GUIDE DES DROITS DE L'HOMME POUR LES UTILISATEURS D'INTERNET

Instruments juridiques

Recommandation CM/Rec(2014)6
et exposé des motifs

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Recommandation CM/Rec(2014)6
du Comité des Ministres aux Etats membres
sur un Guide des droits de l'homme pour les utilisateurs d'internet

(adoptée par le Comité des Ministres le 16 avril 2014,
lors de la 1197e réunion des Délégués des Ministres)

1. Les Etats membres du Conseil de l'Europe doivent reconnaître à toute personne relevant de leur juridiction les droits de l'homme et les libertés fondamentales définis par la Convention européenne des droits de l'homme (STE n° 5, la Convention). Cette obligation est valable également dans le contexte de l'utilisation d'internet. Les autres conventions et instruments du Conseil de l'Europe relatifs à la protection du droit à la liberté d'expression, de l'accès à l'information, du droit à la liberté de réunion, à la protection contre la cybercriminalité et à la protection du droit à la vie privée et des données à caractère personnel s'appliquent eux aussi dans ce contexte.

2. Les obligations des Etats en vue de respecter, de protéger et de promouvoir les droits de l'homme comprennent celle d'exercer un contrôle en ce sens sur les entreprises privées. Les droits de l'homme, universels et indivisibles, et les normes pertinentes en matière de droits de l'homme, priment sur les conditions générales d'utilisation imposées par les acteurs du secteur privé aux utilisateurs d'internet.

3. Internet a valeur de service public. Des personnes, des communautés, des institutions publiques et des organismes privés s'appuient sur internet pour mener leurs activités et sont en droit d'attendre des services en ligne qu'ils soient accessibles, fournis sans discrimination, abordables, sécurisés, fiables et continus. En outre, la jouissance des droits de l'homme et des libertés fondamentales des utilisateurs d'internet ne doit être soumise à aucune restriction illégale, inutile ou disproportionnée.

4. Les utilisateurs devraient pouvoir être aidés à comprendre et à exercer effectivement les droits de l'homme en ligne quand leurs droits et leurs libertés sont restreints ou entravés. Cela implique notamment qu'ils soient renseignés sur les voies de recours effectifs. Compte tenu des possibilités offertes par internet en matière de transparence et de responsabilité dans la gestion des affaires publiques, les utilisateurs devraient pouvoir utiliser internet comme outil de participation à la vie démocratique.

5. Pour garantir que les normes existantes en matière de droits de l'homme et de libertés fondamentales s'appliquent de la même façon en ligne et hors ligne, le Comité des Ministres recommande, conformément à l'article 15.*b* du Statut du Conseil de l'Europe que les Etats membres :

5.1. fassent activement la promotion du Guide des droits de l'homme pour les utilisateurs d'internet, tel qu'il figure en annexe, auprès des citoyens, des institutions publiques et des acteurs du secteur privé, et qu'ils prennent des mesures ciblées en vue de son application pour que les utilisateurs soient en mesure d'exercer pleinement leurs droits de l'homme et leurs libertés fondamentales en ligne ;

5.2. évaluent, examinent périodiquement et, le cas échéant, suppriment les restrictions à l'exercice des droits et libertés sur internet, notamment lorsque ces restrictions ne sont pas conformes à la Convention à la lumière de la jurisprudence pertinente de la Cour européenne des droits de l'homme. Toute restriction doit être prévue par la loi, nécessaire dans une société démocratique pour atteindre un but légitime et proportionnée au but légitime poursuivi ;

5.3. assurent aux utilisateurs d'internet l'accès à des recours effectifs en cas de restriction ou quand ils estiment que leurs droits sont violés, ce qui implique à la fois une coordination et une coopération renforcée entre les institutions, entités et communautés pertinentes. Cela implique également l'engagement d'une coopération active et efficace des acteurs du secteur privé et des organisations de la société civile. Selon le contexte national, cela peut inclure des dispositifs de recours tels que ceux mis en place par des autorités de protection des données, des institutions nationales de protection des droits de l'homme (tel le médiateur), des procédures judiciaires ou des services d'assistance téléphonique ;

5.4. promeuvent une coordination avec d'autres acteurs publics et non gouvernementaux, au sein et au-delà du Conseil de l'Europe, en ce qui concerne les normes et les procédures ayant des incidences sur la protection des droits de l'homme et des libertés fondamentales sur internet ;

5.5. encouragent le secteur privé à engager un véritable dialogue avec les pouvoirs publics pertinents et la société civile dans le cadre de l'exercice de la responsabilité sociale des entreprises, en particulier en matière de transparence et de responsabilité, conformément aux Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies. Le secteur privé devrait être également encouragé à contribuer à la diffusion du guide ;

5.6. encouragent la société civile à aider à la diffusion et à l'application du guide afin qu'il soit un outil efficace au service des utilisateurs d'internet.

