Le darknet et le droit

Boris Barraud

Laboratoire interdisciplinaire droit, médias et mutations sociales (LID2MS),
Université d'Aix-Marseille

La Semaine juridique - Édition générale (LexisNexis), n° 1-2, janv. 2018, p. 6-10

L'internet tend à ignorer les territoires et les frontières. Or, s'il tend à ignorer les territoires et les frontières, il tend à ignorer dans le même mouvement les États qu'ils bornent. Le cyberespace est ambiant, un peu à la manière de l'éther et des ondes électromagnétiques. Et les internautes sont des ubiquitaires, partout et nulle part à la fois, capables d'agir en divers endroits dans le même temps et de former des communautés déterritorialisées. Certaines de ces communautés peuvent se constituer autour d'objets illicites ; des utilisateurs du réseau mondial peuvent en profiter pour commettre des actes illégaux. Cependant, les États sont parvenus, certes non sans mal et imparfaitement, à juridiciser l'internet — *i.e.* à faire en sorte que le droit y soit applicable et, quoiqu'avec davantage de difficultés, appliqué. Nombre de dispositifs législatifs, d'accords internationaux, d'interventions jurisprudentielles, mais aussi de propositions doctrinales, ont permis au droit de saisir l'internet, de lui donner un cadre juridique relativement cohérent, complet et efficace.

Si l'internet et le droit ne s'ignorent donc plus, un nouvel ensemble de réseaux informatiques défie aujourd'hui le droit : le darknet. Beaucoup des activités illégales qui profitaient autrefois de l'impunité offerte par l'internet ont migré vers le darknet. Les nouvelles technologies de l'information et de la communication n'ont ainsi de cesse de bouleverser les sociétés, leurs habitudes et, par suite, le droit qui est censé les accompagner. Celui-ci n'a d'autre choix que de s'adapter, quoique dans sa forme bien plus que dans son contenu. Y parvient-il — et le peut-il seulement — en matière de darknet, dernier témoignage de ces mouvements technologiques incessants ?

Pour être exact, il faudrait évoquer « les darknets », même si l'on a pris l'habitude de parler « du darknet » afin de désigner l'ensemble de ces darknets. Un darknet est un réseau privé et autonome — les différents darknets ne sont pas interopérables, ne s'associent pas afin de former un inter-réseaux. Il profite des technologies de l'internet mais recourt à des logiciels, des configurations et des autorisations spécifiques. La caractéristique essentielle d'un darknet est d'anonymiser les activités de ses utilisateurs, de les crypter. Quant au darkweb, il s'agit d'un des principaux services accessibles grâce aux darknets — comme le web (protocole <http>) est un des principaux services de l'internet.

Le darknet est donc une forme d'internet parallèle, mystérieux et secret. Il est caché et invisible, c'est-à-dire que ses acteurs et utilisateurs sont cachés et invisibles, non identifiables au moyen des technologies habituellement utilisées afin de réguler l'internet et ses services — et sanctionner les éventuels auteurs d'infractions. En premier lieu, le darknet interdit toute identification des adresses IP des ordinateurs connectés, *i.e.* leurs numéros d'immatriculation numérique. Cet

anonymat des darknautes a favorisé le développement du marché noir et des activités délictuelles en tous genres, ainsi que la mise en ligne d'innombrables contenus illicites. Les réseaux sombres servent de support à un nombre croissant d'activités illégales. Or cela s'explique avant tout par l'impression d'une zone de non-droit qu'ils procurent, par le sentiment d'impunité qui anime les cybercriminels.

Si l'on définit le droit en tant que droit de l'État, alors le darknet s'est construit loin du droit et a prospéré notamment en raison de cette image d'ajuridicité qui l'accompagne. Cependant, il ne se développe pas loin des normes. Tout d'abord, il repose sur nombre de normes technologiques. Ensuite, ses acteurs et utilisateurs opèrent dans le cadre de codes et usages privés dont le niveau d'effectivité est remarquable. Seulement ces codes et usages privés ne sont-ils pas toujours compatibles avec les lois, tant s'en faut. En témoigne le sort réservé aux propriétés intellectuelles. Aussi le juriste qui observe ces réseaux parallèles ne peut-il qu'être saisi par leur besoin de droit — *i.e.* par leur besoin de régulation étatique. On ne saurait justifier un quelconque abandon de ce nouvel espace immatériel à des puissances privées défendant des intérêts privés qui, parfois, sont aussi des intérêts crapuleux.

