Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement,
des transports, de l'énergie et de la communication DETEC

Office fédéral de la communication OFCOM

28.8.2017

Révision de l'ordonnance sur les domaines Internet

Rapport explicatif

La révision de l'ordonnance sur les domaines Internet (ODI; RS 784.104.2) s'impose afin d'adapter le cadre réglementaire en matière de lutte contre la cybercriminalité et de tenir compte des expériences faites après un an et demi d'exploitation du «.swiss».

Art. 10, al. 1, let. j et k Tâches

Les registres du «.ch» et du «.swiss» sont tenus non seulement de fournir au public la liste des registraires (art. 18 al. 1 ODI), mais également un annuaire qui soit consultable en fonction des prestations recherchées (art. 10 al. 1 let. j in fine) et qui permette aux registraires de choisir les services liés aux noms de domaine qu'ils souhaitent associer à leur profil (let. k). Cette dernière prestation des registres s'est révélée superfétatoire et doit être abandonnée dans la mesure où elle ne correspond pas à un besoin des registraires, n'est pas exigée par les règles qui s'appliquent à l'échelon international et ne s'est pas du tout imposée dans les usages.

Art. 14, al. 4 Services de règlement des différends

Les décisions des services de règlement concernent les litiges relevant du droit civil survenant entre titulaires du droit d'utiliser un nom de domaine et titulaires de droits attachés à des signes distinctifs (cf. art. 14 al. 1 let. b). La solution apportée à ces litiges ne peut fréquemment se justifier et se comprendre que si le titulaire des droits attachés à un signe distinctif (tels que raison de commerce, nom, nom géographique protégé ou encore marque) et le titulaire du droit d'utiliser un nom de domaine sont clairement identifiés, dans la mesure où cette identité est souvent le facteur essentiel qui fonde la légitimité des droits concernés ou qui s'y oppose. Autrement dit, la publication des décisions des services de règlement peut être sans valeur en l'absence d'une identification claire des parties en présence. Il convient dans ces conditions de lever l'interdiction de principe de publier le nom et d'autres données personnelles des parties qui figure à l'art. 14 al. 4 ODI.

Art. 15 ss Mesures en cas de soupçon d'abus

Une lutte efficace contre les abus commis par le biais de noms de domaines suisses du «.ch» et du «.swiss» contribue à garantir la sécurité sur l'Internet et renforce la confiance des usagers dans les contenus et services en ligne accessibles dans ces domaines Internet. La lutte contre la cybercriminalité est dans ce contexte l'une des tâches essentielles d'un registre (art. 10 al. 1 let. i ODI). En particulier, les règles et processus prévus à l'art. 15 ODI constituent, depuis leur introduction en 2010, le

fondement de cette lutte menée contre certains actes particuliers de cybercriminalité (hameçonnage ou «phishing» et diffusion de logiciels malveillants [«malware»]) impliquant des sites ou des services web identifiés par des noms de domaine suisses. Ces règles et processus ont démontré leur efficacité et permettent aux domaines Internet suisses d'être parmi les plus sûrs au monde. Plus de 11'400 cas de logiciels malveillants et plus de 1'110 cas de hameçonnage au total ont été constatés et traités dans le domaine «.ch» depuis 2010 (Statistiques de SWITCH à fin décembre 2016, avec des données statistiques pour le «phishing» uniquement depuis 2014) et aucun cas d'abus répertorié jusqu'ici concernant le «.swiss» (ouvert depuis septembre 2015).

Sur la base des expériences faites, de l'évolution rapide des pratiques et des modes opératoires des cybercriminels ainsi que des réflexions en cours en matière de lutte contre la cybercriminalité au sein de l'organisme international en charge de la gestion globale du système des noms de domaine (à savoir l'Internet Corporation for Assigned Names and Numbers [ICANN]), il convient d'apporter à ce régime quelques modifications permettant d'étendre et d'optimiser la lutte contre la cybercriminalité ainsi que son efficacité.