Annexe à la Recommandation CM/Rec(2014)6

Introduction

1. Utilisateur d'internet, ce guide est fait pour vous aider à connaître vos droits de l'homme en ligne et leurs limites possibles, et les recours disponibles concernant ces limites. Les droits de l'homme et les libertés fondamentales ont la même valeur dans le monde virtuel que dans le monde réel. Ce principe implique un respect des droits et des libertés des autres utilisateurs d'internet. Vous trouverez dans ce guide des informations et des conseils pour comprendre leur signification dans la pratique dans les environnements internet, pour les affirmer et les exercer concrètement, et pour accéder à des recours. C'est un document évolutif qui sera périodiquement mis à jour.

2. Le guide se fonde sur la Convention européenne des droits de l'homme et d'autres conventions et instruments du Conseil de l'Europe qui concernent différents aspects de la protection des droits de l'homme. Tous les Etats membres du Conseil de l'Europe ont l'obligation de garantir le respect, la protection et la jouissance des droits et libertés énoncés dans les instruments qu'ils ont ratifiés. Le guide s'inspire en outre de l'interprétation continue de ces droits et libertés par la Cour européenne des droits de l'homme et dans d'autres instruments juridiques pertinents du Conseil de l'Europe.

3. Le guide n'instaure pas de nouveaux droits de l'homme ni de nouvelles libertés fondamentales. Il s'appuie sur les normes en vigueur et sur les mécanismes d'application existants[1].

Accès et non-discrimination

1. L'accès à internet est un moyen important pour exercer ses droits et ses libertés, ainsi que pour participer à la démocratie. C'est pourquoi votre accès à internet ne devrait pas être coupé contre votre volonté, hormis par décision judiciaire. Dans certains cas, des dispositions contractuelles peuvent aussi conduire à une interruption de service, mais cela ne devrait intervenir qu'en dernier ressort.

2. Votre accès à internet devrait être à un coût abordable. Il ne devrait pas être discriminatoire. Vous devriez avoir un accès aussi étendu que possible aux contenus, aux applications et aux services sur internet, en utilisant les équipements de votre choix.

3. Si vous vivez dans des zones rurales ou enclavées, si vous avez de faibles revenus ou si vous avez des besoins particuliers ou des handicaps, vous devriez attendre, de la part des pouvoirs publics, qu'ils fassent des efforts raisonnables et prennent des mesures spécifiques pour faciliter votre accès à internet.

4. Dans vos relations avec les pouvoirs publics, les fournisseurs d'accès à internet, les fournisseurs de contenus et de services en ligne, ou avec d'autres utilisateurs ou groupes d'utilisateurs, vous ne devez subir aucune discrimination sous quelque motif que ce soit, qu'elle se fonde sur le sexe, la race, la couleur, la langue, la religion ou les convictions, les opinions politiques ou autres, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance, l'appartenance ethnique, l'âge ou l'orientation sexuelle.

Liberté d'expression et d'information

Vous avez le droit de rechercher, d'obtenir et de communiquer les informations et les idées de votre choix, sans ingérence et sans considération de frontière. Cela signifie que :

1. vous avez le droit de vous exprimer en ligne et d'accéder à l'information et aux opinions et propos d'autres personnes. Ce droit s'applique également aux discours politiques, aux points de vue sur les religions et aux convictions et expressions accueillies favorablement ou considérées comme

[1]. Ce guide fait partie d'une recommandation qui a été adoptée par le Comité des Ministres des 47 Etats membres du Conseil de l'Europe. Les internautes pourront trouver plus d'informations sur le guide dans l'exposé des motifs de cette recommandation.

