economiesuisse
DOSSIER POLITIQUE

7 / 2018

Non aux blocages de sites internet et au protectionnisme numérique

02.05.2018

L'essentiel en bref

Le 10 juin 2018, les citoyens suisses se prononceront sur la loi sur les jeux d'argent. Afin de protéger les casinos suisses, la loi prévoit – et il s'agit d'une nouveauté en Suisse – la possibilité de bloquer l'accès au réseau pour interdire l'utilisation de jeux d'argent proposés par des sociétés étrangères. À l'heure actuelle, il est déjà interdit de proposer de tels jeux en Suisse, mais jouer est autorisé.

Les blocages imposés par l'État visent à interdire à quiconque l'accès à certains sites internet. En principe, il incomberait aux fournisseurs d'accès de procéder à ces blocages.

Commencer à bloquer les jeux de hasard en ligne peut vite conduire à une extension de la censure à d'autres domaines. Une fois que les instruments requis existeront, d'autres groupes d'intérêt trouveront en effet rapidement des motifs de bloquer d'autres sites.

De tels blocages représentent un piège pour une économie ouverte et avancée telle que celle de la Suisse. Ils sont un instrument protectionniste qui peut être contourné en quelques clics même par des profanes. Ils causent simultanément des dommages importants à l'infrastructure réseau, au détriment de l'économie et de la société.

Position d'economiesuisse

La Suisse doit sa prospérité à son ouverture économique et aux libertés. À l'ère numérique, ces deux valeurs revêtent une importance décisive pour notre société et notre économie.

La disponibilité illimitée d'informations et la libre circulation des données jouent un rôle clé dans l'histoire récente. Aujourd'hui, internet représente la colonne vertébrale de l'économie et de la société numériques. C'est pourquoi le web ne doit

Contact et questions

Dominique Rochat
Responsable de projets Senior Énergie, infrastructures et environnement
Erich Herzog
Membre de la direction, responsable du département Concurrence et Réglementation
Christa Hofmann
Head Legal & Public Affairs

pas devenir le jouet de défenseurs d'intérêts en tout genre.

Les blocages d'accès constituent une tentative inappropriée et dangereuse d'étendre les limites des ingérences de l'État. Ils nuisent à notre société libérale, à l'État de droit et à l'économie (en ligne) suisses. Des exceptions ne doivent être tolérées que dans le but de préserver la sécurité publique (protection contre le terrorisme ou la pédopornographie, etc.)

L'introduction de blocages d'accès pourrait ouvrir une brèche dans le domaine de la censure d'internet. Cela donnerait un mauvais signal à d'autres domaines et aurait un effet désastreux sur la perception de la Suisse à l'étranger, en tant que place économique pour les entreprises technologiques tournées vers l'avenir.

Les blocages d'accès portent atteinte à l'infrastructure réseau et peuvent facilement être contournés. La situation deviendrait particulièrement délicate si les blocages devaient s'étendre dans le cadre de futures révisions législatives.

Internet est le moteur du progrès

→ **Internet est la colonne vertébrale de notre société moderne et notre quotidien ne serait plus imaginable sans le web.**

Internet est indispensable au quotidien

Aujourd'hui, nous vivons les prémisses de l'économie et de la société numérique. Les données et les informations constituent les nouvelles matières premières. Internet est l'une des principales technologies faisant avancer la numérisation. C'est devenu une colonne vertébrale de notre société moderne et notre quotidien ne serait plus imaginable sans le web.

Les technologies telles que les smartphones, les courriels, l'informatique en nuage pour n'en citer que quelques-unes ne fonctionnement pas sans internet. De la PME à la haute école en passant par le particulier, nous sommes tous de plus en plus tributaires d'un échange d'information libre et efficace.

Compte tenu de cette évolution et des nouvelles possibilités qui s'offrent, l'échange sans entraves de données revêt une importance sans cesse croissante tant d'un point de vue économique que sociétal.

→ **En tant que système nerveux du réseau, internet apporte une forte valeur ajoutée aux entreprises et à la société civile.**

Valeur ajoutée économique et culturelle

Le mouvement d'innovation déclenché par internet contribue non seulement à l'émergence de nouveaux secteurs économiques, mais engendre aussi un changement fondamental du mode de communication et de l'utilisation des médias dans les domaines professionnel et privé. L'impact culturel de cette interconnexion numérique est parfois comparé à l'invention de l'imprimerie. On constate aujourd'hui à juste titre qu'internet est devenu le système nerveux de la société et des entreprises et leur apporte une valeur inestimable.

