COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

CommDH/IssuePaper(2014)1
Original version

La prééminence du droit sur l'internet et dans le monde numérique en général

Document thématique
publié par le Commissaire aux droits de l'homme du Conseil de l'Europe

Résumé et recommandations du Commissaire

RESUME

Le présent document thématique s'intéresse à une question pressante : comment veiller à l'instauration et au maintien de la prééminence du droit sur l'internet et dans le monde numérique en général ? La première partie décrit l'éventail des activités en ligne et les menaces qui pèsent sur cet environnement. La deuxième partie examine les principes émergents de la « gouvernance de l'internet » et souligne le contrôle particulier que les Etats-Unis (et, en Europe, le Royaume-Uni) exercent sur le monde numérique ainsi que les risques afférents de fragmentation de l'internet. La troisième partie donne un aperçu des normes internationales relatives à la prééminence du droit et présente quelques problèmes d'application du droit dans ce nouvel environnement. Dans la quatrième partie, les grandes problématiques qui se dégagent des parties précédentes – liberté d'expression, privatisation des services de répression, protection des données, cybercriminalité et sécurité nationale – sont analysées plus en détail, ainsi que les délicats équilibres à ménager.

Le Commissaire aux droits de l'homme du Conseil de l'Europe a formulé un certain nombre de recommandations sur la base des questions soulevées dans le présent document thématique ; elles sont présentées à la suite de ce résumé.

Un nouvel environnement pour les activités humaines

Nous vivons dans un environnement numérique mondial, qui est à l'origine de nouveaux modes d'activité au niveau local, régional et mondial : nouveaux types d'engagement politique, échanges culturels, exercice des droits de l'homme, etc. Ces activités ne sont pas virtuelles au sens où elles échapperaient à la réalité. Bien au contraire, elles constituent une part essentielle de la vie réelle des citoyens. Les limitations de l'accès à l'internet et aux médias numériques et les tentatives de contrôle de nos activités en ligne et de nos communications électroniques portent atteinte aux droits fondamentaux que sont la liberté d'expression et d'information, la liberté d'association, et le droit à l'intimité et à la vie privée ; d'autres droits, comme la liberté de religion et de conviction ou le droit à un procès équitable, sont peut-être aussi compromis.

Bien entendu, le nouvel environnement numérique mondial est aussi un nouveau lieu où s'expriment les comportements illicites : diffusion des discours de haine et de la pédopornographie, incitation à la violence, violations de la propriété intellectuelle (« piratage »), fraude, vol d'identité, blanchiment de capitaux et attaques dirigées contre l'infrastructure de communication électronique elle-même, par le biais de logiciels malveillants (chevaux de Troie et vers par exemple) ou selon la technique du « déni de service ». La cybercriminalité et la cybersécurité sont aujourd'hui des problèmes majeurs.

Ces menaces prennent de plus en plus une dimension transnationale. S'il existe aujourd'hui un large consensus international sur la nécessité de s'atteler aux questions de

cybercriminalité, de cybersécurité et de terrorisme, les modalités précises de cette action, voire ce que recouvre la notion même de menace, sont loin de faire l'unanimité.

Quatre problématiques sortent du lot. Premièrement, les mesures mises en place par les Etats afin de lutter contre la cybercriminalité et les menaces contre la cybersécurité et la sécurité nationale sont plus que jamais inextricablement liées ; les frontières entre ces activités sont de moins en moins nettes et les institutions et agences concernées coopèrent plus étroitement. Deuxièmement, les Etats coordonnent aujourd'hui leurs actions dans tous ces domaines. Troisièmement, les agences de sécurité nationale et de renseignement sont de plus en plus souvent amenées à surveiller les activités d'individus et de groupes dans le monde numérique. Quatrièmement, l'accent n'est plus mis sur la répression *a posteriori*, mais sur le travail de renseignement et de prévention, les forces de l'ordre employant aujourd'hui des techniques – et des technologies – auparavant réservées aux services secrets.

Nature de l'environnement numérique

Données dangereuses

A une époque où se développent les « big data » (ou « données massives ») et l'« internet des objets », et où les données de nos activités sont diffusées ou exploitées sous forme agrégée et où de plus en plus d'objets – de choses – communiquent sur l'internet, il devient difficile de garantir un parfait anonymat : plus il y a de données, plus il est facile d'identifier les individus. De plus, l'extraction de données massives par des méthodes de plus en plus perfectionnées permet de créer des profils, lesquels, même s'ils sont exploités pour repérer des phénomènes rares (trouver un terroriste dans un grand ensemble de données comme les dossiers passagers des compagnies aériennes par exemple), ne sont pas fiables et peuvent involontairement aboutir à une forme de discrimination fondée sur la race, le genre, la religion ou la nationalité. L'élaboration de ces profils repose sur des méthodes d'une telle complexité que les décisions qui en découlent peuvent être impossibles à contester : même ceux qui appliquent ces décisions ne comprennent pas parfaitement le raisonnement qui les sous-tend.

L'environnement numérique peut, par sa nature même, porter atteinte au droit au respect de la vie privée et à d'autres droits fondamentaux, et compromettre la prise de décision responsable. Il existe un risque immense de fragilisation de la prééminence du droit – par l'affaiblissement ou la disparition du droit à la vie privée, la restriction de la liberté de communication ou de la liberté d'association – et d'ingérence arbitraire.

Des données mondiales et privées, mais pas si dématérialisées

En raison du caractère ouvert de l'internet (qui est sa plus grande force), tout point terminal du réseau peut communiquer avec quasiment tout autre point terminal, en empruntant l'itinéraire calculé le plus efficace, les données étant acheminées par toutes sortes de commutateurs, de routeurs et de câbles, qui constituent l'infrastructure physique de l'internet.

Par essence, le système de communication électronique est transnational, et même mondial, et, même si l'on parle de « nuage » ou « cloud », son infrastructure est bel et bien matérielle et située dans des lieux bien réels. A l'heure actuelle, bon nombre de ces composants physiques se trouvent aux Etats-Unis et beaucoup sont gérés et commandés non pas par des organismes publics, mais par des entités privées.

L'infrastructure de l'internet est pour l'essentiel composée de câbles sous-marins à fibre optique de capacité élevée, associés à des câbles et à des routeurs terrestres. Pour l'Europe, les câbles les plus importants sont ceux qui relient le continent au Royaume-Uni et, de là, traversent l'océan Atlantique pour rejoindre les Etats-Unis. Compte tenu de la prédominance des entreprises américaines sur l'internet et dans le « cloud », ces câbles acheminent une grande partie du trafic internet et des données de communication reposant sur le réseau, notamment la quasi-totalité des données en provenance et à destination de l'Europe.

Qui a le contrôle ?