inoffensives mais aussi à celles qui peuvent heurter, choquer ou inquiéter autrui. Vous devriez tenir dûment compte de la réputation et des droits des autres, notamment de leur droit à la vie privée ;

2. des restrictions peuvent s'appliquer aux propos qui incitent à la discrimination, à la haine ou à la violence. Ces restrictions doivent alors entrer dans un cadre légal, être étroitement définies et appliquées sous contrôle judiciaire ;

3. vous êtes libres de créer, réutiliser et diffuser des contenus en respectant le droit à la protection de la propriété intellectuelle, y compris le droit d'auteur ;

4. les pouvoirs publics ont le devoir de respecter et de protéger votre liberté d'expression et votre liberté d'information. Les éventuelles restrictions à ces libertés ne doivent pas être arbitraires, elles doivent poursuivre un objectif légitime conforme à la Convention européenne des droits de l'homme, tel que, entre autres, la protection de la sécurité nationale ou de l'ordre public, de la santé publique ou de la morale, et elles doivent respecter la législation en matière de droits de l'homme. Elles doivent en outre vous être communiquées, être assorties d'informations sur les moyens d'obtenir des conseils et de demander réparation. Elles ne doivent pas être plus étendues ni maintenues plus longtemps que ce qui est strictement nécessaire pour atteindre un objectif légitime ;

5. votre fournisseur d'accès à internet et votre fournisseur d'accès aux contenus et aux services en ligne sont tenus, au titre de la responsabilité sociale des entreprises, de respecter vos droits de l'homme et de mettre à votre disposition des mécanismes pour répondre à vos réclamations. Vous devriez toutefois être conscient du fait que les fournisseurs de services en ligne, tels que les réseaux sociaux, peuvent appliquer des politiques de contenu qui imposent des restrictions à la diffusion de certains types de contenus et de comportements. Vous devriez être informé de ces restrictions possibles afin de pouvoir prendre des décisions éclairées sur le fait d'utiliser ou non le service en question. Cela comprend une information spécifique sur les contenus et les comportements que le fournisseur de services en ligne considère illicites et inappropriés dans le cadre de l'utilisation de ses services, ainsi que des modalités d'application mises en place par le fournisseur ;

6. vous devriez être libre de ne pas divulguer votre identité en ligne, par exemple en utilisant un pseudonyme. Toutefois, vous devriez être conscient que, même dans ce cas, les autorités nationales peuvent prendre des mesures conduisant à la révélation de votre identité.

Réunion, association et participation

Vous êtes libre de vous réunir et de vous associer pacifiquement avec d'autres personnes utilisant internet. Concrètement, cela signifie que :

1. vous êtes libre de choisir tout site web, toute application ou tout autre service pour constituer ou mobiliser un groupe de la société ou une association, pour y adhérer ou pour participer à ses activités, indépendamment du fait que cette entité soit ou non officiellement reconnue par les pouvoirs publics. Vous devriez pouvoir également utiliser internet afin d'exercer votre droit de constituer des syndicats et d'y adhérer ;

2. vous avez le droit d'émettre des protestations en ligne de manière pacifique. Vous devriez toutefois être conscient du fait que vous pouvez faire face à d'éventuelles conséquences judiciaires dans les cas où vos protestations en ligne entraîneraient des blocages, des interruptions de services ou des dommages aux biens d'autrui ;

3. vous êtes libre d'utiliser des outils en ligne disponibles pour participer aux débats publics au niveau local, national ou mondial, aux initiatives législatives et à l'observation citoyenne des processus décisionnels ; vous avez notamment le droit de signer des pétitions et de participer à l'élaboration des politiques de gestion d'internet.

Protection de la vie privée et des données personnelles

Vous avez droit au respect de la vie privée et familiale sur internet. Cela inclut la protection de vos données personnelles et le respect de la confidentialité de votre correspondance et de vos communications. Cela signifie que :

1. vous devriez être conscients du fait que, lorsque vous utilisez internet, vos données personnelles sont soumises à une série de traitements. Cela est notamment le cas lorsque vous naviguez sur internet, lorsque vous communiquez par courrier électronique, par messagerie instantanée ou par téléphonie sur internet ou encore lorsque vous utilisez des réseaux sociaux, des moteurs de recherche ou des services de stockage de données « dans un nuage » ;