Pourtant, le droit applicable aux activités du darknet ne manque pas. Si ce dernier se présente tel un supermarché mondial de produits illicites, il est, comme les autres pans du cyberespace, un domaine dans lequel toutes les règles de droit, du droit pénal au droit fiscal, ont vocation à s'appliquer. La difficulté est de les faire respecter concrètement — et ce n'est pas la moindre des difficultés (I). La barrière technologique est-elle infranchissable pour le droit, est-elle capable d'interdire l'entrée à toutes les autorités exécutives et juridictionnelles ? Il faut gager que tel ne saurait être le cas, que le darknet n'est pas incompatible avec le droit. En effet, au cours des derniers mois, les pouvoirs publics sont parvenus à fermer plusieurs sites illégaux comptant au nombre des plus importants du darkweb. C'est pourquoi celui-ci mériterait de moins en moins d'être compris telle une zone de non-droit (II). Pour autant, les services de police devront persévérer et peut-être trouver de nouveaux alliés et de nouveaux moyens (juridiques et/ou technologiques) s'ils entendent endiguer durablement l'hypertrophie criminelle du darknet et du darkweb, s'ils souhaitent permettre au droit de triompher de la force technologique, à la régulation publique de l'emporter sur la régulation privée, à l'intérêt général de dominer les intérêts particuliers et à l'ordre public de s'imposer face au désordre libertaire.

I. Le droit à l'épreuve du darknet

Il existe sans aucun doute un droit du darknet — très peu différent du droit de l'internet, lui même très peu différent du droit commun. Les juristes, dès lors qu'ils sont normativistes-positivistes, c'est-à-dire dès lors qu'ils sont portés à juger le droit à l'aune de sa seule validité, trouveront sans peine un grand nombre de normes applicables aux réseaux parallèles et aux activités qu'elles véhiculent (A). En revanche, qui se focalise non plus sur la validité des normes mais sur leur effectivité opérera sans doute un tout autre constat : il s'avère ô combien difficile de faire respecter le droit dans le monde du darknet (B).

A. La validité du droit : beaucoup de normes applicables au darknet

Autant de règles de droit sont applicables au darknet qu'à l'internet. Le contenu du droit du darknet est semblable au contenu du droit de l'internet. La loi française ne distingue pas entre les différentes couches de réseaux de communication et ce sont les mêmes dispositions qui ont vocation à s'appliquer au clearweb et au darkweb. Les darknets, juridiquement, ne présentent guère de spécificité. Les droits pénal, civil, fiscal, des communications électroniques, des données personnelles, de la propriété intellectuelle ou encore du commerce électronique doivent normalement s'y appliquer. Une infraction est constituée dans le monde du darknet autant qu'ailleurs. Sous l'angle du droit valide, il ne saurait en aucun instant s'agir d'une zone de non-droit.

La difficulté est qu'il en va très différemment sous l'angle du droit effectif : les lois et la justice étatiques y sont peu présentes, peu influentes, tandis que des formes d'autorégulation à base de codes et d'usages privés s'y développent — au service d'intérêts particuliers et d'un esprit libertaire plus qu'au service de l'intérêt général et de l'ordre public. Mais ce ne sont pas les règles de droit qui manquent au darknet ; ce qui lui fait défaut, ce sont les moyens de les appliquer et de les faire respecter. En d'autres termes, le darknet interroge moins le pouvoir législatif que le pouvoir exécutif et le pouvoir judiciaire.

Les juristes normativistes se demandent si le droit est suffisamment performant et si les États sont suffisamment armés juridiquement pour faire face aux problématiques techniques posées par les nouvelles technologies de l'information et de la communication, donc si le contenu des lois et des règlements est adapté aux besoins et aux enjeux. D'un point de vue juspragmatiste, il importe aussi — et peut-être surtout — de se demander si le droit est suffisamment performant dans le sens de suffisamment puissant, suffisamment efficace, suffisamment accepté et respecté par ses destinataires. Or il s'en faut de beaucoup que tel soit le cas concernant le droit du darknet. Un des grands apports du droit de l'internet et, aujourd'hui, du droit du darknet est ainsi d'inciter la doctrine à étudier autant le droit appliqué que le droit applicable, autant les pratiques juridiques que les textes juridiques, autant la vie du droit que la validité du droit — car il peut exister un fossé entre les uns et les autres. C'est pourquoi l'effectivité tend à devenir un critère de juridicité à part entière. Ce qui interroge est moins ce que le droit du darknet est que ce que le droit du darknet fait.