Gouvernance de l'internet

D'importants principes de gouvernance de l'internet ont été préconisés, par le Conseil de l'Europe et par d'autres. Ces principes soulignent la nécessité d'appliquer le droit international public et les normes internationales en matière de droits de l'homme, aussi bien en ligne que hors ligne, et de respecter la prééminence du droit et la démocratie sur l'internet. Ces principes reconnaissent et encouragent l'intervention de multiples parties prenantes dans la gouvernance de l'internet et exhortent tous les acteurs publics et privés à respecter les droits de l'homme dans toutes leurs opérations et activités, y compris dans la conception des technologies, services et applications. Ils appellent en outre les Etats à respecter la souveraineté des autres nations et à s'abstenir de toute action qui porterait atteinte à des personnes ou à des entités ne relevant pas de leur compétence territoriale.

Cela étant, ces principes dépassent rarement le stade des déclarations et des intentions : la gouvernance de l'internet souffre toujours d'un manque de dispositions concrètes sur lesquelles s'appuyer pour mettre ces principes en œuvre.

En outre, en matière de gouvernance de l'internet, il faut tenir compte du fait que les Etats-Unis exercent sur le réseau un contrôle plus important que tout autre Etat (et même que la totalité des autres Etats). Cette situation s'explique en partie par la prédominance du secteur privé, mais aussi par divers accords qui tiennent à l'histoire de l'internet. Ainsi les Etats-Unis et leur partenaire clé, le Royaume-Uni, ont-ils accès à la quasi-totalité de l'infrastructure internet.

L'ancien consultant de la NSA (Agence de sécurité nationale américaine) Edward Snowden a révélé que les Etats-Unis et le Royaume-Uni utilisent cette capacité de contrôle et d'accès pour effectuer une surveillance de masse de l'internet, des systèmes mondiaux de communication électronique et des réseaux sociaux. Certains craignent que ces révélations entraînent une fragmentation de l'internet, les Etats ou les régions insistant pour que leurs

données soient acheminées exclusivement par des routeurs et des câbles situés sur leur territoire et pour qu'elles soient stockées dans des « clouds » locaux. D'où le risque de disparition de l'internet tel que nous le connaissons actuellement, en raison de l'édification d'obstacles nationaux venant entraver le réseau mondial. Si, dans leurs activités ayant trait à l'internet et aux systèmes de communication mondiaux, les Etats-Unis ne respectent pas mieux les normes internationales en matière de droits de l'homme, il sera difficile d'arrêter cette évolution, qui conduira à un internet morcelé.

Contrôle du secteur privé

L'infrastructure internet et l'environnement numérique en général sont pour l'essentiel entre les mains d'entités privées, parmi lesquelles de nombreuses entreprises américaines. Cette situation est doublement problématique : d'une part, les entreprises ne sont pas directement liées par le droit international en matière de droits de l'homme – qui ne s'applique directement qu'aux Etats et aux gouvernements –, d'autre part, il est difficile d'obtenir réparation pour des préjudices causés par ces entreprises. En outre, les entités privées sont soumises à la législation nationale des pays dans lesquels elles sont établies ou actives, législations qui ne respectent pas toujours le droit international ou les normes internationales en matière de droits de l'homme : elles peuvent imposer des restrictions aux activités en ligne (classiquement, la liberté d'expression), en violation des normes internationales en matière de droits de l'homme ; elles peuvent aussi imposer ou autoriser une ingérence contraire à ce droit, comme la surveillance des activités en ligne ou des communications électroniques ; de plus, ces mesures peuvent être appliquées en dehors du territoire, en violation de la souveraineté d'autres Etats.

Il est extrêmement complexe et délicat d'appliquer les législations nationales aux activités d'entités privées contrôlant de vastes parties du monde numérique. Il va de soi que les Etats ont le droit, et même le devoir, de lutter contre les activités criminelles qui exploitent l'internet ou les systèmes de communication électronique. Ils sollicitent pour ce faire l'aide d'acteurs privés compétents. De même, les entreprises privées cherchent à protéger l'utilisation de leurs produits et services à des fins criminelles. Quoi qu'il en soit, dans cette lutte, les Etats doivent pleinement respecter leurs engagements internationaux en matière de droits de l'homme ainsi que la souveraineté des autres Etats. En particulier, ils ne doivent pas contourner les obligations découlant de leur Constitution ou du droit international en encourageant les restrictions aux droits de l'homme imposées par des actions « volontaires » menées par des intermédiaires. Les entreprises aussi doivent respecter les droits fondamentaux des personnes.

La prééminence du droit dans le nouvel environnement numérique

La prééminence du droit

La prééminence du droit est un principe de gouvernance en vertu duquel l'ensemble des individus, des institutions et des entités publiques et privées, y compris l'Etat lui-même, ont à

répondre de l'observation de lois promulguées publiquement, appliquées de façon identique pour tous et administrées de manière indépendante, et compatibles avec les règles et normes internationales en matière de droits de l'homme. Il implique le respect des principes de la primauté du droit, de l'égalité devant la loi, de la responsabilité au regard de la loi, de l'équité dans l'application de la loi, de la séparation des pouvoirs, de la participation à la prise de décisions, de la sécurité juridique, du refus de l'arbitraire et de la transparence des procédures et des processus législatifs.

Les critères fondamentaux élaborés par la Cour européenne des droits de l'homme en matière de « prééminence du droit »

La Cour européenne des droits de l'homme a, dans sa jurisprudence, élaboré des critères détaillés en matière de prééminence du droit, qui ont également été adoptés par d'autres organisations internationales de défense des droits de l'homme. Pour satisfaire à ces critères, toutes les limitations des droits fondamentaux doivent s'appuyer sur des règles juridiques claires, précises, accessibles et prévisibles, et servir des objectifs manifestement légitimes ; elles doivent être « nécessaires » et « proportionnées » au but légitime poursuivi (moyennant une certaine « marge d'appréciation ») ; et il doit exister un « recours effectif [de préférence juridictionnel] » contre les allégations de violations de ces obligations.

« Toute personne », sans discrimination

Le droit international en matière de droits de l'homme possède depuis 1945 une caractéristique essentielle, qui est aussi l'une de ses grandes réussites : les droits de l'homme doivent être accordés à « toute personne », à tous les êtres humains ; il ne s'agit donc pas seulement des droits des citoyens, mais bien des droits de l'homme.

Ainsi, sauf exceptions très limitées, toutes les lois de tous les Etats ayant une incidence ou empiétant sur les droits de l'homme doivent s'appliquer à « toute personne », sans discrimination « de quelque forme que ce soit », y compris la discrimination fondée sur le lieu de résidence ou la nationalité.

Compte tenu du rôle singulier que jouent les Etats-Unis et les entreprises américaines dans le fonctionnement de l'internet, le cadre juridique des institutions et des entreprises dans ce pays revêt une importance particulière. Cela étant, contrairement au principe susmentionné du droit international des droits de l'homme, bon nombre de garanties des droits fondamentaux accordées dans la Constitution des Etats-Unis et dans diverses lois américaines relatives à l'environnement numérique ne s'appliquent qu'aux citoyens américains et aux non-ressortissants résidant aux Etats-Unis (les *US persons* ou « personnes des Etats-Unis »). Ainsi, seules les « personnes des Etats-Unis » bénéficient du Premier Amendement, qui couvre la liberté d'expression et la liberté d'association, du Quatrième Amendement, qui protège les citoyens des Etats-Unis contre les « perquisitions non motivées », et de la plupart des protections (restreintes) contre la surveillance excessive, qui sont garanties par les principaux textes de loi sur la sécurité nationale et le renseignement (*FISA Amendment* et *Patriot Acts*).