Art. 15 Mesures en cas de soupçon d'abus: blocage

Seuls le hameçonnage («phishing») et la diffusion de logiciels malveillants («malware») sont couverts par l'art. 15 ODI lorsqu'ils impliquent l'utilisation de noms de domaine. Cette utilisation peut prendre de nombreuses formes ou techniques tout en recourant à de multiples moyens comme l'exploitation de réseaux de machines zombies («botnet»), l'envoi en masse de courriers électroniques (pourriels), l'usage des failles techniques d'un site web à l'insu de son exploitant, le clonage de sites web ou encore la manipulation du DNS permettant la redirection vers un site web falsifié ou cloné («pharming»). Les modes opératoires avec des noms de domaine pour opérer du hameçonnage ou diffuser des logiciels malveillants se développent, se multiplient et se diversifient rapidement et dans une large mesure. Il convient d'en tenir compte en complétant l'art. 15 al. 1 ODI par la mention selon laquelle un nom de domaine peut non seulement être utilisé pour diffuser mais aussi pour exploiter des logiciels malveillants (let. b); cela permet de cibler les noms de domaine pointant vers des sites web qui transmettent les instructions destinées aux «botnets» (serveurs de commande et de contrôle d'un «botnet» ou «Command & Control server» [serveurs C&C]), ce dispositif faisant souvent appel à des algorithmes de génération de noms de domaine («Domain Generation Algorithm» [DGA]) qui brouillent les pistes. Il convient en outre plus généralement d'introduire une nouvelle lettre c qui permet d'appliquer le régime de l'art. 15 ODI dans tous les cas où un nom de domaine sert en tant que point d'appui ou de manière indirecte («soutenir»), à des activités de «phishing» ou à la diffusion de «malware», afin d'appréhender l'évolution rapide et imprévisible des moyens, des techniques et des modes opératoires utilisés par les cybercriminels. Cette nouvelle lettre c couvre en particulier les cas dans lesquels les noms de domaine sont utilisés en tant que leurres, en lien avec des pratiques de «Social engineering» à des fins de «phishing», ou encore lorsque des noms de domaine sont générés par DGA ou identifient des serveurs configurés de manière à soutenir des actions malveillantes en particulier de diffusion de «malware».

En l'absence d'une demande émanant d'un service de lutte contre la cybercriminalité reconnu (al. 3), le registre peut bloquer techniquement et administrativement un nom de domaine durant 5 jours ouvrables si les conditions pour ce faire sont remplies (al. 1). A l'expiration de ce délai, le registre doit lever toute mesure de blocage qui n'est pas confirmée par une demande émanant d'un service reconnu (al.3) ou par une décision de l'Office fédéral de la police (fedpol) (al. 4). Le registre peut uniquement prolonger de son propre fait le blocage technique et/ou administratif de 5 jours effectué sur la base de l'al. 1 lorsque des raisons fondées permettent de supposer que le titulaire recourt manifestement à de fausses données d'identification ou usurpe l'identité d'un tiers et qu'il est urgent de prévenir la survenance d'un préjudice imminent et difficilement réparable (al. 2). A noter qu'une autorité suisse intervenant dans le cadre de l'exécution de ses tâches peut toujours demander le blocage d'un nom de domaine resp. sa prolongation sur la base de l'art. 30 al. 3 let. a ODI.

Avec la nouvelle version de l'art. 30 al. 3 let. a ODI, un service reconnu comme MELANI n'a plus comme seule possibilité de confirmer un blocage technique complet d'un nom de domaine, mais peut s'en tenir à demander le non rétablissement des serveurs de noms ayant été précédemment supprimés dans le fichier de zone administratif. Cette solution pragmatique peut s'appliquer dans les cas pour lesquels un doute subsiste dans l'intérêt de la sécurité publique (la connectivité à l'Internet et par conséquent la diffusion présumée de «malware» restent suspendues), tout en permettant à ceux dont les noms de domaine auraient été trop rapidement considérés comme laissés à l'abandon de rétablir leur connectivité.

Art. 15*a* Mesures en cas de soupçon d'abus: redirection du trafic

Il convient de compléter le régime actuel de lutte contre la cybercriminalité prévu à l'art. 15 ODI par la possibilité de rediriger le trafic destiné à des noms de domaine servant à du «phishing» ou à la diffusion de «malware» à des fins d'analyse de ce trafic («domain name traffic sinkholing »). Une telle mesure améliore sensiblement la lutte contre ce type de cybercriminalité puisqu'elle permet de déterminer les servers/ordinateurs infectés et d'informer ceux qui en sont les victimes, d'analyser le fonctionnement de ces activités afin de développer les techniques de lutte en recueillant des indices permettant d'en savoir plus sur la menace de manière à pouvoir contrer d'éventuelles futures actions). Cette mesure, qui est préconisée par l'ICANN en matière de lutte contre la cybercriminalité, est facile à mettre en œuvre par le registre dans la mesure où celui-ci peut remplacer les serveurs de noms liés à un nom de domaine dans le fichier de zone par des nouveaux qui permettent de rediriger le trafic (cf. ég. art. 30 al. 3 let. b ODI et explications ad art. 30 y relatives). Lamesure doit cependant être encadrée du fait qu'elle implique le traitement d'informations ou correspondances transmises par télécommunications qui sont originairement destinées à des tiers. L'art. 15*a* fixe ainsi les conditions auxquelles une mesure de «Sinkholing» est autorisée, à savoir:

- Seuls les noms de domaine faisant l'objet d'un blocage technique et administratif au sens de l'art. 15 ODI peuvent faire l'objet d'une redirection du trafic qui est destiné à ces noms de domaine ou qui transite par leur intermédiaire (let. a):

- L'analyse du trafic a pour seul et unique but d'identifier et d'informer les victimes de «phishing» ou de «malware», ainsi qu'à analyser le fonctionnement de ces activités afin de développer les techniques visant à identifier, combattre, limiter ou poursuivre ces activités le trafic collecté et analysé qui ne concerne pas ces buts doit être immédiatement et définitivement supprimé (let. b);

