droit : les saisies de nom de domaine, **bannissement électronique**

Il y a plusieurs siècles, la peine de bannissement consistait à enjoindre à une personne de se retirer d'un lieu ou d'un territoire désigné, avec défense d'y revenir pendant un certain temps ou toute la vie. Il s'agissait de faire perdre la vie civile à la personne frappée par cette sanction. Cette punition sévère a heureusement disparu dans les démocraties occidentales... ou du moins le croyait-on ! Car elle pourrait bien être en train de revenir sous une forme sournoise, sur internet.

Nos existences se vivent toujours plus en ligne : communications écrites ou téléphoniques, partage de photos ou de vidéos, recherche de l'Amour sur les sites spécialisés, militantisme sur les réseaux sociaux, blogs et forums, etc. Ces activités qui prennent forme sur internet reposent toutes, sans qu'on n'y prête attention, sur les mêmes fondations : les noms de domaine. C'est sur la base d'un nom de domaine qu'on peut créer et utiliser une adresse mail permettant la correspondance privée, grâce à ce nom que l'on peut mettre en ligne des informations et qu'un moteur de recherche peut y conduire. Il existe aujourd'hui 250 millions de noms de domaine qui, tous ensemble, constituent la structure de nos activités électroniques.

Les noms de domaine servant à tout, ils sont aussi exploités à des fins illégales : des casinos en ligne sont grâce à eux accessibles dans des pays interdisant cette forme de jeu, le streaming de films ou d'épreuves sportives recourt aussi à ces outils... et les opérateurs de ces sites sont experts en dissimulation, sachant notamment comment cacher leur identité véritable et utiliser des serveurs situés dans des pays *« accueillants »*. La chose n'est pas nouvelle : sur internet, les fraudeurs professionnels usent de toutes les ficelles permettant d'échapper à la justice.

« les administrations mobilisées en Europe sont prêtes à exécuter des décisions prises depuis les États-Unis et dans d'obscures conditions »

Cédric Manara

DR / Henri Thauvoye

des méthodes plus brutales

C'est peut-être parce qu'il est difficile d'utiliser contre eux les voies de droit que des autorités ont décidé d'employer des méthodes plus brutales pour bouter leurs activités hors du web. L'Immigration and Customs Enforcement (ICE), soit les douanes des États-Unis, a lancé un programme d'action baptisé Operation in our sites afin d'enrayer la vente de médicaments contrefaits en ligne ou le piratage d'œuvres (films, musique, logiciels). Si le but est louable, la méthode choisie est critiquable.

Son dispositif central consiste à saisir les noms de domaine des sites visés, de manière à en empêcher l'accès. Point n'est besoin pour cela de connaître celui qui détient le nom de domaine ou l'exploite : il suffit de s'adresser à l'intermédiaire auprès duquel le nom a été enregistré (voire au registre qui est en charge du domaine de premier niveau auquel se nom se rattache, par exemple l'entreprise américaine VeriSign qui gère la zone .com dans laquelle plus de cent millions de noms ont été créés). Nombre de ces intermédiaires se trouvant aux États-Unis, il est facile pour les autorités locales d'enjoindre la suspension

d'un nom de domaine qu'elles ont dans le collimateur ou de le confisquer. Inexistantes il y a encore deux ans et demi, ces mesures semblent désormais avoir les faveurs de ceux qui sont chargés de faire respecter la loi : depuis juin 2010, ce sont 1 630 noms de domaine qui ont été saisis.

un procédé qui a pu se révéler arbitraire

On pourrait applaudir cette efficacité : voici enfin un moyen rapide et peu onéreux d'écraser des sites prospérant dans l'ombre ! Pourtant, on ne peut se satisfaire en droit d'un tel procédé sommaire, qui en outre a pu se révéler arbitraire.

La mesure frappe un nom de domaine parce qu'il offre l'accès à des produits ou services illégaux. Mais il peut aussi dans le même temps permettre la consultation en ligne de contenus conformes au droit. C'est ce qu'a révélé en février 2011 la saisie du nom Mooo.com. Celle-ci fut motivée par la découverte d'activités irrégulières accessibles par un sous-domaine rattaché à ce nom (du type Sousdomaine.mooo.com). En désactivant le nom, les autorités ont entraîné dans les limbes 84 000 autres sites qui dépendaient de lui, pour la simple raison que leur adresse était aussi du type Sousdomaine.mooo.com. C'est un peu comme si on avait bouclé toute une ville pour dératiser une maison en particulier !