« [Se trouvant sur le territoire d'un Etat partie et] relevant de [sa] juridiction »

Le devoir des Etats de s'acquitter des responsabilités qui leur incombent au titre du droit international des droits de l'homme, y compris lorsqu'ils agissent hors de leur territoire

Les grands traités internationaux relatifs aux droits de l'homme, notamment le Pacte international relatif aux droits civils et politiques (PIDCP) et la Convention européenne des droits de l'homme (CEDH), font obligation aux Etats de « garantir » ou de « reconnaître » les droits de l'homme consacrés dans ces traités à « tous les individus relevant de leur compétence » (ou « relevant de leur juridiction »). Cette obligation est de plus en plus souvent interprétée dans un sens fonctionnel plutôt que territorial, ainsi que l'ont récemment réaffirmé le Comité des droits de l'homme des Nations Unies et la Cour européenne des droits de l'homme. Autrement dit, chaque Etat est tenu de garantir ou de reconnaître ces droits à toute personne qui est placée sous son contrôle physique ou dont les droits subissent les effets de ses actions (ou de celles de ses institutions).

Ainsi, les Etats doivent s'acquitter de leurs obligations internationales en matière de droits de l'homme dans toutes leurs actions susceptibles d'avoir une incidence sur les droits fondamentaux des personnes, même lorsqu'ils agissent hors de leur territoire ou qu'ils prennent des mesures ayant un effet extraterritorial.

S'agissant des données – qui constituent la matière même du monde numérique –, cette obligation a des conséquences spécifiques, tout particulièrement en ce qui concerne les données à caractère personnel, comme le reconnaît le droit européen de protection des données, qui protège tous les individus dont les données sont traitées par des responsables européens du traitement des données, et ce quels que soient leur lieu de résidence, leur nationalité ou d'autres statuts. Mais les Etats-Unis rejettent officiellement cette mise en œuvre du droit international en matière de droits de l'homme. Compte tenu de leur prédominance dans le monde numérique (et de celle des entreprises américaines relevant de leur juridiction), cette situation constitue une sérieuse menace pour la prééminence du droit dans ce nouvel environnement.

Problèmes de concurrence et de compatibilité dans l'application simultanée des lois aux activités en ligne, s'agissant notamment de la liberté d'expression

Dans leur application aux contenus et aux activités en ligne, les différentes législations nationales entrent en concurrence et posent des problèmes de compatibilité. Pour garantir la prééminence du droit sur l'internet, ces problèmes doivent être traités de toute urgence.

Cette question ne concerne pas le droit des Etats de prendre des mesures conformes au droit international et nécessaires et proportionnées dans une société démocratique. Cela va de soi, les Etats doivent rester libres de légiférer dans leur propre juridiction. La question est la capacité et le droit des gouvernements ou des tribunaux nationaux à prendre des mesures imposant des restrictions dans des pays tiers, où les intéressés agissent conformément à la législation de leur pays de résidence, législation qu'ils sont censés connaître (ou pouvoir

connaître), contrairement à la législation du pays étranger, et dont l'application devrait être prévisible.

En principe, les personnes et les entreprises qui publient des informations à partir de leur pays de résidence ou d'établissement ne devraient être soumises qu'à la législation du pays en question. Quant aux personnes qui accèdent à des informations provenant de sites web étrangers, ou qui les téléchargent, alors qu'elles pourraient ou devraient savoir que ces informations sont illégales dans leur pays de résidence, on peut estimer qu'elles devraient respecter la législation de ce pays. Les Etats ne devraient exercer leur compétence sur des informations étrangères qui ne sont pas illégales au regard du droit international que dans des cas limités, c'est-à-dire lorsqu'il existe un rapport clair et étroit entre, d'une part, les informations ou celui qui les diffuse et, d'autre part, l'Etat qui prend des mesures.

Droits de l'homme et entités privées

Droit en matière de droits de l'homme, principes de Ruggie et standards du Conseil de l'Europe et d'autres institutions

Le droit international en matière de droits de l'homme ne s'applique fondamentalement qu'aux Etats et aux actions (ou omissions) des pouvoirs publics. Cela étant, de nouvelles normes internationales destinées aux entreprises voient aujourd'hui le jour. Les plus importantes sont les *Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme* (Principes de Ruggie), qui ont été élaborés par John Ruggie, Représentant spécial du Secrétaire général des Nations Unies pour les entreprises et les droits de l'homme. Or ces principes portent toujours sur l'obligation faite aux pays d'accueil de lutter activement contre les violations des droits de l'homme commises par les entreprises, et ne traitent pas en détail de la situation inverse, dans laquelle les Etats imposent aux entreprises des exigences qui, si elles sont satisfaites, amènent ces dernières à commettre des violations du droit international en matière de droits de l'homme.

Il apparaît important que le Conseil de l'Europe et d'autres organisations élaborent de nouveaux principes relatifs à la responsabilité des entreprises auxquelles les Etats ou d'autres entités privées imposent de soutenir des mesures susceptibles d'enfreindre le droit international en matière de droits de l'homme (ou des entreprises qui se placent dans une situation telle qu'elles risquent de s'exposer à de telles exigences) (voir à ce sujet l'examen détaillé au chapitre consacré à la privatisation des services de répression).

Filtrage et blocage de l'internet et des entreprises de communication électronique sur ordre – ou sur « invitation » – des Etats

Outre la criminalisation des informations sur l'internet – pratique de plus en plus courante *a posteriori* après publication et consultation d'informations produites dans un pays tiers –, les Etats cherchent aussi de plus en plus à prévenir (à bloquer) l'accès à certains types de documents et d'informations en ligne. Le blocage ou le filtrage est effectué à l'aide de matériels ou de programmes informatiques, qui examinent les communications et décident,

sur la base de critères prédéfinis, s'il convient ou non de transmettre les documents concernés au destinataire, souvent une personne qui surfe sur le web.

Il n'est peut-être pas surprenant de constater que les Etats répressifs tentent de bloquer l'accès aux sites web d'opposition et que les régimes théocratiques font de même avec les sites qu'ils tiennent pour blasphématoires. Mais de plus en plus souvent, certains Etats, qui respectent prétendument la prééminence du droit – y compris des Etats membres du Conseil de l'Europe –, cherchent aussi à bloquer l'accès à des informations qu'ils jugent inacceptables. Ou, de façon plus insidieuse et moins responsable, ils « encouragent » les contrôleurs d'accès de l'internet – fournisseurs d'accès à internet (FAI) et opérateurs de réseau mobile (ORM) – à adopter « volontairement » de telles pratiques, en dehors de tout cadre juridique de droit public précis.