- Seul un service de lutte contre la cybercriminalité reconnu pour 30 jours au maximum et fedpol peuvent requérir du registre que celui-ci procède à la redirection du trafic à des fins d'analyse (let. c; cf. art. 30 al. 3 let. g ODI en ce qui concerne les autorités intervenant dans le cadre de l'exécution de leurs tâches. Le traitement des informations redirigées est opéré a priori par le service reconnu ou l'autorité intervenante. Rien n'empêche toutefois ces derniers de confier la tâche d'analyse soit au registre soit à des tiers qui sont reconnus pour leurs compétences et leur savoir-faire en la matière ("Security Research partner", organe d'analyse forensique ou autre registraire de quarantaine ["quarantine registrar"]). Celui qui requiert la redirection du trafic à des fins d'analyse reste toutefois responsable du traitement des informations recueillies et doit veiller à ce que lui et son éventuel mandataire respectent les conditions mises à ce traitement par l'art. 15*a*;

- Les informations pertinentes recueillies et les analyses produites qui servent à la lutte contre la cybercriminalité peuvent être partagées conformément à l'art. 16 al. 1, 2 et 4 ODI avec les autorités publiques, services spécialisés de la Confédération et les autres tiers qui prêtent leur concours à l'identification et à l'évaluation des menaces, abus et dangers.

Art. 15*b* Mesures en cas de soupçon d'abus: information et demande d'identification

Le titulaire du nom de domaine concerné par un blocage ou une redirection du trafic doit être informé immédiatement d'une telle mesure (al. 1). L'information peut cependant être différée si cela est indispensable pour protéger des intérêts publics ou privés prépondérants (al. 3), en particulier si cette information aurait pour seule conséquence de prévenir l'auteur présumé du «phishing» ou de la diffusion de «malware» qu'il fait l'objet d'une mesure visant à prévenir ou à combattre ses actions frauduleuses.

Toute mesure au sens des art. 15 et 15*a* est en outre généralement complétée par une demande d'identification et/ou d'établissement d'une adresse de correspondance en Suisse (al. 2).

Art. 15*c* Mesures en cas de soupçon d'abus: décision et révocation

Les demandes d'adresse de correspondance («Rechtsdomizil») et d'identification au sens de l'art. 15*b* al. 2 ODI jouent un rôle essentiel dans la lutte contre la cybercriminalité. Elles complètent les mesures par nature provisoires de blocage prises sur la base de l'art. 15 ODI en offrant un processus simple et efficace permettant de révoquer – de manière définitive – les noms de domaine qui servent à des actes illicites. Ces noms sont en effet généralement acquis sous une fausse identité par des titulaires qui souhaitent conserver leur anonymat protecteur et qui ne répondent donc en principe jamais à des demandes d'identification.

A noter que rien n'empêche le registre de lancer, en dehors de toute procédure au sens des art. 15 ss ODI, des demandes d'identification des titulaires sur la base de l'art. 29 al. 1 ODI et de révoquer, conformément à l'art. 30 al. 2 let. c ODI, les noms de domaine pour lesquels les titulaires concernés ne se sont pas exécutés dans un délai de 30 jours ou se sont manifestement identifiés de manière incorrecte.

fedpol rend une décision sur le blocage et/ou sur la redirection du trafic si, dans les 30 jours suivant la communication immédiate ou différée au titulaire de la mesure par le registre, ce dernier demande une telle décision, s'identifie correctement et indique une adresse de correspondance valable en Suisse lorsqu'il est établi à l'étranger (al. 1).

Art. 15*d* Mesures en cas de soupçon d'abus: noms de domaine non attribués

En parallèle à l'art. 15*a* ODI, l'art. 15*d* ODI permet au registre, de son propre fait ou sur demande d'un service de lutte contre la cybercriminalité reconnu par l'OFCOM, de prendre certaines mesures à l'encontre de noms de domaine qui ne sont pas attribués mais dont l'attribution pourrait être requise par les cybercriminels. Cela concerne en particulier les réseaux de machines zombies («botnet») ou autres systèmes exerçant des activités malveillantes qui recourent à des algorithmes de génération de noms de domaine (DGA). Les noms de domaine ainsi générés, qui correspondent à des dénominations plus ou moins aléatoires en fonction de paramètres divers, servent directement ou en tant que relais pour piloter un « botnet» afin d'opérer des activités illégales ou simplement en tant que leurres pour rendre tout traçage difficile. Dans le cadre d'expertises technico-légales des ordinateurs infectés, il est possible grâce à des techniques de «reverse-engineering» de reconstituer les algorithmes DGA et par conséquent de dresser la liste des noms de domaine qui pourraient être utilisés par des «botnets». Le registre a dans un tel cas la faculté de s'attribuer ou d'attribuer ces noms à un tiers qui prête son concours à la lutte contre la cybercriminalité comme un registraire de quarantaine ("quarantine registrar") (let. a), et en dernier lieu de rediriger à des fins d'analyse le trafic destiné au nom de domaine ou transitant par un nom de domaine dans le but d'identifier, de corriger ou d'atténuer des attaques ou menaces cybercriminelles (let.b; «Sinkholing»). Le registre peut par ailleurs interdire l'attribution de ces noms de domaine sur la base de l'art. 25 al. 2 let. c ODI.