2. les pouvoirs publics et les entreprises privées qui traitent vos données personnelles ont l'obligation de respecter des règles et des principes particuliers dans le cadre de ce traitement ;

3. le traitement de vos données personnelles devrait se limiter aux cas prévus par la loi ou auxquels vous avez consenti. Vous devriez disposer d'informations indiquant quelles sont les données personnelles traitées et/ou communiquées à des tiers, quand le traitement a lieu, par qui il est effectué et à quelles fins. En règle générale, vous devriez pouvoir exercer un contrôle sur vos données personnelles (vérifier leur exactitude, demander leur rectification, leur suppression, ou qu'elles ne sont pas conservées plus longtemps que nécessaire) ;

4. vous ne devez pas être soumis à des mesures générales de surveillance ou d'interception des communications. La loi n'autorise la violation de la confidentialité des données personnelles que dans des circonstances exceptionnelles, par exemple dans le cadre d'enquêtes pénales. Des informations accessibles, claires et précises devraient être mises à votre disposition pour vous permettre de connaître les règles et la législation en vigueur, ainsi que vos droits à cet égard ;

5. votre vie privée doit être respectée sur le lieu de travail également. Cela inclut la confidentialité de votre correspondance et de vos communications privées en ligne. Votre employeur est tenu de vous informer de toute éventuelle mesure de surveillance et/ou de suivi de sa part ;

6. vous pouvez obtenir de l'aide auprès des autorités de protection des données, qui existent dans la plupart des pays européens, pour vous assurer du respect des lois et des principes relatifs à la protection des données.

Education et connaissances générales

Vous avez un droit à l'instruction, y compris l'accès aux connaissances. Cela signifie que :

1. vous devriez avoir accès à l'éducation en ligne et aux contenus culturels, scientifiques, spécialisés et autres sur internet, dans les langues officielles. Un tel accès peut être soumis à des conditions liées à la rémunération des détenteurs de droits sur ces travaux. Vous devriez également pouvoir bénéficier d'un accès libre sur internet aux travaux de recherche et aux œuvres culturelles financés par des fonds publics, qui sont dans le domaine public, lorsqu'ils sont disponibles en version numérique ;

2. vous devriez avoir accès aux ressources d'éducation et de connaissance dans le domaine des technologies numériques dans le cadre de l'éducation à internet et aux médias, pour être en mesure d'exercer vos droits et vos libertés. Cela implique la capacité de comprendre, d'utiliser et d'exploiter une large gamme d'outils en ligne. Ces connaissances devraient vous permettre de porter un regard critique sur la justesse et la fiabilité des contenus, des applications ou des services auxquels vous accédez ou souhaitez accéder.

Enfants et jeunes

Les enfants et les jeunes jouissent de tous les droits et de toutes les libertés exposés dans ce guide. Si vous êtes un enfant ou un jeune, vous avez droit à une protection particulière et à un accompagnement spécifique lorsque vous naviguez sur internet. Cela signifie que :

1. vous avez le droit d'exprimer librement votre opinion, de participer à la société, d'être entendu et de contribuer aux prises de décision sur les affaires qui vous concernent. Vos opinions doivent être dûment prises en considération, eu égard à votre âge et à votre degré de maturité, et sans discrimination ;

2. vous pouvez vous attendre à recevoir des informations dans un langage adapté à votre âge et une formation de la part de vos enseignants, éducateurs, parents ou tuteurs sur les moyens d'utiliser internet sans risque, y compris sur la façon de protéger votre vie privée ;

3. vous devriez être conscients du fait que les contenus que vous créez sur internet, ou ceux créés par d'autres et qui vous concernent, peuvent être accessibles dans le monde entier et peuvent nuire à votre dignité, à votre sécurité et à votre vie privée, ou qu'ils peuvent avoir des répercussions négatives pour vous ou pour vos droits, aujourd'hui ou plus tard dans votre vie. Sur votre demande, ces contenus devraient être retirés ou supprimés dans un délai raisonnablement court ;

4. vous pouvez attendre des informations claires sur les contenus et les comportements interdits sur internet (par exemple le harcèlement en ligne) ainsi que sur la possibilité de signaler des contenus apparemment illicites. Cette information devrait être adaptée à votre âge et à votre situation ; et vous devriez pouvoir recevoir des conseils et de l'aide d'une manière qui respecte votre droit à la confidentialité et à l'anonymat ;

5. vous devriez bénéficier d'une protection spéciale contre les atteintes à votre bien-être physique, mental et moral, en particulier contre l'exploitation et les abus sexuels sur internet et d'autres formes de cybercriminalité. En particulier, vous avez le droit à l'éducation pour vous protéger de ces dangers.