En règle générale, dans les pays démocratiques, les mesures de blocage ou de filtrage ont visé, du moins officiellement et dans un premier temps, des cibles résolument légitimes : « discours de haine » racistes ou religieux et pédopornographie. Mais, dans leur façon de fonctionner, les différents systèmes mis en place présentent des déficiences majeures :

- par essence, le blocage a toutes les chances de produire (sans que cela soit voulu) de faux positifs (sites bloqués alors qu'ils ne présentent pas de contenus interdits) ainsi que de faux négatifs (sites présentant des contenus interdits, mais qui échappent au système de filtrage) ;
- les critères utilisés pour bloquer certains sites, mais pas d'autres, ainsi que les listes de sites bloqués sont très souvent au mieux opaques, au pire secrets ;
- les voies de recours peuvent être onéreuses, peu connues ou inexistantes, en particulier lorsque la décision de blocage ou de non-blocage est – délibérément – laissée aux entités privées ;
- les mesures de blocage sont faciles à contourner, même pour des personnes techniquement peu expérimentées ;
- point essentiel, en particulier en ce qui concerne la pédopornographie, le blocage ne s'attaque absolument pas au problème réel, à savoir les abus commis sur les enfants en question.

Ces déficiences sont aggravées par le fait que les Etats, après avoir mis en place des systèmes de blocage contre les problèmes les plus graves (pédopornographie, discours de haine, etc.), ont tendance à étendre cette pratique à toutes sortes de sujets qu'ils désapprouvent. A travers le monde, y compris en Europe, des Etats ont ainsi tenté de bloquer non seulement des sites affichant des discours de haine ou prônant le terrorisme, mais aussi, par exemple, des sites de débat politique ou d'information sur les droits des minorités ou les droits en matière de sexualité.

Deux cas de figure se dégagent naturellement : le blocage licite et le blocage illicite de contenus. Certains types de contenu font l'objet de mesures de blocage à juste titre (blocage licite de contenus illégaux), cela est incontestable. Néanmoins, pour déterminer si une mesure de blocage est proportionnée et donc licite, il est essentiel d'en examiner l'objectif et les moyens techniques employés pour la mettre en œuvre. Par exemple, si rien ne permet

d'affirmer que les accès accidentels au contenu concerné sont significatifs et s'il est facile d'accéder intentionnellement au contenu malgré la mesure de blocage, la proportionnalité de la mesure est discutable.

La question se complique lorsque le choix des sites à bloquer est laissé à l'appréciation d'entités privées « encouragées » par les Etats qui déclarent ne pas endosser la responsabilité du blocage (blocage non licite de contenus). Certains pays comme le Royaume-Uni et la Suède ont mis en place des systèmes de blocage reposant sur des accords volontaires conclus avec des FAI. Si toutes les considérations touchant à l'efficacité et à la proportionnalité de la mesure restent pertinentes, ce type de blocage soulève une question plus générale et plus fondamentale qui appelle une réponse : dans quelle mesure ces décisions de blocage sont-elles vraiment volontaires et/ou engagent-elles la responsabilité de l'Etat ? Si, s'agissant de ce droit, l'article 10 de la CEDH ne mentionne que les ingérences « d'autorités publiques », cela ne signifie pas que l'Etat peut, purement et simplement, décliner toute responsabilité vis-à-vis de mesures d'entités privées produisant cet effet, et ce d'autant moins s'il encourage vivement ces mesures *de facto*. Dans ces circonstances, l'Etat est responsable de ne pas avoir donné à un tel système une base législative : sans cette base, les restrictions ne sont pas prévues par la « loi ».

Dans sa jurisprudence récente, la Cour européenne des droits de l'homme a clairement relevé les dangers du blocage indifférencié. Dans son arrêt concernant l'affaire *Yildirim c. Turquie*, la Cour fait observer que la mesure objet du litige – blocage de l'accès à tous les sites web hébergés par Google Sites en Turquie en vue de bloquer l'un d'eux, considéré comme irrespectueux vis-à-vis de Kemal Atatürk – a eu des effets arbitraires et ne saurait être considérée comme visant uniquement à bloquer l'accès au site litigieux, étant donné qu'elle consistait en un blocage général de tous les sites hébergés par Google Sites. En outre, la Cour a considéré que le contrôle juridictionnel du blocage de l'accès aux sites internet ne réunissait pas les conditions suffisantes pour éviter les abus, étant donné que le droit interne ne prévoyait aucune garantie pour éviter qu'une mesure de blocage visant un site précis ne soit utilisée comme moyen de blocage général. La Cour a donc conclu à une violation de l'article 10 de la CEDH.

Inspection détaillée des paquets (IDP) indifférenciée, réalisée par des entreprises sur injonction d'un tribunal suite à la demande d'autres entreprises en vue d'assurer le respect du droit de propriété intellectuelle

De plus en plus souvent, les détenteurs de droits de propriété intellectuelle demandent que soient imposés des filtrages ou des blocages analogues à ceux décrits ci-dessus à l'encontre de sites internet qui facilitent prétendument le partage de contenus piratés ; ils exigent aussi, plus que jamais, l'accès à des informations personnelles concernant les internautes en lien avec ces allégations de partage, notamment via le recours obligatoire à des IDP réalisées par les FAI en vue de repérer de probables (ou possibles) contrevenants.

L'IDP fait obligation à l'« inspecteur » d'examiner non seulement les métadonnées générales concernant l'origine et la destination du « paquet », mais aussi le contenu des communications. Les « paquets » sont sélectionnés sur la base d'un schéma ou d'un

algorithme lié à la spécificité du contenu. Pour les détenteurs de droits de propriété intellectuelle, il s'agira d'un marquage particulier sur une vidéo ou une photographie donnée, protégée par le droit d'auteur. Mais cette technologie permet aussi de rechercher quasiment n'importe quelle information : un discours politique, un chant révolutionnaire, une banderole de syndicat. Ces mesures sont très intrusives, car elles demandent la surveillance de tous les utilisateurs d'un FAI (ou réseau de téléphonie mobile) pour tenter d'identifier les quelques personnes qui enfreignent probablement (ou éventuellement) le droit de propriété intellectuelle. Elles soulèvent donc de très vives inquiétudes quant à leur nécessité et à leur proportionnalité.

Tant la Cour européenne des droits de l'homme que la Cour de justice de l'Union européenne ont rendu des arrêts importants qui laissent clairement entendre que le filtrage indifférencié de l'ensemble des communications acheminées par un FAI (ou un ORM) – autrement dit, le suivi ou la surveillance généralisé – à des fins d'identification d'éventuels contrevenants parmi la masse des utilisateurs innocents est contraire au droit en matière de droits de l'homme.