Au-delà de l'exigence générale d'un indice fondé qui laisse supposer qu'un nom de domaine pourrait faire l'objet d'une demande d'attribution ou d'une utilisation à une fin ou d'une manière illicite, l'art. 15*d* ODI ne prévoit pas contrairement à l'art. 15*a* ODI de conditions particulières qui sous-tendraient la prise de mesures. Cela se justifie du fait que les mesures pouvant être prises par le registre sur la base de l'art. 15*d* ODI concernent des noms de domaine qui n'ont jamais été attribués et pour lesquels aucun titulaire ne peut faire valoir un quelconque droit d'utilisation ou à une quelconque protection.

Art. 15*e* Mesures en cas de soupçon d'abus: documentation et rapports

Les rapports livrés à l'OFCOM sur les blocages devront dans le futur aussi porter sur les mesures de redirection à des fins d'analyse («domain name traffic sinkholing»). Par ailleurs, les rapports sont en pratique délivrés non pas chaque trimestre (qui reste dans tous les cas la périodicité minimale à respecter), mais sur une base mensuelle et annuelle; il convient d'adapter à cet égard l'art. 15*e* («périodiquement» en lieu et place de «chaque trimestre»).

Art. 16 Assistance administrative et coopération

Dans l'univers global de l'Internet qui fonctionne généralement de manière relativement informelle, il est essentiel que le registre puisse collaborer de manière diligente non seulement avec les autorités publiques mais aussi avec les tiers luttant contre les menaces qui touchent le domaine dont il a la charge, et traiter des informations personnelles à ce sujet. Dans ce contexte, il y a lieu d'amender l'art. 16 ODI afin de permettre au registre de donner au besoin un accès aux services spécialisés de la Confédération comme MELANI, par procédure d'appel ou par transfert en bloc de données, aux bases de données relatives à la gestion du domaine concerné (fichier de zone notamment [cf. art. 10 al. 1 let. a chif. 2 ODI]) (al. 2) ou, par procédure d'appel , à tout autre personne reconnue pour son activité dans le domaine de la lutte contre la cybercriminalité comme les services au sens de l'art. 15 al. 1 let. b ODI (al. 1). Une communication particulière de données par tout autre moyen de communication (e-mail notamment) reste par ailleurs bien entendu toujours possible.

A des fins d'efficacité et de praticabilité, il convient par ailleurs de simplifier le processus de requête d'une adresse de correspondance en Suisse ("Rechtsdomizil" qui permet la notification par les autorités suisses compétentes de communications officielles et autres décisions administratives ou judiciaires en particulier à des titulaires domiciliés à l'étranger) en supprimant l'étape du registraire (al. 3 en relation avec l'art. 23 al. 3 ODI qui est supprimé). Le fait de permettre au registre d'agir immédiatement permet de gagner un temps précieux dans la notification et la mise en œuvre par les autorités suisses de leurs communications, décisions et autres mesures de lutte contre la cybercriminalité. La suppression de l'intervention des registraires se justifie d'autant plus que ceux-ci mettent avant tout l'accent sur les aspects commerciaux dans leurs relations avec leurs clients titulaires de noms de domaine et négligent quelque peu pour certains les processus de lutte contre les abus. Sans compter que les registraires étrangers sont souvent peu au fait des procédures suisses prévues par l'ODI.

Art. 21 al. 3 Devoir d'information

Seuls les registraires ayant conclu un contrat de registraire au sens de l'art. 17 al. 1 let. b et 2 ODI accèdent au système d'enregistrement électronique du registre. Ce sont donc uniquement les registraires qui peuvent formellement requérir l'attribution de noms de domaine pour le compte de requérants ou gérer administrativement les noms de domaine attribués pour le compte de leurs titulaires. Il n'en demeure pas moins qu'un registraire peut recourir à des revendeurs et autres intermédiaires qui démarchent commercialement les clients intéressés par l'acquisition de noms de domaine. Les registraires ne sont de ce fait pas toujours en contact direct avec les requérants ou titulaires de noms de domaine. Ils n'en demeurent pas moins tenus et responsables de transmettre - ou de faire transmettre

comme le spécifie désormais expressément l'art. 21 al. 3 ODI - aux titulaires ou aux requérants dans les meilleurs délais les informations émanant du registre pour ces derniers.

