketplaces*

Ces opportunités cybercriminelles offertes par les *marketplaces* reposent en réalité sur une architecture extrêmement répandue sur le *clearweb*. En effet, elles fonctionnent comme un site marchand classique (Amazon) imitant jusqu'aux fonctionnalités de panier, de messages privés, de suivi de commande ou de commentaires et évaluation des produits et des vendeurs. Tout est fait pour mettre vendeurs et acheteurs en confiance. De ce fait, nous étudierons successivement les produits et services proposés sur ces *marketplaces* puis leur fonctionnement.

Les produits et services des *marketplaces* du *darkweb*

Historiquement, les *marketplaces* communément appelées *dark markets* ou *cryptomarkets* se sont développées dès les prémices du *darkweb*. La première était la *marketplace* Silk Road créée en 2011. D'autres ont suivi : AlphaBay Market, Utopia, Atlantis, Agora, Dream Market, etc.

Contrairement au *clearweb*, pour accéder à ces contenus, il faut utiliser des moteurs de recherche spécifiques et dont les résultats sont très variables et parfois peu fiables. En effet, le *darkweb* est caractérisé par des données extrêmement volatiles : les sites changent très régulièrement d'adresses. De ce fait, certaines *marketplaces* ont mis en place des groupes spécifiques sur des messageries chiffrées comme Telegram pour permettre aux utilisateurs de suivre les changements récurrents d'adresses.

Toutefois, des recherches sur le *clearweb* permettent d'identifier rapidement les *marketplaces* proposant des produits et services illégaux : produits stupéfiants, *malwares*[1], faux

[1] Virus informatiques.

documents, *carding*[2], pédocriminalité, armes et munitions, etc. Par ailleurs, si certains sites sur le *darkweb* sont peu prudents, d'autres ont considérablement renforcé leur sécurité. L'accès peut être payant ou rendu possible par cooptation.

Dernièrement, le trafic d'informations personnelles accompagnées de justificatifs dématérialisés a connu un certain essor. Les données sont issues de *leaks*[3] ou de piratages informatiques. Ces données et justificatifs peuvent être vendus de manière autonome ou inclus dans un kit de fraude plus complet qui comprend notamment les guides et les outils pour commettre des fraudes bancaires ou des fraudes à l'identité.

De même, sont régulièrement proposés à la vente des comptes de services de *streaming*[4] ou des comptes de services de paiement[5].

Les cybercriminels proposent également leurs services sous la forme de *Hacking As a Service* sur le modèle des solutions légales Saas[6]. Ces services proposent des piratages de messagerie jusqu'au piratage de terminaux[7]. Une forme de division du travail apparaît dans ce domaine : certains se spécialisent dans le piratage de systèmes informatiques, d'autres en font le commerce sur le *darkweb* et les acheteurs les exploitent ultérieurement. Pour le cas spécifique des ransomware, le *darkweb* comprend des solutions de piratage intégrées nommées *Ransomware as a service*.

Enfin, ces *marketplaces* du *darkweb* comportent, comme les sites marchands sur le *clearweb*, de nombreuses escroqueries. Par exemple, des observateurs ont relevé la vente de services d'assassinat dont la réalité est très souvent fantasmée par les médias. En réalité, la quasi-totalité des sites ou *marketplaces* proposant ce « service » se sont révélés être des escroqueries au même titre que la vente d'êtres humains.

Le fonctionnement des *marketplaces* sur le *darkweb*

Pour comprendre comment fonctionnent ces *marketplaces*, il faut distinguer deux situations, à savoir celle où l'administrateur de la plateforme est un vendeur et celle où l'administrateur ne fait que faciliter la mise en relation entre acheteurs et vendeurs.

De manière générale, ces *marketplaces* partagent toutes l'héritage des sites marchands légaux avec des produits rangés par catégorie, des descriptions, des notes et évaluations, des fonctionnalités de panier, de paiements, de réclamation, de signalement. Tout est fait pour mettre vendeurs et acheteurs en confiance. Les plus élaborées sont celles où les administrateurs se sont spécialisés dans la gestion et l'administration de ces plateformes, autrement dit, ils ne sont pas vendeurs mais tirent leurs revenus d'une « taxe » permettant d'utiliser leurs plateformes.

Outre les produits et services illégaux, ces *marketplaces* diffèrent des sites marchands légaux au travers des moyens de paiement utilisables. Elles n'ont quasiment jamais recours aux monnaies fiduciaires et donc au système bancaire. Dans de rares cas, les cartes prépayées en dollars sont utilisées pour limiter la traçabilité des échanges. Majoritairement, ces plateformes privilégient les actifs numériques ou cryptoactifs[8]. De plus, le recours aux cryptoactifs est souvent accompagné de l'emploi de services de mixages

[2] Données de cartes bancaires.

[3] Fuites de données à caractère personnel.

[4] Netflix, Amazon Prime, etc.

[5] Paypal par exemple.

[6] Software as a service.