→ **Les ingérences de l'État dans l'infrastructure réseau menacent le fonctionnement de l'économie et de la société.**

La dépendance est source vulnérabilité

La numérisation en cours engendre une dépendance grandissante à l'égard de l'infrastructure de communication et d'internet. En conséquence, la vulnérabilité de nombreux processus augmente. La portée de cette évolution est d'autant plus grande que cette dépendance va bien au-delà des processus de communication. C'est l'interconnexion croissante des humains et des appareils qui apporte une valeur ajoutée substantielle.

→ **Un libre accès à internet est le reflet de l'ouverture économique de la Suisse et constitue un facteur d'implantation décisif.**

À l'ère de l'information, l'ouverture attire les entreprises

Grâce à son climat d'ouverture, la Suisse dispose d'une base excellente pour profiter de cette révolution numérique. Preuve en sont les entreprises comme Google, IBM, Microsoft ou Oracle, qui ont choisi la Suisse pour implanter un site de développement important. La Suisse est en outre un coffre-fort de données attrayant et est très prisée par les entreprises qui misent sur la technologie blockchain.

L'un dans l'autre, la Suisse attire de nombreux investisseurs et entrepreneurs étrangers innovants en raison de son ouverture économique, de son infrastructure (réseau) performante et du libre accès à internet

L'ouverture influence la réflexion et l'action
L'ouverture économique est une pièce maîtresse du modèle auquel la Suisse doit son succès. Sa prospérité élevée et diversifiée serait impensable sans des marchés ouverts ou sans liberté d'entreprise. Cette ouverture a permis à notre pays de largement bénéficier de la mondialisation et des progrès technologiques de ces dernières décennies. Elle stimule également la concurrence, ce qui incite les entreprises à développer l'innovation et à s'adapter aux évolutions. La Suisse parvient ainsi souvent à surmonter des crises et des changements structurels mieux que d'autres pays. Ces bonnes dispositions incitent à penser qu'elle n'a pas à craindre la numérisation.

→ **Dans sa stratégie «Suisse numérique», le Conseil fédéral a lui aussi souligné l'importance de l'échange de données sans entraves.**

Le Conseil fédéral a également reconnu cette nécessité et avait déjà souligné dans la stratégie Suisse numérique 2016 que la Suisse devait

- s'établir comme un site international sûr pour stocker des données et fournir des prestations informatiques et disposer d'une politique des données qui tienne compte des intérêts nationaux également dans le domaine numérique;
- marquer de son empreinte la discussion sur l'avenir d'internet;
- saisir les opportunités offertes par l'espace économique virtuel international, notamment pour écarter le risque d'une marginalisation.

Par conséquent, il convient de ne pas sous-estimer l'importance de l'échange de données sans entraves pour la poursuite du développement économique et social de notre pays. Il s'agit de la clé de notre succès économique futur.

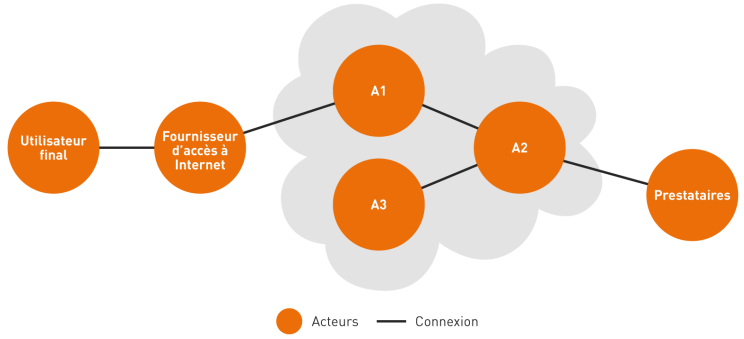
Mise en place et fonction des blocages d'accès

Fonctionnement d'internet

Internet est un réseau informatique mondial constitué d'un ensemble de réseaux d'ordinateurs autonomes et de terminaux permettant d'y accéder. Internet garantit la connexion entre ces réseaux et permet ainsi d'utiliser des services et des applications comme le web, les courriels, les applications et bien d'autres encore. En principe, chaque terminal peut se connecter à tous les autres terminaux. L'échange de données entre les terminaux connectés au réseau se fait via des protocoles internet normalisés.

Figure 1

Représentation simplifiée d'Internet avec trois acteurs principaux



Source: Thouvenin/Stiller/Hettich/Bocek/Reutimann: Keine Netzsperren im Urheberrecht, dans sic!, 2017, p. 704
www.economiesuisse.ch

→ **Étant donné sa construction sous forme de structure réseau, Internet est en principe stable.**

Construction fiable

Internet est conçu pour être un réseau fondamentalement fiable. Il y a toujours plusieurs voies menant au but recherché. En cas de défaillance de l'une de ces voies, il est possible d'en emprunter une autre. Les blocages de réseaux rendent cependant internet plus vulnérable et son utilisation moins sûre.