Voies de recours

1. Vous avez droit à un recours effectif lorsque vos droits et vos libertés ont subi des restrictions ou des violations. Pour obtenir réparation, vous ne devriez pas nécessairement avoir à engager immédiatement une action en justice. Les voies de recours devraient être disponibles, connues, accessibles, abordables et permettre d'obtenir une réparation appropriée. Un recours effectif devrait pouvoir être obtenu directement auprès des fournisseurs d'accès à internet, des pouvoirs publics et/ou des institutions nationales des droits de l'homme. En fonction de la violation subie, un recours effectif peut entraîner une enquête, des explications, une réponse, une rectification, des excuses, le rétablissement d'un statut, le rétablissement d'une connexion ou une réparation. Dans la pratique, cela signifie que :

1.1. votre fournisseur d'accès à internet, les fournisseurs d'accès aux contenus et aux services en ligne, ou les autres entreprises concernées et/ou les pouvoirs publics devraient vous informer de vos droits, de vos libertés, des recours possibles et des moyens de les obtenir. Des informations expliquant comment signaler d'éventuelles atteintes à vos droits, comment porter plainte et comment demander réparation devraient être facilement accessibles ;

1.2. des informations complémentaires et des conseils devraient être mis à disposition par les pouvoirs publics, les institutions nationales des droits de l'homme (tel le médiateur), les autorités de protection des données, les services d'aide aux particuliers, les associations de protection des droits de l'homme ou des droits numériques, ou les organisations de défense des consommateurs ;

1.3. les pouvoirs publics nationaux ont le devoir de vous protéger contre les activités criminelles et les infractions pénales commises sur internet ou par l'utilisation d'internet, en particulier en cas d'accès illicite, d'intrusion, de falsification ou autre manipulation frauduleuse concernant votre identité numérique, votre ordinateur ou les données qu'il contient. Les autorités en charge de l'application de la loi, compétentes dans votre pays, ont le devoir d'enquêter et de prendre des mesures appropriées si vous portez plainte pour des dommages ou une ingérence dans votre identité ou de votre propriété en ligne, et veiller à ce que des sanctions soient prises.

2. Dans le cadre de toute procédure destinée à établir vos droits et obligations ou le bien-fondé de toute accusation portée contre vous au pénal en rapport avec l'utilisation d'internet :

2.1. vous avez droit à un procès équitable, dans un délai raisonnable, par un tribunal indépendant et impartial ;

2.2. vous avez un droit de recours individuel devant la Cour européenne des droits de l'homme après épuisement de toutes les voies de recours internes disponibles.

COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Documents CM

CM(2014)31 addfinal 16 avril 2014[1]

Recommandation CM/Rec(2014)6 du Comité des Ministres aux Etats membres sur un guide des droits de l'homme pour les utilisateurs d'internet – Exposé des motifs

Introduction

1. Internet joue un rôle important dans la vie quotidienne des individus et dans tous les aspects de la société humaine. Il évolue en permanence et offre aux citoyens des possibilités d'accéder à des informations et des services, de se connecter et de communiquer, ainsi que de partager des idées et des connaissances, et ce à l'échelle planétaire. L'impact d'internet sur les activités sociales, économiques et culturelles ne cesse également d'augmenter.

2. Un nombre croissant d'affaires en relation avec internet sont soumises à la Cour européenne des droits de l'homme[2] (la Cour). La Cour a d'ailleurs affirmé que « [L]'internet est aujourd'hui devenu l'un des principaux moyens d'exercice par les individus de leur droit à la liberté d'expression et d'information : on y trouve des outils essentiels de participation aux activités et débats relatifs à des questions politiques ou d'intérêt public. »[3]

3. La Stratégie du Conseil de l'Europe sur la gouvernance de l'internet 2012-2015 attache une grande importance aux droits des usagers de l'internet. La ligne d'action « Renforcer au maximum les droits et les libertés des usagers de l'internet », qui vise à promouvoir l'accès à internet et son bon usage, englobe entre autres mesures : « l'élaboration d'un compendium des droits de l'homme garantis aux utilisateurs de l'Internet afin de leur permettre de communiquer avec les acteurs principaux de ce dernier et les instances publiques compétentes et de disposer d'un recours effectif quand ils estiment que leurs droits et libertés sont remis en cause : signaler un incident, déposer une plainte, demander réparation ou un droit de réponse, ou accéder à une autre voie de recours ».