L'al. 3 précise en sus les exigences liées à l'information concernant un refus par le registre d'attribuer un nom de domaine, information qui doit être transmise immédiatement par le registraire concerné au requérant débouté mais au plus tard dans les 3 jours qui suivent la communication de ce refus par le registre au registraire en principe par l'intermédiaire du système d'enregistrement (voire exceptionnellement par un autre moyen [cf. art. 27 al. 3 in fine ODI]). Il est en effet essentiel pour un requérant d'avoir connaissance dans les plus brefs délais de la communication d'un refus d'attribuer par le registre puisque c'est à partir de cette communication que court, conformément à l'art. 27 al. 4 ODI, le délai pour demander une décision formelle au sens de l'art. 5 de la loi fédérale sur la procédure administrative (PA; RS 172.021) (cf. ég. explications ad art. 27 al. 4). Compte tenu de l'importance pour les requérants de pouvoir prendre connaissance à temps d'un refus, une violation systématique ou répétée de son obligation d'information par un registraire pourrait conduire à la résiliation du contrat l'autorisant à exercer son activité (cf. art. 17 al. 7 ODI).

Art. 23 al. 3 Obligation de collaborer

A des fins d'efficacité et de praticabilité, il convient de simplifier le processus de requête d'une adresse de correspondance en Suisse ("Rechtsdomizil") en supprimant l'étape du registraire (suppression de l'al. 3 ODI en relation avec la modification de l'art. 16 al. 3; cf. à ce sujet les explications ad art. 16 al. 3).

Art. 25 al. 3 Conditions générales d'attribution

Sous le régime actuel, le registre doit refuser l'attribution d'un nom de domaine lorsque la dénomination choisie est contraire à l'ordre public, aux bonnes mœurs ou au droit en vigueur, ou lorsque des motifs techniques l'exigent (art. 25 al. 2 ODI), et peut refuser l'attribution lorsque le requérant se trouve en état de faillite, en liquidation ou dans une procédure concordataire (al. 3). Au regard des expériences faites et des abus constatés en particulier par le SECO dans le commerce électronique, les possibilités de refuser une attribution se révèlent par trop limitées. Certains acteurs de mauvaise foi n'hésitent en effet pas à demander la réattribution des noms de domaine qui se trouvent dans le délai de quarantaine de l'art. 31 al. 3 ODI à la suite notamment d'une révocation pour violation de dispositions légales comme celles sur l'indication des prix.

Dans ce contexte, il convient de prévoir que l'attribution de noms de domaine doit être refusée lorsque des raisons fondées permettent de supposer que le requérant utilisera le nom de domaine qu'il demande à une fin ou d'une manière illicite (al. 2 let. c). Un tel refus doit toutefois être considéré à la lumière du fait qu'un registre n'est qu'un intermédiaire «technico-administratif» qui a pour seul rôle de mettre à disposition des usagers une ressource - les noms de domaine - en tant que moyen permettant d'utiliser de l'Internet et que cet intermédiaire n'a ni pour rôle ni pour compétence de juger la licéité de l'utilisation qui est faite des noms de domaine attribués (cf. art. 10 al. 2 ODI). L'obligation du registre de refuser l'attribution ne ne s'impose dès lors que si ce dernier reçoit à temps des indications circonstanciées provenant d'une autorité agissant a priori dans son domaine de compétence concernant un nom de domaine déterminé qui devrait être demandé par un acteur agissant de manière ou à des fins illicites.

Un refus doit par ailleurs être prévu pour les cas où un requérant demande l'attribution d'un même nom de domaine ayant été révoqué conformément à l'art. 16 al. 3 ou à l'art. 15c al. 2 ODI, sans indiquer une adresse de correspondance valable en Suisse (let. d).

Art. 27 al. 4 Processus d'attribution

Le traitement d'une demande d'enregistrement d'un nom de domaine par le registre s'effectue a priori uniquement par l'intermédiaire du système d'enregistrement électronique mis à disposition des registraires (art. 10 al. 1 let. b, 24 al. 1 et 2 et 27 al. 1 à 3 ODI), ces derniers agissant en tant qu'intermédiaire exclusif entre le registre et le requérant (art. 24 al. 1 et let. m Annexe CDI). Le complément apporté à l'art. 27 al. 4 (« … communication de ce refus par le registre au registraire opérant pour le compte du requérant concerné par le registre au registraire concerné …») ainsi que les corrections rédactionnelles de la version allemande visent à ne laisser aucun doute quant au fait que tout refus d'une attribution est uniquement communiqué par l'intermédiaire du système d'enregistrement voire exceptionnellement par d'autres moyens conformément à l'al. 3, et que c'est à partir de cette communication en principe sous forme électronique du registre au registraire agissant pour le compte du requérant que le délai durant lequel ce dernier peut demander une décision formelle commence à courir. A noter que la réception de la communication électronique du refus intervient de manière immédiate et sans contestation possible chez le registraire concerné au travers du système électronique d'enregistrement.