Internet, un réseau décentralisé

L'internet est constitué de plusieurs réseaux indépendants qui sont raccordés. Ce sont principalement les réseaux des fournisseurs d'accès internet, auxquels sont branchés les appareils des utilisateurs finaux.

Un grand nombre de liaisons internet importantes (dorsales) sont interconnectées au niveau de nœuds internet, par des connexions rapides et des appareils puissants (routeurs et commutateurs). L'échange d'informations relatives à l'accessibilité entre deux réseaux est organisé sous la forme d'un échange de trafic, autrement dit sur la base de la réciprocité. Cela permet d'échanger des données.

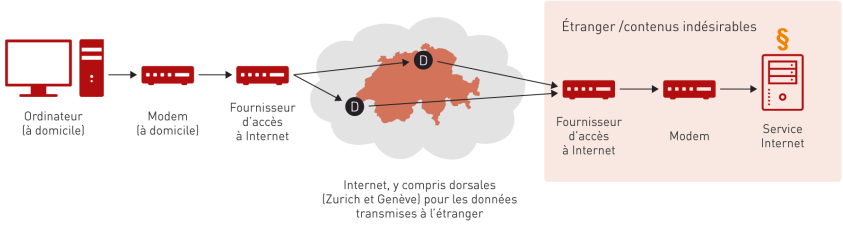
Le premier réseau d'internet, l'Arpanet, a été conçu comme un réseau décentralisé, dans une optique de fiabilité maximale. Ses créateurs n'ont pas prévu d'ordinateur central où convergent toutes les connexions. La structure en réseau d'internet contribue aujourd'hui encore à sa grande fiabilité. Pour la communication entre deux utilisateurs, il existe plusieurs chemins possibles via des routeurs avec des systèmes d'exploitation différents. En règle générale, la défaillance d'une connexion physique dans le noyau central d'internet ne se traduit pas par des conséquences dommageables.

Le protocole internet (IP) établit et utilise l'adressage unique des ordinateurs connectés à travers le monde. Afin de pouvoir atteindre un appareil final donné, le protocole internet l'identifie au moyen d'une adresse IP unique. Ces adresses fonctionnent un peu comme des numéros de téléphone et contiennent également un indicatif propre à chaque pays, qui permet le géociblage. Pour simplifier, on peut dire qu'une adresse IP peut être considérée comme l'identité d'un utilisateur final sur internet.

Le Domain name system (DNS) sert d'annuaire automatique et constitue un élément important de l'infrastructure internet. Cette banque de données internationale met à disposition un mécanisme qui traduit une adresse IP (86.125.22.1, par exemple) en un nom de domaine plus parlant (economiesuisse.ch, par exemple). Ces conversions sont réalisées sans que l'utilisateur s'en aperçoive chaque fois qu'il clique sur un nouveau lien dans un navigateur internet ou qu'il saisit directement l'adresse d'une page internet. Le navigateur commence par interroger un serveur DNS qu'il connaît sur l'adresse IP du lien inconnu au moyen d'un paquet. Ensuite, il échange des paquets avec l'adresse en question pour consulter les contenus des services proposés, des pages internet entre autres.

Figure 2

Circulation des données sur Internet



Source: Thomas Verasani, digital-liberal.ch
www.economiesuisse.ch

→ **Les blocages de réseaux visent à empêcher l'accès à certains sites internet. Il existe trois possibilités de bloquer des sites internet, avec des conséquences variables.**

Types de blocages de réseaux et fonctionnement

Les blocages de réseaux visent à empêcher les utilisateurs finaux d'accéder à certains sites internet et au contenu de ces derniers. Il s'agit principalement de contenus non souhaitables menaçant la paix publique. Il est ainsi possible d'utiliser les blocages de réseaux pour empêcher les utilisateurs finaux d'accéder à des offres clairement illégales comme la pornographie dure et les contenus terroristes ou extrémistes.

Chaque appareil connecté à internet dispose (au minimum) d'une adresse IP (86.125.22.1, par exemple). Étant donné que ces adresses ne sont pas faciles à lire et à retenir pour les humains, un nom de domaine (swico.ch, par exemple) est associé aux adresses IP purement numériques à l'aide du Domain name system (DNS). Ce nom de domaine est traduit de manière standardisée en adresses IP par les serveurs DNS des fournisseurs d'accès à internet (résolution de nom). Une adresse IP permet d'atteindre le site internet de divers prestataires proposant des contenus différents sous leur nom de domaine propre.