La mesure peut aussi revenir à frapper une personne n'ayant rien à voir avec les activités illégales exercées sous la bannière du nom de domaine qui lui appartient. Sur les plateformes de blogs, sur les forums, ce sont les utilisateurs qui publient des informations qui peuvent s'avérer contraires à la loi. Si ces contenus venaient à entraîner les foudres des douanes américaines et la saisie du nom de domaine sous l'ombrelle duquel ils sont accessibles, la mesure viendrait heurter l'éditeur de l'espace de blogs ou du forum qui est un tiers aux utilisateurs indélicats. Un peu comme si l'on sanctionnait l'exploitant d'une autoroute du sud de la France parce qu'on y a trouvé des véhicules en provenance d'Espagne transportant de la drogue.

Surtout, la mesure est prononcée par une autorité compétente à l'intérieur des frontières des États-Unis sur le fondement de règles applicables dans ce seul pays. Mais elle a mécaniquement un effet dans le monde entier ! Ce qui circule sur internet peut être illégal dans un pays, mais pas d'autres. Depuis l'épicentre américain, ont donc été prises plus de 1 500 fois des décisions de portée globale. Des précédents annonciateurs d'un nouveau mode de régulation des réseaux ? En tout cas des exemples aussi répétés que fâcheux.

iniquité des procédures de saisie

Car non seulement chaque saisie est contestable dans son principe et dans ses effets, mais en plus elle s'opère de manière opaque. Certes, on peut comprendre que les autorités ne puissent communiquer à l'avance la liste de leurs cibles et les raisons qui les amènent à agir, afin de pouvoir le faire par surprise. Néanmoins, on pourrait espérer qu'après une opération, l'objet des saisies et les motifs soient connus. Ce n'est pourtant pas le cas : il faut se contenter de lire les communiqués de l'ICE, qui sont parfois si sibyllins qu'on croirait interpréter l'oracle ! C'est de façon éparse, par des témoignages ou des enquêtes, que l'on finit par apprendre que des noms de domaine comme Rojadirecta.com ou Dajaz1.com ont pu être saisis. L'histoire de ces deux derniers noms est particulièrement révélatrice de l'iniquité des procédures de saisie :

- Suite à une opération douanière, le titulaire du premier a engagé une action en justice afin de récupérer son bien. Sans succès. Mais dix-neuf mois après la saisie, les autorités lui ont restitué le nom de domaine, sans explication... ni excuse.
- Le nom Dajaz1.com a quant à lui été saisi un an – semble-t-il sur la seule foi d'un affidavit (attestation établie par un professionnel du droit) – puis rendu à son titulaire qui a ainsi été privé pendant douze mois d'un moyen de communication et d'existence en ligne !

Si la lutte contre la contrefaçon ou les contenus illicites est justifiée, la saisie de noms de domaine à cette fin ne l'est pas. Dans le monde physique, quand on saisit un local où étaient entreposées des armes, on place des scellés, mais on ne mure pas les portes et les fenêtres, pas plus qu'on ne condamne la boîte aux lettres. C'est pourtant ce que l'on fait désormais sur internet : saisir un nom de domaine est une méthode excessive, notamment parce qu'elle a pour effet d'empêcher l'utilisation des e-mails associés à ce nom et même de permettre le détournement de correspondance par le tiers saisissant.

violations des libertés fondamentales

Fin novembre 2012, l'ICE a annoncé, par un nouveau communiqué peu transparent, qu'elle avait invité différents homologues européens à participer avec elle à une nouvelle opération de saisie. Avec le concours d'Europol et de plusieurs autorités nationales — dont la France, selon le communiqué —, 132 nouveaux noms de domaine ont été saisis. Ainsi apprit-on que les saisies ne se limitent plus aux noms en .com ou .us, mais peuvent désormais s'étendre aux domaines .eu, .be, .dk, .ro... et peut-être bien .fr. Et que les administrations mobilisées en Europe sont prêtes à exécuter des décisions prises depuis les États-Unis et dans d'obscures conditions. Il ne s'agit *« que »* de 1 630 noms sur les 250 millions que l'on dénombre. Mais il s'agit d'autant de violations des libertés fondamentales : droits de la défense, droit à un procès équitable, obligation de motivation des décisions, droit au respect de la vie privée sont en cause ici. Ce sont des captures sauvages d'avoirs électroniques. Non seulement elles se multiplient, mais d'autres autorités que celles des États-Unis les amplifient. Qu'il y ait en ligne des contenus illicites est illégal et nécessite des mesures, mais ne justifie pas que soient prises des mesures illégales. ■

Cédric Manara

[Professeur à l'Edhec Business School (LegalEdhec Research Center), travaille sur les questions juridiques liées à internet. Auteur de *Le droit des noms de domaine* (éd. LexisNexis, collection IRPI, 2012). Membre de l'Adij et lauréat du Prix Adij 2007]