[7] Ordinateurs, serveurs, téléphones, etc.

[8] Bitcoin, Monero, Ether, Altcoins, etc.

et d'échangeurs dans le but de brouiller les flux financiers sur la *blockchain* de l'actif numérique utilisé. Aussi, pour limiter le nombre d'escroqueries, ces *marketplaces* ont intégré des tiers de confiance ou *escrow* pour sécuriser les transactions. Cela permet à un acheteur de confier le paiement d'un service ou d'un bien à un tiers qui réalisera la transaction en prélevant une taxe. La somme sera remise au vendeur une fois que l'acheteur aura confirmé la livraison du bien ou service illégal.

Enfin, les échanges sur le *darkweb*, notamment entre acheteurs et vendeurs, ont lieu quasiment *via* des solutions de communications chiffrées légales proposées par des entreprises[9] ou le chiffrement des messages à l'aide de clés PGP.

Une fois ces différents éléments appréhendés, il convient à présent d'étudier comment les acteurs étatiques luttent contre les *marketplaces* sur le *darkweb*.

L'APPRÉHENSION DES *MARKETPLACES* SUR LE *DARKWEB* PAR LES ACTEURS ÉTATIQUES

La réponse des acteurs étatiques repose sur des capacités opérationnelles en évolution permanente et sur l'évolution des outils juridiques à cette forme particulière de cyberdélinquance.

Les capacités opérationnelles pour lutter contre les *marketplaces* sur le *darkweb*

Gendarmerie et police nationales, cyberdouanes, de nombreux acteurs étatiques réalisent de multiples investigations sur le *darkweb* et plus particulièrement sur ces *marketplaces*.

Généralement, tout commence par des opérations de veille spécifique durant lesquelles les enquêteurs vont constater que les services ou biens proposés sur telle ou telle *marketplace* sont illégaux. Les enquêteurs vont alors ouvrir une enquête judiciaire et vont travailler respectivement sur les vendeurs, les acheteurs et les administrateurs de ces plateformes.

Outre leur attribut d'officiers de police judiciaire, les services de l'État ont développé depuis plusieurs années des formations et des moyens spécifiques pour ces investigations particulièrement complexes. Par exemple, la gendarmerie nationale a créé depuis plus de vingt ans les enquêteurs en technologies numériques[10] qui sont à même de réaliser des investigations techniques sur la structure de ces *marketplaces* ou encore de réaliser des perquisitions en ligne ou des saisies informatiques. L'enquête sous pseudonyme est également extrêmement précieuse puisqu'elle permet aux enquêteurs de se faire passer pour un acheteur potentiel. Dans ce cas, les enquêteurs peuvent réaliser, soit un achat de confiance[11], soit un coup d'achat[12].

Plus récemment la gendarmerie a développé les enquêteurs spécialisés en actifs numériques ou FINTECH qui sont en mesure de réaliser des investigations sur les différentes *blockchains*, de suivre les flux financiers et de procéder à la « désanonymisation » de certaines transactions. Dans cet objectif, ils vont procéder au traçage des cryptoactifs, à l'étude des services de mixage

[9] Proton mail, Tutanota, Elude, SecMail, etc.

[10] NTECH.

[11] La transaction est réalisée, l'argent public est engagé et le bien ou le service illégal est mis à la disposition des enquêteurs qui vont pouvoir réaliser des investigations.

[12] C'est l'hypothèse où l'argent n'est pas versé mais qu'une rencontre est organisée. Ces opérations permettent des interpellations en flagrant délit.

Leur objectif ultime est ensuite de procéder à la saisie des actifs numériques ou cryptoactifs qui seront conservés. Ainsi, le volet blanchiment des investigations est souvent déterminant puisqu'il permet à la fois d'identifier les acheteurs et les acquéreurs.

L'adoption de nouveaux outils juridiques

Indissociable de l'action des enquêteurs, plus largement des autorités publiques, les outils juridiques ont évolué pour appréhender les actions illicites commises sur les *marketplaces* du *darkweb*. La loi n°2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur est venue apporter des outils précieux aux enquêteurs.

S'agissant des outils procéduraux, la loi permet dorénavant aux enquêteurs de réaliser des investigations plus poussées dans le cadre des enquêtes sous pseudonyme pour confondre les auteurs des infractions commises dans les espaces numériques. Ainsi, les enquêteurs peuvent désormais « après autorisation du procureur de la République ou du juge d'instruction saisi des faits, en vue de l'acquisition, de la transmission ou de la vente par les personnes susceptibles d'être les auteurs de ces infractions de tout contenu, produit, substance, prélèvement ou service, y compris illicite, mettre à la disposition de ces personnes des moyens juridiques ou financiers ainsi que des moyens de transport, de dépôt, d'hébergement, de conservation et de télécommunication[13] ». Avec ces dispositions, les enquêteurs vont pouvoir davantage pénétrer en profondeur les réseaux criminels sur le *darkweb*.