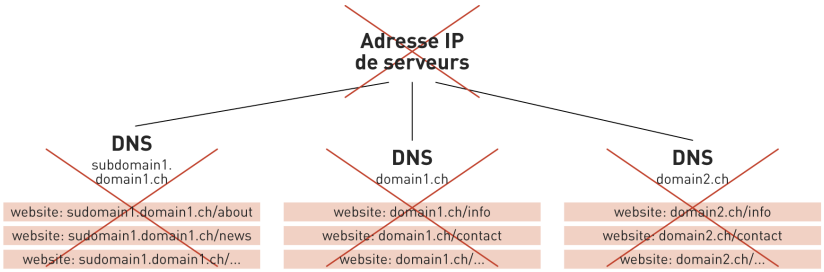
Trois options s'offrent actuellement pour le blocage de sites.

Option 1: Blocage d'une adresse IP

Pour le blocage d'adresses IP, les fournisseurs d'accès à internet filtrent les demandes de leurs clients sur la base des adresses IP figurant sur une liste de blocage. Soit ils bloquent ce site, soit ils redirigent les internautes vers un site les informant qu'ils ont tenté de consulter une adresse IP bloquée. Le blocage s'applique à l'ensemble des contenus – légaux ou illégaux – pouvant être consultés sur les adresses IP bloquées (cf. également le paragraphe sur les risques de surblocage).

Figure 3

Blocage d'adresses IP: bloquer des adresses d'ordinateurs



Source: Thouvenin/Stiller/Hettich/Bocek/Reutimann: Keine Netzsperren im Urheberrecht, dans sic!, 2017, p. 704
www.economiesuisse.ch

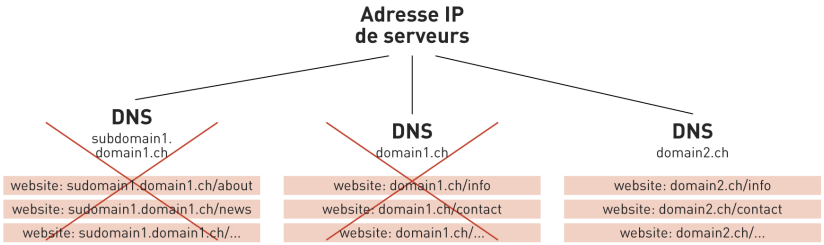
Option 2: Blocage DNS

Dans le cas d'un blocage DNS, soit la résolution de nom est empêchée par le serveur DNS, soit la demande est redirigée par le fournisseur d'accès vers une page internet informant le client qu'il a tenté de consulter un site internet bloqué. Le blocage DNS s'applique à l'ensemble des contenus consultables sur les domaines bloqués. Les

autres contenus consultables à la même adresse IP (mais sous un autre nom de domaine) ne sont en revanche pas touchés par le blocage.

Figure 4

Le blocage du DNS empêche la résolution d'adresses d'ordinateur



Source: Thouvenin/Stiller/Hettich/Bocek/Reutimann: Keine Netzsperren im Urheberrecht, dans sic! 2017, p. 704
www.economiesuisse.ch

→ **Les filtres d'application analysent les paquets de données en vue de définir leur finalité, ce qui leur permet d'empêcher certaines prestations (téléphonie IP, messagerie).**

Option 3: Filtre d'application

Avec les filtres d'application, les fournisseurs d'accès et les prestataires procèdent à un filtrage du trafic internet. De tels outils techniques, appelés filtres d'application, permettent notamment d'identifier dans les datagrammes IP transportés les contenus nuisibles d'un point de vue technique (vers, virus ou malware, par exemple). Une forme de filtrage peut être réalisée au moyen d'une Deep packet inspection (DPI). Cette dernière permet notamment de déclencher des actions après une analyse précise du contenu et de la finalité de paquets de données IP, ou sur la base de mots-clés. Un tel filtrage ne peut être utilisé que pour les données qui ne sont pas cryptées, mais inclut également les requêtes adressées aux moteurs de recherche.

Problèmes techniques

→ **Les blocages de réseaux menacent inutilement la sécurité.**

Des risques de sécurité supplémentaires

Les blocages de réseaux menacent la sécurité d'internet, car les fournisseurs d'accès seront obligés de falsifier des paquets de données. Ces interventions affaiblissent les technologies de détection des falsifications et des manipulations (criminelles) sur internet. En outre, les blocages de réseaux ne permettent plus non plus de constater si le fournisseur supposé se trouve effectivement derrière une offre. Si, du fait des blocages de réseaux, de plus en plus d'utilisateurs sont contraints de naviguer anonymement sur internet, la sécurité s'en trouvera menacée et la lutte contre la cybercriminalité deviendra plus difficile. Ces répercussions seraient malvenues à une époque où la cybercriminalité gagne du terrain.