B. L'effectivité du droit : peu de normes appliquées au darknet

Les nouveaux réseaux de communication transnationaux, outils privilégiés de la mondialisation, permettent à une personne ressortissante d'un État A de commettre une infraction sur le territoire d'un État B tout en demeurant sur le territoire de l'État A. Pour les autorités publiques, l'informatique en nuage s'apparente à un informatique en nuage de Tchernobyl : la souveraineté ne suffit pas à se préserver de certains phénomènes indésirables. Des frontières technologiques remplacent les frontières géographiques et politiques. L'État peine à saisir normativement les activités en ligne parce que son droit est territorialisé quand ces dernières sont déterritorialisées. Toutefois, les grandes problématiques de la loi applicable et de la juridiction compétente semblent désormais en passe d'être résolues. Les règles (et les difficultés) en matière de compétences sont les mêmes qu'il

s'agisse de clearweb ou de darkweb. Elles dépendent d'approches identiques et appellent des solutions identiques.

Si les darknets constituent des espaces abstraits transterritoriaux ou aterritoriaux qui malmènent les États, c'est surtout une autre difficulté qui rend l'application du droit difficile : l'immense majorité des infractions commises grâce aux réseaux parallèles sont invisibles ; leurs auteurs ne sont l'objet d'aucune sanction parce qu'ils ne sont pas identifiables, si bien qu'ils demeurent inaccessibles aux services de police et, par suite, aux institutions judiciaires. C'est pourquoi, du point de vue du droit appliqué, le darknet se présente telle une zone de non-droit bien que, du point de vue du droit applicable, il soit pleinement saisi par les normes. Les juristes parviennent à adapter le droit — qui n'en a d'ailleurs besoin que de temps à autre — aux bouleversements des technologies de l'information et de la communication qui se produisent au XXI^{e} siècle. Ils définissent de nouvelles catégories et élaborent de nouveaux concepts qui confèrent au droit une évolutivité suffisante. Mais, dès lors qu'il s'agit de faire en sorte que ces catégories et concepts produisent leurs effets en pratique, régulant concrètement les comportements des acteurs et utilisateurs des darknets, les obstacles changent de dimensions.

Même en développant les services de police transfrontalière et les ententes douanières, la répression des infractions commises dans le darknet n'en achoppe pas moins sur leur transparence et sur l'anonymat dont leurs auteurs profitent. Le cyberespace a amené les pouvoirs publics à se poser la question de la saisissabilité juridique du réseau mondial comme ils se sont posés la question de la saisissabilité juridique des mers ou de l'espace extra-atmosphérique. Avec le darknet, il convient de s'interroger en outre quant à la saisissabilité technologique des activités dématérialisées. Il se pourrait que cette problématique, moins juridique que matérielle au contraire des « simples » questions de territorialité des compétences, soit plus difficile à résoudre. Toujours est-il que les autorités publiques s'y emploient et que leurs efforts commencent à porter leurs fruits.

II. Le droit à la conquête du darknet

Au cours des derniers mois, plusieurs opérations policières d'envergure ont permis de fermer certaines des principales places fortes du e-commerce clandestin. Les arrestations des créateurs et administrateurs des sites Alpha Bay et Hansa, durant l'été 2017, ont constitué des étapes importantes de ce processus de soumission effective du darknet au droit (A). Mais cela suffira-t-il à mettre fin au sentiment d'impunité ou sentiment de non-droit qui anime ceux qui profitent de l'anonymat offert par les réseaux parallèles pour s'y livrer à des activités répréhensibles (B) ?