Exercice de la compétence extraterritoriale par les Etats

Tout Etat qui utilise ses pouvoirs législatif et répressif pour s'emparer de données qui ne sont pas détenues sur son territoire physique, mais sur le territoire d'un autre Etat, en vue d'exercer un contrôle sur ces données – en général en exploitant l'infrastructure matérielle de l'internet et les systèmes de communication mondiale pour extraire ces données de serveurs situés dans l'autre Etat, ou en chargeant des organismes privés ayant accès à ces données à l'étranger de les extraire de serveurs situés dans un autre pays et de les remettre à l'Etat intéressé – exerce sa compétence de manière extraterritoriale au sein de la juridiction de l'autre Etat.

En vertu du droit international public général et en l'absence de traités octroyant à des organismes étrangers des compétences en matière d'exécution extraterritoriale, il n'est pas légal que le premier Etat agisse ainsi sans l'accord du second.

Les questions en jeu et le juste équilibre à trouver

Les questions en jeu

Pour établir la prééminence du droit sur l'internet et dans le monde numérique en général, une clarification des règles touchant à la liberté d'expression, aux entités privées (en particulier aux grandes sociétés) et aux droits de l'homme, ainsi qu'à la protection des données et à la cybercriminalité, est nécessaire. Il faudra ensuite répondre à la question suivante : comment trouver un juste équilibre entre ces règles dans ce nouvel environnement ?

Liberté d'expression

Les législations nationales relatives aux activités sur l'internet et dans l'environnement numérique en général, notamment les lois concernant la liberté d'expression, sont souvent contradictoires. Dans de nombreux pays, la législation interne dispose que les personnes tenant des propos sur l'internet ou dans des communications électroniques, dans un pays ou à partir de ce pays, peuvent être poursuivies aux termes de la législation d'un autre pays si les propos en question constituent une violation de celle-ci, quand bien même ils seraient conformes au droit du pays où ils ont été exprimés. Cet état de fait constitue une menace fondamentale pour la prééminence du droit sur l'internet et dans cet environnement. La jurisprudence de la Cour européenne des droits de l'homme ne rend pas encore pleinement compte de cette question.

Comme il a été proposé plus haut, la seule façon de résoudre ce problème serait que les Etats et les tribunaux nationaux fassent clairement preuve de modération en s'abstenant d'imposer leurs normes juridiques internes aux propos et aux informations diffusés sur l'internet à partir de l'étranger, à moins que ceux-ci ne soient contraires au droit international ou qu'ils ne présentent des liens manifestes justifiant l'exercice de la compétence de l'Etat.

Autre aspect important dont il faut tenir compte : la responsabilité des personnes ou des entreprises gérant un site web, voire des FAI, au regard des contenus publiés sur un site. Là aussi, la jurisprudence à l'échelle européenne est encore limitée. Pour l'heure, les sociétés privées semblent être prises entre, d'un côté, des obligations clairement définies (retrait du contenu ou risque de sanction) et, de l'autre, des obligations plus difficiles à cerner (garantir l'accès des utilisateurs aux contenus licites). Par conséquent, les sociétés privées peuvent avoir tendance à opter pour l'excès de conformité et à interdire à tous les utilisateurs l'accès à des documents parfaitement licites, tout en se protégeant d'éventuelles réclamations de la part des utilisateurs lésés en imposant des conditions contractuelles peu précises. Il s'agit là de problèmes essentiels qui doivent être résolus.

Privatisation des services de répression

Le fait que l'internet et l'environnement numérique mondial soient largement contrôlés par des entités privées (en particulier mais pas seulement des sociétés établies aux Etats-Unis) constitue également une menace pour la prééminence du droit. Ces entités privées peuvent limiter (et être « encouragées » à limiter) l'accès aux informations, sans être soumises aux contraintes du droit constitutionnel ou du droit international, qui s'appliquent aux restrictions du droit à la liberté d'expression imposées par les Etats. Les tribunaux nationaux, agissant à la demande d'autres entités privées, peuvent aussi leur enjoindre d'effectuer des analyses très intrusives de leurs propres données en vue de déceler de probables (ou simplement de possibles) atteintes aux droits à la propriété privée, souvent aux droits à la propriété intellectuelle. Elles peuvent se voir ordonner de procéder à l'« extraction » de données, en particulier de données gouvernementales, commerciales ou à caractère personnel, se trouvant dans des serveurs situés dans d'autres pays, à des fins d'application de la loi ou de sécurité nationale, sans le consentement du pays tiers – ou le consentement des entreprises ou des

personnes concernées de ce dernier –, en violation de la souveraineté du pays tiers, de la confidentialité commerciale à laquelle les entreprises ont droit et des droits fondamentaux des personnes concernées.

Les Principes de Ruggie édictés par les Nations Unies soulignent qu'il importe de s'atteler à ces questions, mais n'apportent pas de réponses. Nous l'avons dit, de nouvelles approches et de nouveaux principes directeurs sont donc nécessaires. Le Conseil de l'Europe a largement contribué à ce débat en proposant, d'une part, que les Etats rendent des comptes s'ils ne garantissent pas que les entités privées respectent les droits fondamentaux de leurs citoyens et, d'autre part, qu'ils aient l'obligation de garantir que les conditions générales des entreprises privées non conformes aux normes internationales en matière de droits de l'homme soient obligatoirement réputées nulles et non avenues.

Protection des données

Le droit européen en matière de protection des données repose sur un ensemble de principes fondamentaux (traitement loyal, détermination et limitation des finalités, minimisation des données, qualité des données et sécurité des données) et sur un ensemble de droits (droits de la personne concernée par les données) et de voies de recours (contrôle par des autorités de protection des données indépendantes), qui sont la traduction, dans ce contexte particulier, des principes généraux de « prééminence du droit » élaborés par la Cour européenne des droits de l'homme. La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention n° 108) et les règles élaborées par l'Union européenne sur ce thème précisent comment remplir les obligations générales du droit en matière de droits de l'homme dans le contexte particulier du traitement des données à caractère personnel. Le modèle européen de protection des données est de plus en plus adopté hors de la zone du Conseil de l'Europe : la Convention n° 108 (en cours de modernisation) acquiert petit à petit le statut de texte de référence dans le monde en ce qui concerne le respect de la prééminence du droit à l'échelle internationale dans ce domaine particulier, ce qui constitue une évolution essentielle pour l'internet et le monde numérique en général.

La protection des données en Europe a encore été renforcée par un arrêt de la Cour de justice de l'Union européenne, qui a invalidé la conservation de données obligatoire, sans suspicion et non ciblée. Dans le contexte du débat sur les pratiques des services de renseignement et de sécurité suscité par les révélations d'Edward Snowden, il est de plus en plus manifeste que les programmes de surveillance secrète, massive et indifférenciée ne sont pas conformes avec le droit européen en matière de droits de l'homme et ne peuvent être justifiés par la lutte contre le terrorisme et autres menaces majeures pour la sécurité nationale. De telles ingérences ne peuvent être acceptées que si elles sont strictement nécessaires et proportionnées à un but légitime.