Risques de surblocage

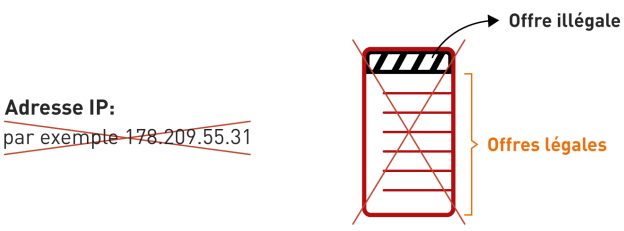
En raison de leur fonctionnement, les blocages de réseaux peuvent aussi bloquer l'accès à des contenus légitimes. C'est le risque de «surblocage». Celui-ci est particulièrement grand pour le blocage d'adresses IP, car une même adresse IP peut conférer un accès à des sites web de différents fournisseurs et de contenus variés. Pour le blocage DNS, les risques de surblocage sont moindres, mais il est encore plus facile à contourner que le blocage d'adresses IP.

Le surblocage a ceci de perfide qu'il soustrait des contenus légaux à la vue des internautes. En règle générale, les utilisateurs ne remarquent pas qu'une offre disparaît soudainement d'internet ou qu'elle n'est plus disponible.

Les blocages non intentionnels dus au surblocage peuvent être lourds de conséquences pour une entreprise. En créant l'amalgame entre des contenus parfaitement légaux et des contenus criminels, ils nuisent à l'image de l'entreprise, voire entraînent une perte de confiance préjudiciable aux affaires. Dans le cas extrême, le surblocage peut aller jusqu'à menacer l'existence d'une entreprise en rendant introuvable son magasin en ligne pour les clients (en Suisse).

Figure 5

Les blocages sont souvent excessifs et bloquent plus de pages que prévu



Source: economiesuisse
www.economiesuisse.ch

Conséquences du cryptage

De plus en plus d'entreprises choisissent de sécuriser leur site internet avec le protocole HTTPS. Le cryptage des connexions a aussi une incidence sur les blocages de réseaux. Il empêche les blocages au moyen de filtres d'application ou de serveurs proxy. Souvent, le cryptage empêche également de rediriger l'utilisateur vers une page d'information lui annonçant que la page téléchargée n'est plus disponible.

→ **Un énorme travail pour les fournisseurs internet et un désavantage pour les PME face à la concurrence.**

Désavantages pour les PME

Les blocages imposés par l'État représentent des interventions massives dans l'infrastructure réseau. Ils obligent en effet les fournisseurs internet à prendre des mesures à l'encontre de la logique et de la structure d'internet, soit à bloquer des sites web isolés sur un réseau décentralisé conçu pour ignorer ou contourner ce genre de perturbations. Les blocages de réseaux signifient donc un énorme travail pour les fournisseurs et désavantagent les plus petits d'entre eux sur un marché concurrentiel. En poussant des PME vers la sortie, les blocages de réseaux accroissent les risques de concentration du marché.

Possibilités de contournement

Chaque blocage de réseau peut être contourné

Le blocage d'adresses IP et le blocage DNS peuvent être contournés par des mesures techniques ou organisationnelles simples, parfois même sans que des tiers (autorités de poursuite pénale, par exemple) ne soient en mesure de détecter, de prouver ni même d'empêcher le contournement.

Contourner le blocage d'adresses IP

Il est possible de contourner le blocage d'adresses IP et le blocage DNS en se connectant à un réseau privé virtuel (VPN). L'utilisateur accède à l'adresse IP bloquée en passant par un serveur VPN situé à l'étranger, la résolution du nom étant effectuée par un serveur DNS qui n'est pas concerné par le blocage. Ces deux types de blocage peuvent aussi être contournés techniquement à l'aide d'outils et de systèmes d'anonymisation du trafic internet, comme Tor (cf. ci-dessous).

Contourner le blocage DNS

Il est possible de contourner le blocage DNS par exemple en interrogeant des serveurs DNS étrangers qui ne sont pas concernés par le blocage ou en exploitant son propre DNS local. Dans de nombreux cas, aucun serveur DNS n'est même nécessaire. Il suffit d'utiliser directement l'adresse IP du serveur web qui est divulguée par des forums ou des messages personnels. Depuis peu, il existe aussi un nouveau protocole, DoH (DNS over HTTPS). Développé pour protéger la sphère privée, il commence même à être intégré dans des navigateurs (Firefox, par exemple) et contourne automatiquement tous les blocages DNS.