Le délai de 30 jours durant lequel le requérant concerné par le refus d'attribution peut demander auprès de l'OFCOM une décision formelle au sens de l'art. 5 PA correspond au délai ordinaire de contestation, d'opposition ou de recours dans les processus administratifs. Ce délai doit être étendu à 40 jours afin de tenir compte du fait qu'il commence effectivement à courir dès la communication électronique de refus par le registre au registraire, quand bien même le requérant n'aurait pas encore reçu cette information de la part de son registraire (même si cette information doit lui être transmise immédiatement, mais au plus tard dans les 3 jours qui suivent la communication du refus par l'intermédiaire du système d'enregistrement [cf. explications ad art. 21 al. 3 ODI]). Autrement dit, le fait de prolonger à 40 jours le délai pour demander une décision formelle permet de tenir compte du fait que la connaissance dont le requérant a d'un refus d'attribution dépend principalement de la diligence de son registraire dans un régime d'attribution qui fonctionne par l'intermédiaire exclusif de registraires et d'un système électronique d'enregistrement.

Art. 30, al. 3 Révocation

Les mesures provisionnelles sont essentielles pour le système des noms de domaine (DNS), puisqu'une bonne mise en œuvre des règles concernant les noms de domaine et la lutte contre la cybercriminalité dépend essentiellement de la vitesse à laquelle une irrégularité ou une menace est désamorcée. Au regard de leur importance, les mesures préliminaires prévues à l'art. 30 al. 3 ODI doivent être quelque peu adaptées et complétées:

- Le fait d'ordonner des mesures préliminaires incombe au premier chef aux tribunaux étatiques ou arbitraux, aux autorités publiques et autres services de règlement des litiges qui ont la compétence d'ordonner la révocation d'un nom de domaine conformément à l'al. 2 et il convient d'adapter dans ce sens la formulation de l'al. 3. Le registre exécute les mesures requises par ces organismes lorsque cette requête relève a priori de leurs domaines de compétence légale, quand bien même aucune décision n'aurait encore été formellement rendue. Les mesures préliminaires de l'al. 3 sont toutefois par nature provisionnelles et doivent dès lors être logiquement suivies, resp. confirmées par des décisions d'experts ou d'autorités sur la base de l'art. 5 PA, des décisions arbitrales et autres ordonnances, arrêts ou jugements de tribunaux.

- Bien qu'il constitue avant tout un acteur «technico-administratif» qui n'a pas à juger de la licéité de l'utilisation qui est faite des noms de domaine attribués (cf. art. 10 al. 2 ODI), le registre doit tout de même se voir reconnaitre la compétence de prendre des mesures préliminaires au sens de l'al. 3 dans deux cas particuliers, à savoir (al. 4):
    - lorsque cela s'avère nécessaire afin de protéger l'intégrité ou la stabilité du système des noms de domaine (DNS) et s'il est urgent de prévenir la survenance d'un préjudice imminent et difficilement réparable (let. a). Le fait de prendre les mesures

propres à assurer la fiabilité, la résilience, l'accessibilité, la disponibilité et la sécurité de l'infrastructure ainsi que des prestations nécessaires à la gestion du DNS constitue l'une des tâches essentielles d'un registre (cf. art. 10 al. 1 let. g ODI);
    - durant 5 jours ouvrables au maximum lorsque le registre a des raisons fondées de supposer que le titulaire utilise des noms de domaine à une fin ou d'une manière illicite et s'il est urgent de prévenir la survenance d'un préjudice imminent et difficilement réparable (let. b). Cette règle reprend le régime de l'art. 24h de l'ordonnance sur les ressources d'adressage dans le domaine des télécommunications (ORAT; RS 784.104) qui permet le blocage provisoire par les fournisseurs de services de télécommunication de l'accès aux numéros attribués individuellement, en étendant à 5 jours ouvrables la période de blocage en cohérence avec l'art. 15 al. 1 ODI.