Genèse et contexte

4. Le Comité directeur sur les médias et la société de l'information (CDMSI), à sa 1ère réunion tenue du 27 au 30 avril 2012, a proposé au Comité des Ministres la création d'un Comité d'experts sur les droits des usagers d'internet (MSI-DUI) et défini son mandat. A la suite de la proposition du CDMSI, le Comité des Ministres a adopté son mandat à la 1147e réunion des Délégués des Ministres le 6 juillet 2012.[4] Aux termes de son mandat, le résultat attendu des travaux du MSI-DUI est le suivant :

> *« Un inventaire des droits de l'homme en vigueur dont jouissent les usagers d'internet est préparé, afin de les aider à comprendre et à exercer leurs droits lorsque, considérant qu'il a été porté atteinte à leurs droits et libertés, ils communiquent avec les principaux acteurs d'internet et les organismes publics et recherchent auprès d'eux une voie de recours efficace (2013) » (ci-après l'Inventaire).*

[1] Ce document a été classé en diffusion restreinte jusqu'à la date de son examen par le Comité des Ministres.
[2] Pour un aperçu de la jurisprudence de la Cour européenne des droits de l'homme, consulter la fiche thématique sur les nouvelles technologies, octobre 2013. http://echr.coe.int/Documents/FS_New_technologies_FRA.pdf.
[3] Voir Yildirim c. Turquie, n° 3111/10, § 54.
[4] Voir CM(2012)91.

5. Le MSI-DUI a tenu sa première réunion les 13 et 14 septembre 2012 à Strasbourg. Il a été convenu que l'objectif des travaux du MSI-DUI ne devrait pas être celui de mettre en place de nouveaux droits de l'homme, mais d'examiner l'application des droits existants aux environnements en ligne. Le MSI-DUI a décidé de rassembler des informations, au moyen d'un questionnaire envoyé à ses réseaux et communautés, sur les problèmes pratiques rencontrés par les usagers et, de ce fait, les éventuelles violations des droits de l'homme ainsi que les voies de recours disponibles.

6. Des consultations avec les partenaires ont eu lieu lors du Forum sur la gouvernance de l'internet (6-9 novembre 2012, Bakou) dans le cadre de l'atelier sur l'autonomisation des utilisateurs d'internet (« Empowerment of Internet Users – which tools? »). Les membres présents du MSI-DUI ont mis à profit les possibilités d'échanges offertes par cet événement pour solliciter l'avis des partenaires sur différents sujets présentant un intérêt pour l'Inventaire. Les discussions de l'atelier ont attiré l'attention sur plusieurs problèmes rencontrés par les usagers d'internet, comme la suppression de contenus créés par des usagers sans procédure régulière, la protection des données à caractère personnel et le manque de recours effectifs.

7. Le MSI-DUI a tenu sa deuxième réunion les 13 et 14 décembre 2012 à Strasbourg. Il a examiné les réponses renvoyées à son questionnaire et discuté des informations collectées par le biais de ses échanges avec les divers partenaires. Le MSI-DUI a décidé de mettre un point final à la phase analytique préliminaire de son travail et, sur cette base, de démarrer la rédaction de l'Inventaire ; un premier jet a été présenté à l'occasion de cette réunion.

8. A sa troisième réunion, qui s'est tenue les 20 et 21 mars 2013 à Strasbourg, le MSI-DUI a examiné en détail les questions en relation avec le droit à la liberté d'expression, le droit au respect de la vie privée, la liberté de réunion et d'association et la sécurité en ligne, le droit à l'éducation, les droits de l'enfant, la non-discrimination et le droit à un recours effectif. Cet examen a été conduit à la lumière des normes contraignantes et non contraignantes du Conseil de l'Europe et de la jurisprudence de la Cour européenne des droits de l'homme. Le MSI-DUI a également réfléchi au type d'instrument que le Conseil de l'Europe pourrait adopter pour approuver l'Inventaire, comme une déclaration ou une recommandation du Comité des Ministres. L'instrument devrait satisfaire à un double objectif, à savoir fournir aux utilisateurs d'internet des conseils simples et clairs sur leurs droits de l'homme en ligne et garantir l'adoption par les Etats membres d'un texte qui soit conforme aux obligations qui leur incombent au titre de la Convention européenne des droits de l'homme (CEDH) et d'autres instruments du Conseil de l'Europe.