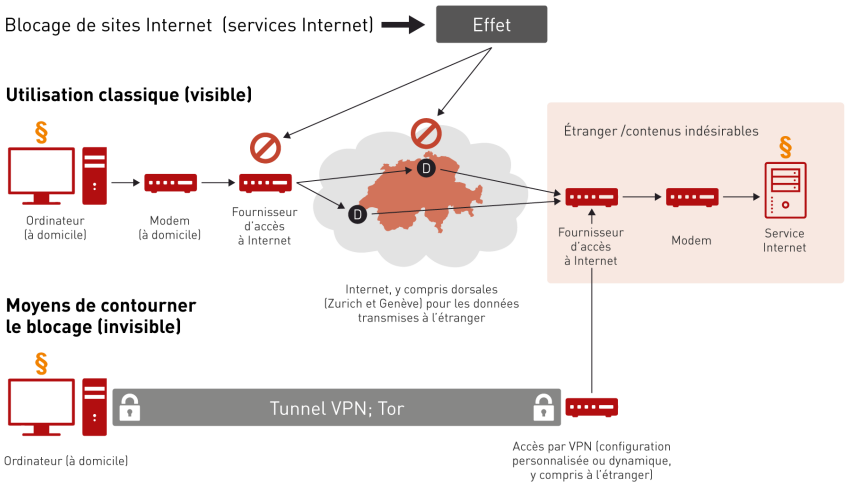
Contourner un filtre d'application ou un serveur proxy

Même les filtres d'application et les serveurs proxy sophistiqués peuvent être contournés. L'utilisateur peut ainsi recourir à une transmission cryptée, par exemple sous la forme d'un VPN. Une autre possibilité consiste à utiliser SSL/TLS (Secure socket layer/transport layer security) ou HTTPS (HTTP secure). L'utilisateur peut aussi établir son propre serveur proxy ou utiliser ceux qui sont proposés sur internet.

En définitive, il existe une pléthore d'outils et de systèmes pour anonymiser l'origine des connexions.

Figure 6

Effet du blocage de sites Internet et possibilités de le contourner



Source: Thomas Verasani, digital-liberal.ch
www.economiesuisse.ch

→ **Les blocages sont couramment contournés, même dans des pays ayant un gouvernement autocratique.**

Que se passe-t-il vraiment dans les pays autocratiques?
Certains pays vont très loin dans la censure d'internet. Ces pays touchent aussi à leurs limites avec le blocage de sites. L'Iran, par exemple, a bloqué toutes les pages dont le contenu ne cadre pas avec son idéologie religieuse, rigoureusement islamique, ou qui critiquent le gouvernement. Beaucoup d'Iraniens utilisent des VPN et autres moyens techniques pour regarder des films ou des chaînes de télévision occidentaux et lire des journaux internationaux. En Russie, l'État vient de bloquer Telegram, le service de messagerie le plus populaire là-bas, car il permet de crypter des messages et que les services secrets n'ont pas réussi à craquer les clés de cryptage. Les mesures de blocage prises par l'État russe à l'encontre de Telegram ont paralysé Google et Amazon, mais le service de messagerie fonctionnait toujours parfaitement. Cela montre que, même dans des États autocratiques qui sanctionnent régulièrement l'utilisation de VPN avec des amendes lourdes, il n'est pas possible de supprimer des contenus indésirables avec une précision chirurgicale.

Seuls des pays qui, à l'instar de la Corée du Nord, interdisent à leur population d'utiliser internet peuvent garantir un contrôle total. Le revers de la médaille est évident: l'économie numérique y est inexistante et la liberté personnelle des citoyens est fortement restreinte. Là aussi, l'individu trouve des solutions: une des réponses est un marché noir pour les clés USB et autres supports de données, par exemple.

VPN (réseau privé virtuel)
Un accès par VPN peut être installé avec des logiciels accessibles légalement en Suisse. Et il n'est pas nécessaire d'être un spécialiste pour cela. Il suffit de

télécharger l'application sur son appareil ou d'activer une extension pour un navigateur. Le VPN crypte ensuite la connexion internet depuis la carte réseau jusqu'au serveur VPN. On peut comparer ce système à un tunnel qui permet d'accéder, depuis son appareil personnel, à un lieu de confiance à l'étranger. Quand on navigue sur internet, c'est l'adresse de ce lieu de confiance qui est considérée comme l'origine des actions. De nombreux prestataires proposent des VPN, un service généralement payant. Il existe des vues d'ensemble des VPN recommandés actuellement, sous https://vpncreative.net/vpn-providers/, par exemple.

Tor (The onion routing)

Le réseau Tor permet à tous les utilisateurs finaux de surfer de manière anonyme sur internet. Tor utilise le principe du routage «en oignon» pour crypter les connexions et les données de transfert des internautes. Il permet de surfer sur internet de manière anonyme en toute sécurité. Pour utiliser Tor, l'internaute commence par télécharger un logiciel nommé Client et appelé un «proxy» dans le jargon. Ce logiciel établit une connexion avec le réseau Tor et indique tous les serveurs disponibles avec lesquels l'internaute peut se connecter. Les serveurs affichent une clé publique qui leur permet de dissimuler leur appartenance au réseau. Aussitôt que l'utilisateur reçoit la liste des serveurs sur son appareil, un itinéraire aléatoire se crée entre les serveurs Tor. À des fins d'anonymisation, le réseau n'utilise pas un serveur unique mais passe en règle générale par trois serveurs au minimum. Sur la page internet du projet Tor, on peut voir des détails ainsi qu'un lien pour télécharger le «proxy»: https://www.torproject.org/projects/torbrowser.html.en.