La protection des données axée sur les critères européens constitue le premier et le plus important pilier de la prééminence du droit sur l'internet et dans le monde numérique en général. Il sera donc primordial de veiller à ce que la révision (modernisation) de la

Convention n° 108, qui est en cours, n'aboutisse pas à un relâchement des niveaux d'exigence. L'adhésion des Etats-Unis à cette Convention serait tout particulièrement appréciable, non seulement pour les citoyens américains, mais aussi parce qu'elle serait un pas vers une approche mondiale et plus globale du respect du droit fondamental à la protection des données et des autres droits qui en découlent.

Cybercriminalité

La Convention sur la cybercriminalité fait obligation aux Etats parties d'ériger en infraction pénale, au titre de leur législation nationale, certains actes tels que l'accès illégal à des systèmes informatiques (piratage), l'interception illégale de communications électroniques, l'envoi de logiciels malveillants, les violations du droit de propriété intellectuelle et la production ou la diffusion de contenus à caractère pédopornographique ; en outre, en vertu du protocole additionnel à cette Convention, les Etats parties ont l'obligation d'ériger en infraction pénale la diffusion de contenus racistes et xénophobes (discours de haine). De plus, la Convention contient des dispositions très poussées en matière de coopération internationale dans la lutte contre ces infractions, notamment l'entraide judiciaire en matière d'enquête et de conservation des preuves, d'extradition et de questions analogues. Elle est ouverte aux Etats non européens : cinq l'ont ainsi ratifiée, notamment les Etats-Unis.

Si la nécessité de trouver un accord pour lutter contre la criminalité dans l'environnement numérique mondial est indiscutable – et le Conseil de l'Europe doit être salué pour avoir engagé ce processus –, la Convention n'est pas encore pleinement à même d'assurer la conformité avec la prééminence du droit dans sa mise en œuvre par les Etats parties.

L'une des raisons de cette difficulté est que la Convention ne contient pas de clause suffisamment exhaustive en matière de droits de l'homme et que, par conséquent, elle n'offre pas de protection contre les Etats qui imposent des infractions pénales de trop vaste portée ou qui omettent d'intégrer des exceptions ou des moyens de défense dans leur droit matériel (défense de l'intérêt général pour les donneurs d'alerte par exemple) ; elle ne protège pas non plus contre la double incrimination ni contre l'assistance (formelle ou informelle) apportée aux Etats parties lorsqu'elle est susceptible de porter atteinte aux droits de l'homme.

Une autre raison tient au fait que la Convention n'est pas liée à d'autres instruments majeurs élaborés par le Conseil de l'Europe afin d'assurer la prééminence du droit dans les environnements numériques et/ou transnationaux. Cette mise en relation semble d'autant plus nécessaire que la Convention est ouverte aux Etats qui ne sont pas parties à la CEDH ou qui n'ont pas pleinement accepté les exigences comparables du PIDCP (par exemple, les Etats-Unis en ce qui concerne ses activités extraterritoriales ou les droits des « *non-US persons* »). Du point de vue de la prééminence du droit en Europe, l'adhésion à la Convention sur la cybercriminalité devrait imposer aux Etats qu'ils acceptent pleinement les obligations qui leur incombent au titre de la CEDH et/ou du PIDCP et qu'ils ratifient la Convention sur la protection des données, la Convention européenne d'extradition et la Convention européenne d'entraide judiciaire en matière pénale.

Enfin, il apparaît que les articles 26 et 32 de la Convention soutiennent la tendance des services répressifs à recourir à des moyens « informels » de collecte de données, même d'un pays à l'autre, sans que soient fixées des garanties claires (notamment le fait que ce type de mesures informelles ne devrait pas être utilisé pour des activités de collecte intrusive de données qui, normalement, dans un Etat régi par la prééminence du droit, nécessitent un mandat de l'autorité judiciaire) ; ces deux articles semblent aussi favoriser la tendance croissante de ces autorités à « extraire » des données directement à partir de serveurs situés dans d'autres pays, ou à exiger que des sociétés relevant de leur juridiction – en particulier les principaux géants de l'internet – le fasse pour leur compte, sans recourir à des accords formels d'entraide judiciaire entre Etats, ce que l'on pourrait considérer comme une violation de la souveraineté de l'Etat dans lequel les données se trouvent.

En outre, la Convention sur la cybercriminalité devrait être davantage guidée par le principe établi à l'article 16 de la Convention n° 108, s'agissant de l'entraide entre autorités chargées de la protection des données, principe selon lequel il existe des limitations précises quant aux circonstances dans lesquelles des données à caractère personnel peuvent être collectées et/ou transmises dans le cadre d'activités transnationales. Plusieurs recommandations et déclarations du Comité des Ministres du Conseil de l'Europe fournissent des indications utiles sur la façon de trouver un juste équilibre entre le respect des principes de protection des données et l'application suffisante de la loi. Il convient de renforcer la conformité des Etats membres parties à la Convention sur la cybercriminalité avec ces instruments.

La rédaction du nouveau protocole additionnel à la Convention sur la cybercriminalité, qui est proposé, offre une occasion de résoudre au moins quelques-uns de ces problèmes. Grâce à ces améliorations, la Convention sur la cybercriminalité pourrait constituer le deuxième pilier de la prééminence du droit sur l'internet et dans le monde numérique en général.

Sécurité nationale

En principe, la Convention européenne des droits de l'homme et la Convention sur la protection des données du Conseil de l'Europe s'appliquent à toutes les activités des Etats signataires : ces deux Conventions intègrent certes des règles spéciales et des exceptions, mais les questions de sécurité nationale n'en sont pas expressément exclues. En cela, le mandat du Conseil de l'Europe et la portée de ces instruments diffèrent du droit communautaire, qui exclut expressément la sécurité nationale de la compétence et de la juridiction de l'Union. Autrement dit, s'agissant des réglementations juridiques internationales des activités des agences de sécurité nationale et de renseignement, le Conseil de l'Europe doit montrer la voie, sinon à l'échelle planétaire, du moins en Europe.

A la lumière des révélations d'Edward Snowden à propos des opérations mondiales de surveillance de la NSA (Agence de sécurité nationale américaine), du GCHQ (Agence de renseignement du Royaume-Uni) et de leurs partenaires du groupe 5EYES (Australie, Canada et Nouvelle-Zélande) en particulier, il est devenu incontestablement nécessaire de reconnaître la prééminence du droit dans le contexte des activités des agences de sécurité nationale et de renseignement. Ces révélations ont montré que ces agences ont pour habitude de placer sur

écoute les câbles à fibre optique de haute capacité qui constituent les systèmes dorsaux de l'internet et aussi d'intercepter en masse des communications mobiles et autres dans le monde entier, par exemple en captant des communications hertziennes au moyen de « portes dérobées » (*backdoors*) qu'elles ont installées dans les grands systèmes de communication et en exploitant les failles de sécurité de ces systèmes.