- Le catalogue des mesures préliminaires à l'al. 3 doit être précisé et complété, ce qui permet de lever tout incertitude quant aux mesures qui peuvent effectivement être prises et de considérer la pratique qui se développe à l'échelon international (cf. en particulier ICANN, Framework for Registry Operator to Respond to Security Threats):
    - La let. a autorise le registre à agir de toutes les manières au niveau des serveurs de noms liés à un nom de domaine particulier («Domain Name Server») qui permettent d'associer ce nom à une adresse IP sur l'Internet (résolution) et d'assurer ainsi la connectivité sur l'Internet. Un registre peut dès lors à titre provisoire supprimer les serveurs de noms liés à un nom de domaine dans le fichier de zone et bloquer ainsi la connectivité du nom de domaine concerné, remplacer les serveurs de noms utilisés par des nouveaux qui permettent de rediriger le trafic (cf. let. g) ou renoncer à rétablir les serveurs ayant été précédemment supprimés du fichier de zone, à charge pour les titulaires de noms de les rétablir eux-mêmes (cf. à ce sujet aussi les explications ad art. 15 ODI);
    - La let. b permet désormais, au titre du blocage administratif, d'interdire non seulement la réattribution d'un nom de domaine possédé par un titulaire, mais aussi l'attribution d'un nom de domaine a priori libre; il s'agit de bloquer les noms de domaine qui sont créés automatiquement – et donc déterminables de manière anticipée - par les algorithmes de génération de noms de domaine («Domain Generation Algorithm» [DGA]) (cf. explications ad art. 15 et 15*a* ODI);
    - La let. c permet de requérir du registre qu'il transfère la gestion administrative d'un nom de domaine à un nouveau registraire (cf. let. t Annexe ODI), ce qui permet de contrer les agissements d'un registraire de mauvaise foi qui participerait, faciliterait ou couvrirait les activités illicites de ses clients titulaires de noms de domaine;
    - Les let. d et e autorisent toute modification, correction ou suppression des informations ou paramètres techniques ou administratifs qui concernent la gestion d'un nom de domaine (contact technique [Tech-C], contact administratif [Admin-C], etc.), ou qui figurent dans la banque de données WHOIS (cf. art. 46, 52 et let. k Annexe ODI);
    - La let. f permet au registre de s'attribuer un nom de domaine ou de l'attribuer à la personne désignée par l'instance compétence qui ordonne cette mesure;
    - Au-delà des processus et des compétences prévues par les art. 15 ss ODI, le «sinkholing» constitue aussi une mesure provisionnelle qui doit être prise par le registre sur requête d'une autorité qui l'ordonne conformément à ses compétences légales (let. g; cf. à ce sujet explications ad art. 15*a* et 15*d* ODI).

A noter finalement que la terminologie de l'al. 3 a été adaptée dans la version allemande afin de la faire coïncider avec la terminologie utilisée dans d'autres actes législatifs («sperren» au lieu de «blockieren»).

Art. 46, al. 1, let. b à f Données mises à la disposition du public

Conformément à l'art. 46 al. 1 let. e ODI, la langue déterminante lors d'éventuelles procédures de règlement des différends au sens de l'art. 14 ODI doit être publiée dans la banque de données pu-

blique WHOIS (let. k Annexe ODI). Cette publication implique des modifications importantes du système informatique WHOIS et un gros effort administratif pour collecter cette information pour l'ensemble des quelques 2 millions de noms de domaine du «.ch» qui ont été attribués jusqu'ici. Cet effort apparaît disproportionné dans la mesure où le fait de connaître la langue déterminante d'un litige n'est nécessaire que dans les quelques cas de figure qui se présentent chaque année et que l'information peut être simplement fournie sur requête par le registre pour chaque litige, sans que cela n'ait une quelconque conséquence sur la procédure de résolution.

Il convient par ailleurs d'abroger la let. d qui exige la publication du nom d'une personne physique autorisée à représenter la personne morale concernée. Cette information n'est pas comprise des personnes morales ou de leur registraires qui indiquent souvent en lieu et place des services internes permanents («Domain Name Administrator», «Service informatique», «Hostmaster» ou encore «Service clients»). L'indication d'une seule personne physique n'apporte du reste en définitive pas de véritable clarté quant à la représentation juridique d'une personne morale qui nécessite souvent l'accord de deux personnes et qui est sujette à des changements fréquents figurant avant tout au registre du commerce.

Finalement, les let. b et c (indications relatives aux titulaires) ainsi que f (indications relatives aux responsables techniques) peuvent être simplifiés à l'exemple de ce qui se fait pour le «.swiss» (art. 52 al. 1 ODI); ce qui permet en particulier de supprimer l'indication superflue de l'Etat ou de la province. Il convient en revanche de compléter les indications qui doivent figurer au WHOIS avec les données des serveurs de noms qui sont assignés à un nom de domaine dans le cas où celui-ci est activé (nouvelle let. c). Il s'agit par la même occasion de préciser la formulation qui figure à l'art. 52 al. 1 let. f ODI pour le «.swiss» («dans le cas où le nom de domaine concerné est activé») dans la mesure où un nom de domaine peut être attribué sans qu'il y ait obligatoirement des serveurs de noms qui lui soient assignés (en pratique, 2 serveurs de noms sont requis par nom de domaine activé).

Art. 52, al. 1, let. e Données mises à la disposition du public

Sous réserve de l'exception concernant les noms de domaine attribués sous mandat de nommage (art. 56 al. 7 ODI), un nom de domaine du «.swiss» ne doit pas obligatoirement être activé, c'est-à-dire se voir assigner des serveurs de noms qui permettent la connectivité sur l'Internet. C'est uniquement en cas d'activation que les – au minimum – deux serveurs de noms assignés à un nom de domaine particulier doivent être indiqués dans la banque de données WHOIS (al. 1 let. e).

Art. 54 Attribution privilégiée

L'art. 54 ODI règle la phase d'attribution privilégiée de noms de domaine du «.swiss» («sunrise period»), phase qui a précédé l'ouverture générale ou domaine «.swiss» en date du 11 janvier 2016. Dans la mesure où le domaine «.swiss» se trouve désormais et va rester dans sa phase d'exploitation ordinaire, les règles spécifiques de l'art. 54 ODI sont caduques, n'ont plus aucune raison d'être et doivent en conséquence être abrogées.