Préoccupations d'ordre juridique

→ **Le blocage de réseaux est une atteinte à nos droits qu'il ne faut pas sous-estimer et donc un instrument préoccupant dans un État de droit.**

Intervention étatique

Du point de vue juridique, le blocage de réseaux doit être considéré dans de nombreux cas comme une atteinte disproportionnée du fait de son caractère inadéquat et excessif. Dans l'évaluation de ces aspects, il faut considérer les points suivants:

- les possibilités techniques et, avec elles, les possibilités de contournement; - les effets indirects des blocages de réseaux sur les utilisateurs et les fournisseurs internet au lieu des contrevenants (exploitants de sites web);
- la menace potentielle sur des biens juridiques beaucoup plus importants (droits fondamentaux), voire leur violation;
- la sécurité juridique, qui ne peut guère être aménagée de manière parfaite sous l'angle des principes de l'État de droit (droit d'être entendu)

Certains experts [1] voient dans les blocages de réseaux une atteinte grave au droit fondamental à la libre communication. Par conséquent, les blocages de réseaux requièrent dans tous les cas une base légale. Toute restriction d'un droit fondamental doit en effet se fonder sur une base légale et cette dernière doit figurer dans la loi concernée (art. 36, al. 1, Cst.).

→ **Les blocages de réseaux peuvent porter atteinte aussi à différents droits fondamentaux.**

Atteinte aux droits fondamentaux

Du fait du risque de surblocage et de la licéité par exemple des jeux d'argent sur des plateformes étrangères, le blocage de réseaux doit pouvoir se justifier envers les personnes concernées qui, en tant que tierces personnes agissant dans leur bon droit, sont touchées par le blocage.

Selon les cas, la liberté d'information, la liberté économique ou, si le blocage de réseaux est en lien avec l'analyse de paquets de données, la liberté personnelle sont touchées à des degrés divers. Le droit à la protection de la sphère privée et au libre choix en matière d'information (art. 13 Cst.) est le premier touché.

Il convient également de mentionner diverses garanties de procédure, comme la garantie générale de procédure, qui inclut le droit d'être entendu (art. 29 Cst.), la garantie de l'accès au juge (art. 29a Cst.) ainsi que des standards minimaux d'une procédure judiciaire (art. 30 Cst.). L'utilisation de listes noires que les fournisseurs internet doivent respecter soulève la question du droit d'être entendu. La décision de blocage d'un réseau est souvent publiée dans la Feuille fédérale; elle n'est pas communiquée directement à toutes les personnes concernées. Les fournisseurs internet doivent donc eux-mêmes vérifier les listes des sites à bloquer. Si ces listes sont publiées sans entendre les exploitants de ces sites, on porte atteinte à leur droit d'être entendu. Il en va de même pour les titulaires de droits qui n'ont pas demandé eux-mêmes le prononcé d'une décision de blocage de réseau.

La compatibilité avec les accords commerciaux internationaux des blocages de réseaux en Suisse pour des offres légales à l'étranger n'a pas encore été clarifiée.

→ **Le blocage de réseaux est en particulier préoccupant quand ils cherchent à empêcher des comportements licites.**

Législation contradictoire

Les blocages de réseaux qui cherchent à empêcher des comportements licites posent un problème particulier. Si le comportement qu'un blocage de réseau vise à empêcher n'est pas punissable, l'instrument du blocage est alors contradictoire. Un comportement en soi licite ne peut être empêché. Le législateur ne peut pas simultanément maintenir la licéité (en droit) d'un comportement (jouer à des jeux d'argent étrangers sur internet, par exemple) et introduire une réglementation visant à empêcher (de fait) l'accès à de tels sites sur internet. Par analogie, on pourrait imaginer que l'État ne veuille pas interdire une route au trafic tout en s'employant activement à la couvrir de glace ou à y déverser des clous. Si le législateur ne veut pas s'exposer au reproche d'être contradictoire, il n'a que deux possibilités: soit s'en tenir à la situation juridique actuelle et renoncer à introduire les blocages de réseaux, soit introduire le blocage de réseaux et, pour être cohérent, interdire de jouer sur des plateformes étrangères de jeux d'argent. Une voie médiane entre ces deux positions est en soi contradictoire.