Dans le droit européen et international en matière de droits de l'homme, la sécurité nationale n'est pas un motif suprême qui surpasse toutes les autres considérations. De fait, la question même de ce que l'on peut légitimement englober sous le concept de « sécurité nationale » relève de la compétence des tribunaux : il devrait leur appartenir de déterminer, à la lumière du droit international en matière de droits de l'homme, ce qui est légitimement visé par ce terme, et ce qui ne l'est pas. Les *Principes de Johannesburg relatifs à la sécurité nationale, la liberté d'expression et l'accès à l'information*, rédigés par l'ONG Article 19 et adoptés par diverses enceintes internationales, notamment le Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, fournissent des indications à ce sujet. Ces principes affirment clairement que les Etats ne peuvent invoquer la sécurité nationale pour justifier une atteinte aux droits de l'homme que si l'identité même et les fondements des institutions de la nation sont menacés. Si le terrorisme peut parfois atteindre ce degré, ce phénomène devrait, dans la plupart des cas, être traité en faisant appliquer la loi et non dans un cadre de sécurité nationale. Cette approche s'applique également aux mesures prises par les Etats en lien avec l'internet et les communications électroniques.

Il n'existe pas suffisamment de règles conventionnelles claires qui régissent les interventions des agences de sécurité nationale et de renseignement, et qui décrivent les principes sur lesquels elles s'appuient pour fonctionner et échanger des données. De nombreux pays ne disposent que de quelques lois précises et publiées pour réglementer le travail de ces agences. Et dans certains, il n'existe absolument aucune règle officielle. Tant que les règles régissant le fonctionnement de ces agences et de ces services – en interne, à l'extérieur du territoire ou en coopération les uns avec les autres – ne sont pas connues, les activités de ces organes ne peuvent pas être supposées conformes aux principes de prééminence du droit. Une autre source de vive préoccupation concerne l'inefficacité patente de nombreux systèmes de surveillance.

Autrement dit, en matière de sécurité nationale, il n'existe pas encore de véritable pilier pour soutenir la prééminence du droit. On compte toutefois des principes fondamentaux qui pourraient constituer la base de cette pièce maîtresse de l'édifice universel des droits de l'homme.

Les services de répression et les agences de renseignement et de sécurité instaurent des partenariats de plus en plus nombreux. Cette négation de la prééminence du droit menace de se propager de ces agences aux agents de police et aux procureurs. L'absence de cadres juridiques clairs à cet égard, à l'échelon national comme au niveau international, est une menace supplémentaire pour la prééminence du droit sur l'internet et dans l'environnement numérique mondial.

RECOMMANDATIONS DU COMMISSAIRE

Au vu des constats et des conclusions du présent document thématique, le Commissaire formule les recommandations suivantes, qui visent à améliorer le respect de la prééminence du droit sur l'internet et dans l'environnement numérique en général.

I. Sur l'universalité des droits de l'homme et leur application sur un pied d'égalité en ligne et hors ligne

1. Les exigences fondamentales en matière de prééminence du droit s'appliquent, et il convient de les faire appliquer dans la pratique, sur un pied d'égalité en ligne et hors ligne. Cela signifie en particulier :

   - qu'aucun Etat (et qu'aucune de ses agences, notamment ses services de répression et ses agences de renseignement et de sécurité nationale), européen ou non, ne devrait accéder à des données conservées dans un autre pays – ou acheminées par les câbles des réseaux dorsaux de l'internet et des communications électroniques qui relient différents pays – sans le consentement clair et exprès du ou des pays tiers concernés. L'obtention du consentement des personnes concernées par les données (que ce soit indirectement, via les conditions générales des fournisseurs de communication, ou directement, selon des modalités qui ne seraient pas incontestablement libres, éclairées et suffisamment précises) ou la coopération d'entités privées établies dans le premier pays (ou dans le ou les pays cibles) ne saurait remplacer le consentement du pays cible ;

   - que la Convention européenne des droits de l'homme (CEDH) et toutes les règles du Conseil de l'Europe en matière de protection des données s'appliquent à toutes les activités de traitement des données à caractère personnel menées par toutes les agences de tous les Etats membres du Conseil de l'Europe, y compris les agences de renseignement et de sécurité nationale des Etats membres ;

   - que les obligations en matière de prééminence du droit, y compris celles découlant des articles 8 (droit au respect de la vie privée et familiale) et 10 (liberté d'expression) de la CEDH, ne peuvent pas être contournées au moyen d'accords *ad hoc* conclus avec des acteurs privés qui contrôlent l'internet et l'environnement numérique en général ; et

   - que les Etats membres du Conseil de l'Europe devraient tout mettre en œuvre pour que les Etats non européens respectent, de la même façon, leurs obligations internationales en matière de droits de l'homme dans toutes leurs actions qui touchent des personnes utilisant l'internet ou qui sont actives par ailleurs dans l'environnement numérique en général.

II. Sur la protection des données

2. Les Etats membres qui ne l'ont pas encore fait devraient ratifier la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention n° 108). Cette convention, également ouverte aux Etats non membres, peut, si elle est largement adoptée, devenir le pilier le plus important de la prééminence du droit sur l'internet et dans l'environnement numérique en général.

3. Les Etats membres qui ont déjà ratifié cette Convention devraient veiller à ce qu'elle soit pleinement mise en œuvre au niveau national.

4. La révision en cours de la Convention n° 108 ne devrait pas aboutir à un abaissement des niveaux d'exigence en matière de protection des données à l'échelle européenne ou mondiale. Bien au contraire, elle devrait permettre de préciser les règles et d'en renforcer l'application, en particulier en ce qui concerne l'internet et le monde numérique en général, ainsi que la surveillance à des fins de renseignement et de sécurité nationale.

5. S'agissant de la réforme actuelle des règles de l'Union européenne en matière de protection des données, les règles existantes susceptibles de porter atteinte à la prééminence du droit, notamment celles concernant le consentement, le profilage ou l'accès par des services de répression étrangers à des données à caractère personnel, devraient être précisées et harmonisées avec les obligations internationales en matière de droits de l'homme, y compris celles découlant de la Convention n° 108, et avec les recommandations et lignes directrices pertinentes du Conseil de l'Europe.

6. La conservation en masse et sans suspicion de données de communication est fondamentalement contraire à la prééminence du droit, incompatible avec les principes fondamentaux de protection des données et inefficace. Les Etats membres ne devraient pas y avoir recours ni imposer à des tiers la conservation obligatoire de données.

III. Sur la cybercriminalité

7. Les Etats parties à la Convention du Conseil de l'Europe sur la cybercriminalité doivent pleinement honorer leurs obligations internationales en matière de droits de l'homme dans toutes leurs actions (ou inactions) relevant de la Convention, que ce soit dans la définition des infractions correspondantes (ainsi que des éléments, des exceptions et des moyens de défense afférents), dans toutes les enquêtes ou poursuites pénales ou dans le cadre de l'entraide judiciaire et de l'extradition.