A. La multiplication des interventions afin de juridiciser concrètement le darknet

Les réseaux obscurs n'étant pas des réseaux fermés, les services de renseignement et d'enquête peuvent sans peine s'y introduire, profitant à leur tour de l'anonymat offert. Mais être présent dans les darknets ne saurait suffire à y constater les infractions et à identifier leurs auteurs. Traquer les délinquants au sein des réseaux parallèles suppose d'engager des moyens importants et de faire face à des contraintes nouvelles, sans garantie d'obtenir des résultats probants. Contrairement à la situation de l'internet, il n'existe que peu d'opérateurs techniques prêts à coopérer et sur lesquels

s'appuyer ; les contraintes technologiques sont sensiblement plus fortes ; et les coûts d'établissement des preuves se trouvent largement augmentés en raison des méthodes et instruments particuliers à mobiliser.

Reste que le FBI, le FSB, Europol et les autres polices nationales ou internationales multiplient les opérations visant à décriminaliser le darknet. Par conséquent, celui-ci constitue de moins en moins un espace libéré du droit dans lequel il serait loisible de commettre impunément toutes formes d'infractions. Les derniers développements de cette entrée effective des règles de droit dans le monde du darknet correspondent aux fermetures, durant l'été 2017, d'Alpha Bay et Hansa, respectivement première et troisième plus grosses plateformes commerciales du darkweb. Il s'agit peut-être d'un tournant dans le processus de juridicisation du darknet ; à moins que les cybertrafiquants ne parviennent à construire rapidement de nouvelles places de marché hors d'atteinte des forces de police. L'enjeu, du point de vue de ces cybertrafiquants, est évident : que ne se rompe pas la confiance de leurs « clients », que ceux-ci continuent à voir dans le darknet un espace protégé contre toute contrainte juridique.

Au total, près de 10 000 acheteurs ont été identifiés et leurs coordonnées ont été transmises aux autorités des pays concernés. Certainement le mythe d'un darknet terre d'élection des criminels ne sort-il pas indemne de ces opérations policières menées avec succès. Celles-ci devraient porter atteinte à la confiance que beaucoup de leurs utilisateurs font aux plateformes de commerce électronique illégal. Cependant, il faut gager que d'autres opérations d'envergure seront nécessaires afin que, réellement, le sentiment d'impunité et de non-droit laisse la place à l'ordre public et au respect du droit dans le darknet.

B. La diminution insuffisante du sentiment de non-droit dans le darknet

La fermeture d'Alpha Bay a entraîné l'évaporation de millions d'euros de Bitcoins que les utilisateurs avaient placés dans leurs portemonnaies électroniques. Peut-être ces utilisateurs ne seront-ils pas tentés de se reporter incontinent vers d'autres sites illégaux, au risque que pareille mésaventure se reproduise. Le meilleur moyen de juridiciser le darkweb, de faire en sorte qu'il ne soit plus perçu telle une zone de non-droit, serait donc de multiplier autant que possible les interventions touchant le plus grand nombre d'acteurs du darkmarket soit directement, soit indirectement à travers leur médiatisation.

L'enjeu est de susciter un sentiment d' « insécurité criminelle ». Les trafics de produits illicites reposent essentiellement sur la confiance. Par conséquent, plus les acheteurs et vendeurs potentiels ressentent qu'ils peuvent s'adonner à des activités prohibées à l'abri de la loi et de la justice, moins ils auront de scrupules à passer à l'acte. Ce serait ainsi contre la confiance générée par le darknet grâce à l'anonymat et à l'absence de traçabilité des échanges que les autorités publiques devraient lutter en priorité, en montrant (ou en faisant croire) que cet anonymat et cette absence de traçabilité des échanges sont tout à fait relatifs.

Néanmoins, par le passé, les places de marché illégales se sont illustrées par leur grande résilience, de nouveaux sites remplaçant les anciens en gagnant à chaque fois de nouveaux utilisateurs. Les autorités publiques seraient ainsi lancées dans une course-poursuite interminable, chaque destruction d'une place forte du e-commerce illégal engendrant l'avènement d'une autre. Il semble excessivement difficile d'endiguer la croissance de la demande de produits ou données illicites ; et il paraît quasi-impossible d'empêcher qu'une offre se développe afin d'y répondre. Enfin, il faut craindre que d'autres technologies apparaissent et permettent aux trafiquants de mieux masquer

leurs identités et dissimuler leurs activités. Grâce à ces technologies, se consoliderait à nouveau la confiance que les forces de police s'évertuent à fragiliser. Les nouvelles technologies de l'information et de la communication se présenteraient donc tel un rocher de Sisyphe pour le droit et la justice. Mais jamais le droit et la justice ne démissionnent.