Collaborer volontairement, un instrument efficace

Il existe des domaines dans lesquels on ne peut pas laisser une liberté absolue sur internet et ce pour de bonnes raisons. C'est le cas quand il s'agit de lutter contre le terrorisme ou la pédopornographie. Ainsi, le Service national de coordination de la lutte contre la criminalité sur internet (SCOCI) collabore étroitement avec les fournisseurs d'accès internet. En 2007, le SCOCI et les principaux fournisseurs d'accès internet de Suisse ont conclu un accord sur le blocage de pages internet présentant des contenus interdits relevant de la pédopornographie. Le blocage vise exclusivement des pages internet étrangères qui proposent de télécharger des contenus pornographiques mettant en scène des enfants et interdits par l'art. 197, al. 4 et 5 CP. Les fournisseurs d'accès internet bloquent l'accès aux pages concernées sur la base de leurs conditions commerciales générales et de principes éthiques et aiguillent l'internaute vers une page d'avertissement. Le SCOCI a établi une liste répertoriant entre 700 et 1000 pages internet qu'il met à jour. Dans le cadre de ce projet, le SCOCI collabore étroitement avec Interpol. La liste établie en Suisse contribue largement à alimenter la liste «Worst-of» d'Interpol, qui répertorie les pages internet avec des contenus pédopornographiques. Le SCOCI cherche activement de nouvelles pages internet avec des contenus pédopornographiques et complète continuellement la liste d'Interpol, également mise à jour en collaboration avec plusieurs pays. On peut se demander si le fait d'ancrer cette collaboration dans la loi est utile. Du point de vue de l'État de droit, la liste devrait être soumise au contrôle d'une autorité ou d'un tribunal, car elle serait à l'origine d'une mesure étatique contraignante. Cela dit, il n'est pas dans l'intérêt de la collectivité que de telles listes deviennent accessibles au public.

Il faut renoncer aux blocages de réseaux

→ **Il faut renoncer au blocage de réseaux pour des raisons économiques, sociales, techniques et juridiques.**

De nombreux désavantages

Une analyse circonstanciée des blocages de réseaux des points de vue économique, social, technique et juridique montre qu'ils sont une tentative inadéquate et dangereuse d'étendre les limites de l'interventionnisme étatique. Les blocages de réseaux nuisent à notre société libre, à l'État de droit et à l'économie (d'internet) de la Suisse.

Autre fait choquant, les blocages de réseaux portent atteinte à l'infrastructure d'internet tout en étant faciles à contourner. Un surblocage de contenus web licites serait presque inévitable. Enfin, les blocages de réseaux qui limitent un comportement licite du citoyen sont contradictoires (comme dans le cas de la loi sur les jeux d'argent).

L'internet et la libre circulation des données constituent l'un des fondements de notre société et font pratiquement partie intégrante de notre quotidien. Ils ne doivent pas devenir le terrain de jeu de groupes d'intérêt, quels qu'ils soient, et doivent rester libres d'accès. Des experts renommés considèrent que l'introduction des blocages de réseaux dans le droit d'auteur est excessive et disproportionnée. Des exceptions ne sont admises que pour la protection de la sécurité publique (protection contre le terrorisme, la pédopornographie, etc.).

On le voit, l'introduction des blocages de réseaux n'est donc pas souhaitable, pour des raisons de principe fondamentales.

→ **Le blocage de réseaux dans la loi sur les jeux d'argent risque d'avoir un effet de domino.**

Loi sur les jeux d'argent: attention à l'effet de domino

Le 10 juin 2018, la population suisse se prononcera sur la nouvelle loi sur les jeux d'argent. Pour protéger les casinos en Suisse, la loi autorisera, et c'est nouveau, des blocages de sites internet pour empêcher l'accès aux offres de jeux d'argent en ligne basées à l'étranger. S'il est actuellement interdit d'offrir de tels jeux en Suisse, il est en revanche autorisé d'y jouer.

economiesuisse s'oppose à la loi sur les jeux d'argent en raison des blocages de réseaux qu'elle prévoit d'introduire. La Fédération des entreprises suisses redoute un dangereux précédent.
L'abandon du libre accès à internet risquerait d'ouvrir grand la porte à la censure. Car une fois que les instruments ad hoc existeront, d'autres groupes d'intérêt trouveront rapidement des prétextes pour demander d'autres blocages de réseaux. Le signal envoyé à d'autres branches et à l'étranger, où la Suisse est considérée comme une terre d'accueil des entreprises technologiques du futur, serait néfaste.

1. Florent Thouvenin, Burkhard Stiller, Peter Hettich, Thomas Bocek, Kento Reutimann dans sic!, 2017, pages 701 ss.