8. Tout Etat partie prenant des mesures à l'encontre de personnes situées en dehors de son territoire n'est pas pour autant exonéré de ses obligations contractées au titre de la Convention sur la cybercriminalité ou de traités internationaux en matière de droits de

l'homme (en particulier la CEDH et le PIDCP) ; bien au contraire, ces obligations s'appliquent de la même façon à ces mesures extraterritoriales.

9. Tous les Etats parties à la Convention sur la cybercriminalité devraient également ratifier et rigoureusement mettre en œuvre la Convention sur la protection des données, la Convention européenne d'extradition et la Convention européenne d'entraide judiciaire en matière pénale.

10. Les Etats membres, y compris leurs services de répression, devraient mettre en œuvre la Recommandation n° R (1987) 15 du Comité des Ministres du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, sa Recommandation Rec(2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage et sa déclaration de 2013 sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux.

11. Les Etats membres devraient s'assurer que leurs services de répression n'obtiennent pas, en vertu d'accords informels, de données à partir de serveurs et d'infrastructures situés dans un autre pays. Au lieu de cela, ils devraient faire appel aux accords d'entraide et aux accords spéciaux sur la conservation rapide de données, mis en place par la Convention sur la cybercriminalité. Les services de répression d'un pays ne devraient pas s'appuyer sur le fait que des entités privées de pays tiers – fournisseurs d'accès à l'internet, réseaux sociaux, opérateurs de réseau mobile, etc. – ont été autorisées à divulguer les données de leurs clients en vertu de leurs conditions générales ; l'obtention de ces données dans ces circonstances est contraire à la prééminence du droit et ne devrait pas se produire.

IV. Sur la compétence

12. Il devrait exister des limites à l'exercice extraterritorial de la compétence nationale en matière de cyber infractions transnationales. Ces limites devraient tenir compte de l'effet des restrictions matérielles aux infractions ainsi que des exceptions ou des moyens de défense dans le pays d'origine de l'intéressé (ou dans le pays où les actes ont été commis), au vu également de la compétence invoquée par d'autres Etats qui ne reconnaissent pas ces restrictions, exceptions et moyens de défense.

13. S'agissant du droit à la liberté d'expression en particulier, les personnes et les entreprises qui publient des informations à partir de leur pays de résidence ou d'établissement devraient en principe être tenues de ne respecter que la législation du pays en question. Quant aux personnes qui accèdent à des informations provenant de sites web étrangers, ou qui les téléchargent alors qu'elles pourraient ou devraient savoir que ces informations sont illégales dans leur pays de résidence, on peut estimer qu'elles devraient respecter la législation de ce pays. Mis à part les contenus qui sont illégaux en vertu du droit international, un Etat ne devrait exercer sa compétence sur

des informations numériques étrangères que dans des cas limités, notamment lorsqu'il existe un rapport clair et étroit entre l'Etat en question et les informations et/ou celui qui les diffuse.

V. Sur les droits de l'homme et les entités privées

14. Les Etats membres devraient cesser de s'appuyer sur des entreprises privées qui contrôlent l'internet et l'environnement numérique en général pour imposer des restrictions qui constituent une violation de leurs obligations en matière de droits de l'homme. A cet effet, il est nécessaire de donner des orientations générales indiquant dans quelles circonstances des actions ou des omissions d'entreprises privées contraires aux droits de l'homme engagent la responsabilité de l'Etat. Il s'agit notamment de définir des orientations générales sur le degré nécessaire d'implication de l'Etat dans la violation pour que sa responsabilité soit engagée et sur ses obligations de garantir que les conditions générales des entreprises privées ne sont pas en contradiction avec les normes relatives aux droits de l'homme. Il convient aussi d'examiner les responsabilités de l'Etat au regard des mesures prises par des parties privées à des fins commerciales et sans intervention directe de l'Etat.

15. Sur la base des Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme (Principes de Ruggie), il conviendrait de définir de nouvelles orientations générales sur les responsabilités des entreprises commerciales au regard de leurs activités sur (ou touchant à) l'internet ou dans l'environnement numérique en général, en particulier pour prendre en compte les cas où des entreprises risquent de devoir faire face à des demandes des pouvoirs publics susceptibles de porter atteinte au droit international en matière de droits de l'homme, ou risquent de s'être elles-mêmes placées dans des situations où elles pourraient fort bien devoir faire face à de telles demandes.

VI. Sur le blocage et le filtrage

16. Les Etats membres devraient veiller à ce que les restrictions d'accès à des contenus en ligne touchant des utilisateurs relevant de leur compétence reposent sur un cadre juridique, strict et prévisible, réglementant la portée de ces restrictions et offrant la garantie d'une contrôle judiciaire (ou d'un examen *a posteriori* en cas d'urgence authentique et incontestable) pour prévenir d'éventuels abus. De plus, les tribunaux internes doivent déterminer si une mesure de blocage est nécessaire, efficace et proportionnée, et en particulier si elle est suffisamment ciblée pour n'avoir d'incidence que sur le contenu spécifique dont le blocage est requis.

17. Les Etats membres ne devraient pas avoir recours à des acteurs privés qui contrôlent l'internet et l'environnement numérique en général, ni les encourager à effectuer un blocage en dehors d'un cadre répondant aux critères décrits ci-dessus.

VII. Sur les activités de sécurité nationale

18. La CEDH et la Convention n° 108 doivent être appliquées à toutes les activités des Etats parties à ces conventions, y compris les activités du pays en matière de renseignement et de sécurité nationale.

19. En particulier, pour parvenir au respect de la prééminence du droit sur l'internet et dans l'environnement numérique en général :

    - les Etats ne devraient être autorisés à invoquer la sécurité nationale pour justifier une atteinte aux droits de l'homme que si l'identité même et les fondements des institutions de la nation sont menacés ;
    - les Etats qui veulent poser des limites aux droits fondamentaux sur la base d'une menace supposée contre la sécurité nationale doivent apporter la preuve que la menace en question ne peut être contrée au moyen du droit pénal commun, notamment par des lois spéciales de lutte contre le terrorisme qui restent dans les limites admises du droit pénal et de procédure pénale applicables en temps de paix et qui satisfont aux normes internationales en matière de droit pénal et de procédure pénale ;
    - cette obligation s'applique également aux mesures prises par les Etats en lien avec l'internet et les communications électroniques.

20. Les Etats membres devraient inscrire les activités des agences de sécurité nationale et de renseignement dans un cadre juridique d'ensemble. Tant que les règles régissant le fonctionnement de ces services – en interne, à l'extérieur du territoire et/ou en coopération les uns avec les autres – ne sont pas plus transparentes, les activités de ces services ne peuvent pas être supposées conformes aux principes de prééminence du droit.

21. Les Etats membres devraient en outre veiller à ce que les services de sécurité nationale fassent l'objet d'un contrôle démocratique efficace. Pour cela, il convient de promouvoir une culture du respect des droits de l'homme et de la prééminence du droit, en particulier parmi les agents des services de sécurité.