De plus s'agissant des usages illicites des actifs numériques ou cryptoactifs, la loi permet aux officiers de police judiciaire, sur autorisation du procureur de la République ou du juge d'instruction, de réaliser, au même titre de ce qui existe déjà pour les actifs bancaires, des saisies d'actifs numériques qui sont aujourd'hui plus rapidement et aisément dissimulables que des actifs bancaires. L'objectif ici est de lutter plus efficacement contre la volatilité et la fongibilité des actifs numériques : suivre les flux financiers permet régulièrement d'identifier les auteurs d'infractions.

Enfin, la loi d'orientation et de programmation du ministère de l'Intérieur est venue cibler spécifiquement les *marketplaces* sur le *darkweb* en créant deux nouveaux délits introduits à l'article 323-3-2 du Code pénal.

En premier lieu, il s'agit du délit d'administration d'une plateforme en ligne pour permettre la cession de produits, de contenus ou de service dont la cession, l'offre, l'acquisition ou la détention sont manifestement illicites. Le législateur a délibérément ciblé les *marketplaces* sur le *darkweb* puisqu'il vise spécifiquement les plateformes en ligne restreignant l'accès aux personnes « utilisant des techniques d'anonymisation des connexion[14] » ou les plateformes qui ne respectent pas les obligations légales relatifs à la collecte et la conservation des données techniques de connexion.

En second lieu, le législateur a créé le délit d'intermédiation ou de séquestre ayant pour objet unique ou principal, la mise en œuvre, la dissimulation ou la facilitation de ces opérations. Autrement dit, ce sont ici les services d'*escrow* qui sont ciblés.

In fine, le législateur a complété le dispositif juridique de lutte contre les *marketplaces*, d'une part en s'attaquant directement aux administrateurs de ces plateformes et d'autre part en ciblant tous les services de paiement par un tiers de confiance qu'elles utilisent.

Ces deux infractions autonomes présentent un avantage. Contrairement aux autres infractions pouvant leur être imputées, elles ne nécessitent pas de caractériser la compli-

[13] Article 230-46 du Code de procédure pénale.

[14] Article 323-2-2 du Code pénal.

cité dans la commission d'un fait principal punissable. Autrement dit, nous avons ici deux infractions autonomes qui ciblent directement les *marketplaces* sur le *darkweb*.

Pour conclure, les *marketplaces* sur le *darkweb* présentent toujours de nombreuses opportunités cybercriminelles mais les autorités publiques ont massivement investi le *darkweb* pour identifier les administrateurs de ces plateformes et les acheteurs et vendeurs qui utilisent leurs services. La clé des investigations réside souvent dans le suivi des transactions financières sur la *blockchain*. C'est le principal enjeu en lien avec l'évolution exponentielle des actifs numériques : suivre les transactions, les désanonymiser et pouvoir saisir les fonds provenant de ces activités criminelles.

Bibliographie

CHARPENEL Y. (2017), *Le darkweb, un objet juridique parfaitement identifié*, Dalloz IP/IT, p. 71.

DE MAISON ROUGE O. (2017), *Darkweb* : *plongée en eaux troubles*, Dalloz IP/IT, p. 74.

DUSSOPT O. (2021), *Les enjeux juridiques de la cybercontrefaçon*, Dalloz IP/IT, p. 483.

KELLER S. (2019), *Corréler les transactions bitcoins avec les informations disponibles dans le darkweb – le projet iTrac*, Dalloz IP/IT, p. 543.

LAURENT X. (2021), *Retour d'expérience sur le premier démantèlement d'une plateforme francophone du darkweb : le dossier Back Hand*, Dalloz IP/IT, p. 79.

LEVASTRE-BODOULE A. & SOSSO D. (2021), *Les principaux usages illicites de l'Internet sombre*, Dalloz IP/IT, p. 83.

LEVASTRE-BODOULE A. & SOSSO D. (2021), *Tor en pratique*, Dalloz IP/IT, p. 89.

MARTINON J. (2021), *Propos introductifs sur les darknets*, Dalloz IP/IT, p. 69.

MARTINON J. (2019), *Crypto-actifs : la justice pénale à l'épreuve des crypto-monnaies*, Dalloz IP/IT, p. 531.

PERNET C. (2021), *Le darknet*, Dalloz IP/IT, p. 73.

PERRIER J.-B. (2023), « Les infractions et sanctions de la LOPMI, ou la répression de Potemkine », *RSC*, p. 381.

PETIT A. (2017), *Visite guidée du darkweb cybercriminel*, Dalloz IP/IT, p. 86.

QUEMENER M. (2017), *Enquêtes dans le darkweb*, Dalloz IP/IT, p. 83.

STAMBOLIYSKA R. (2017), *La face cachée d'Internet : Hackers, Darkweb, Tor, Anonymus, Wikileaks, Bitcoins...*, Larousse, 07 juin.

TOULLIER M. (2017), « Lumière sur un arsenal de lutte contre une délinquance tapie dans l'ombre », *AJ pénal*, p. 312.