Art. 55 Eligibilité

L'actuel article 55 ODI permet l'ouverture échelonnée de l'éligibilité à l'attribution d'un nom de domaine du «.swiss» en fonction de différentes catégories ou classes de personnes éligibles, en donnant au DETEC la compétence d'en fixer la planification. Le Département s'est acquitté de sa tâche dans son ordonnance du 11 août 2015 sur le domaine Internet «.swiss» (RS 784.104.253) qui exclut, jusqu'au 31 décembre 2017, l'éligibilité des personnes physiques ayant leur domicile en Suisse ou possédant la nationalité suisse.

L'ouverture de l'éligibilité aux personnes physiques n'est toutefois pour l'heure ni souhaitée ni souhaitable. Comme l'a souligné le Conseil fédéral à de nombreuses reprises, la gestion du «.swiss» par la

Confédération vise avant tout à défendre les intérêts de la Suisse en mettant ce nouveau domaine Internet à disposition de l'économie, de la culture et des institutions du pays. Le domaine «.swiss» s'est ainsi jusqu'ici positionné en tant que vitrine Internet des entreprises et des institutions suisses, qui bénéficient de la sorte d'une indication de provenance claire sur l'Internet. Ce positionnement est fondé sur des enquêtes préalables auprès des milieux concernés, a été appuyé par des campagnes de marketing et s'est imposé dans les milieux économiques ainsi que dans l'esprit de la population suisse. Le «.swiss» est désormais largement perçu comme un complément au très populaire «.ch». Si toute personne physique peut requérir l'attribution d'un nom domaine du «.ch», seules celles qui sont inscrites en tant qu'entreprises individuelles au registre du commerce peuvent le faire dans le «.swiss» (let. b). Dans un tel contexte, l'ouverture du «.swiss» aux personnes physiques non inscrites au RC ne peut, en l'état et pour l'heure, guère se justifier. Une telle ouverture devrait au contraire porter atteinte à l'image du «.swiss» tant au niveau national qu'international et à son positionnement actuel. Elle devrait buter sur l'incompréhension des entreprises suisses qui ont investi dans le «.swiss», compte tenu des attentes légitimes que ces entreprises ont développées à l'égard du domaine. Un mélange des genres pourrait finalement n'avoir en l'état pour seules conséquences que d'affaiblir le positionnement distinctif des deux domaines.

Compte tenu de la portée et des conséquences importantes que revêt une telle décision, il convient de confier au Conseil fédéral le soin de déterminer si et quand une éventuelle ouverture de l'éligibilité du «.swiss» en faveur des personnes physiques devrait lieu par la grâce d'un amendement de la liste des personnes éligibles figurant à l'art. 55. L'actuelle délégation de compétence au DETEC est dès lors supprimée et son ordonnance sur le domaine Internet «.swiss» abrogée (cf. ci-dessous).

Art. 61 à 64 Dispositions transitoires

Die Übergangsbestimmungen äussern sich zu den Rechten und Pflichten von Switch im Rahmen des Delegationsverähltnisses nach dem Vertrag vom 31. Januar 2007. Die Bestimmungen sind obsolet geworden und können demzufolge aufgehoben werden.

Annexe

La définition de la notion de «dénomination à caractère générique» qui figure dans l'annexe de l'ODI (let. q) fait l'objet d'une légère adaptation, dans la mesure où la notion de «choses» est remplacée par celle de «produits» dans l'énumération des catégories ou classes de ce qui constitue une dénomination à caractère générique au sens de l'ODI.

La notion de «choses» se réfère à tout ce qui est, tout ce qui existe, à la réalité de toute espèce. Cette notion universelle se révèle en définitive trop large en englobant des dénominations qui ne devraient en principe pas tomber sous le coup de l'art. 56 ODI. Celui-ci vise principalement à préserver les dénominations qui peuvent en tant que noms de domaine procurer un avantage concurrentiel disproportionné à leurs titulaires sur l'Internet et dont la monopolisation est contraire à l'intérêt collectif de la communauté suisse. La notion de «produits» en tant que choses, substance et autres marchandises nées de l'activité de l'homme et généralement commercialisables est mieux adaptée au but visé par les règles de l'ODI concernant les dénominations à caractère générique.

Abrogation

L'ordonnance du DETEC du 11 août 2015 sur le domaine Internet «.swiss» (RS 784.104.253) n'a plus de portée propre et doit en conséquence être abrogée:

- Les précisions apportées sur la base de l'art. 54 ODI à la phase d'attribution privilégiée de noms de domaine du «.swiss» («sunrise period») sont désormais caduques du fait que le domaine «.swiss» est dans sa phase d'exploitation ordinaire;

- La question de l’ouverture échelonnée de l’éligibilité à l’attribution d’un nom de domaine du «.swiss» relève désormais exclusivement de l’art. 55 ODI (cf. ci-dessus explications ad art. 55).