*

* *

Accusés non sans raison d'être la terre d'asile de nombreuses formes de délinquance, les darknets ont néanmoins été créés à des fins tout autres. S'ils ont largement été détournés de leur usage premier, ils avaient initialement vocation à permettre aux internautes d'utiliser le web tout en protégeant leurs données personnelles et leurs vies privées. Alors que les multinationales de l'internet reposent pour la plupart sur un modèle économique consistant à vendre à des annonceurs la vie privée et les informations personnelles de leurs utilisateurs, les technologies permettant d'échapper au traçage et au suivi des activités en ligne prennent tout leur sens. Les données personnelles sont peut-être le pétrole du XXI^e^ siècle. De nombreuses entreprises, mais aussi de nombreux États, mettent en œuvre des moyens colossaux afin de les recueillir et de surveiller, quelles qu'en soient les fins, les informations échangées dans le cyberespace. Aussi différents médias ont-ils créé des coffres-forts numériques dans le darknet où les lanceurs d'alerte peuvent déposer discrètement les documents sensibles en leur possession.

Ce darknet ne répond donc pas uniquement à la demande de cyberdélinquants à la recherche de technologies leur permettant de commettre impunément des infractions ; il répond aussi à la demande d'usagers de l'internet qui souhaitent échapper à la surveillance de « Big Brother », *a fortiori* après les révélations d'Edward Snowden concernant la surveillance de masse opérée par la NSA. Les réseaux parallèles peuvent donc desservir le droit, mais aussi le servir en garantissant, grâce à l'anonymat, la protection de la vie privée.

Plus encore, les darknets peuvent être d'un précieux secours au sein de certains régimes tyranniques ou autoritaires qui, d'une part, brident largement l'accès à internet de la population et, d'autre part, surveillent les activités en ligne des journalistes, opposants politiques, défenseurs des droits de l'homme et autres activistes. Car les États ne sont pas aussi démunis face au cyberespace qu'on peut le penser au premier abord et la non maîtrise de celui-ci est autant choisie que subie par les pouvoirs publics. Si, dans certains pays, les autorités se préoccupent davantage de garantir la liberté d'expression et autres droits et libertés en ligne que de prévenir la commission de nombre d'infractions, dans d'autres, en revanche, on préfère sacrifier les droits et libertés fondamentaux sur l'autel d'une raison d'État particulière, donc empêcher matériellement certaines communications. Les réseaux alternatifs peuvent dès lors constituer de précieux alliés pour l'exercice des libertés fondamentales. En somme, ce qui apparaît telle une menace dans les pays démocratiques est perçu comme une chance dans les pays soumis à la dictature, à l'oppression et à la censure de masse.

La liberté numérique — comprise comme liberté naturelle et non politique ou juridique — n'est en soi ni bonne ni mauvaise, ni bénéfique ni nuisible. Elle permet aux hommes d'exprimer leur pleine nature loin de toute tutelle publique. Mais Thomas Hobbes n'a-t-il pas, il y a déjà longtemps, mis en garde contre le fait que « l'homme est un loup pour l'homme » et montré combien le « besoin d'État » est fort ? Seulement l'État, dans le cyberespace du XXI^e^ siècle, n'est-il plus le Léviathan d'hier. Il semble de plus en plus dépassé, de plus en plus concurrencé, de plus en plus démythifié.

Les opérations de police précédemment évoquées montrent que les États ne sont cependant pas totalement démunis. Mais elles ne sauraient suffire à enrayer la frénésie délictuelle qui empreint le darkweb. Dans ces conditions, peut-être la juridicisation de ce dernier en passera-t-elle par

l'intervention de puissances privées au moins autant que par l'intervention de puissances publiques. Le cyberespace étant le monde de technophiles parmi lesquels seule une minorité est animée par des desseins illicites, ceux-ci pourraient, par divers modes d'autorégulation, lutter contre la prolifération des activités interdites. En témoigne le fait que les Anonymous et les « *dark hunters* », prenant acte des carences de pouvoirs publics, jouent un rôle de plus en plus cardinal dans la régulation des darknets.

Aussi ces darknets constituent-ils un témoignage de plus du défi que les nouvelles technologies de l'information et de la communication lancent au pouvoir de régulation des États, à leur souveraineté et à leur puissance.