9. Le CDMSI, à sa troisième réunion tenue du 23 au 26 avril 2013 à Strasbourg, a considéré que l'Inventaire devait parvenir à associer un jargon formel et un langage simplifié, en évitant toute simplification excessive des normes en vigueur concernant les droits de l'homme et la jurisprudence de la Cour européenne des droits de l'homme. Les discussions ont aussi mis en lumière le souhait que l'Inventaire soit actualisé régulièrement de manière à refléter comme il se doit les politiques relatives à internet, qui évoluent rapidement. Le CDMSI a également décidé de soumettre des commentaires sur le projet d'Inventaire, dans son état d'avancement au moment des consultations, précisant qu'il s'agit d'un document « en cours d'élaboration » destiné à fournir des orientations et des conseils généraux. Les réponses reçues viennent à l'appui de l'approche choisie par le MSI-DUI, à savoir préparer un document de sensibilisation facile d'emploi, qui mette l'accent sur le droit à la liberté d'expression, le droit au respect de la vie privée, le droit à l'éducation, les droits de l'enfant et la protection contre la cybercriminalité.

10. Le projet d'Inventaire a été présenté pour discussion avec les partenaires dans le cadre du Dialogue européen sur la gouvernance de l'internet (EuroDIG, 20-21 juin 2013 à Lisbonne), notamment lors de l'atelier dédié aux règles, droits et responsabilités de notre cyber-environnement (« Towards a Human Internet? Rules, Rights and Responsibilities for our Online Future »). Une réunion informelle des membres du MSI-DUI présents à l'atelier s'est tenue à Lisbonne. Il en est ressorti que le projet d'Inventaire devait être raccourci dans l'objectif d'être plus accessible aux utilisateurs. Suite à ces discussions, et aux travaux entre les réunions du MSI-DUI, une réunion ad hoc a rassemblé les membres du MSI-DUI disponibles le 10 septembre 2013 à Strasbourg. Le MSI-DUI a examiné un projet de recommandation du Comité des Ministres sur les droits de l'homme des utilisateurs d'internet, qui inclut dans son annexe un projet d'Inventaire sur les droits de l'homme et les libertés fondamentales pour les utilisateurs d'internet. L'angle choisi pour ce projet d'Inventaire étant

de s'adresser directement à l'utilisateur, il a été décidé de rebaptiser l'Inventaire « Guide des droits de l'homme pour les utilisateurs d'internet ».

11. A sa dernière réunion tenue les 1er et 2 octobre 2013 à Strasbourg, le MSI-DUI a examiné et finalisé ses propositions au CDMSI d'un projet de recommandation du Comité des Ministres sur un guide des droits de l'homme pour les utilisateurs d'internet (ci-après le Guide). Il a convenu d'organiser des consultations multipartenaires, dont un forum public du Conseil de l'Europe sur le Guide durant le Forum sur la gouvernance de l'internet (22-25 octobre 2013, Indonésie). Plusieurs partenaires choisis, représentant le secteur privé, la société civile et les milieux techniques et universitaires, ont été invités à soumettre leurs commentaires et suggestions sur le Guide. De plus, d'autres comités directeurs pertinents du Conseil de l'Europe ont été sollicités pour des observations et des réactions informelles sur le projet de recommandation, et notamment le Comité directeur pour les droits de l'homme (CDDH), le Comité européen de coopération juridique (CDCJ), le Comité européen pour les problèmes criminels (CDPC), ainsi que des comités conventionnels dont le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), le Comité de la Convention sur la cybercriminalité (T-CY*)*, le Comité d'experts sur le terrorisme (CODEXTER) et le Comité des parties à la Convention sur la protection des enfants contre l'exploitation et les abus sexuels (T-ES). Le CDDH, le CDCJ ainsi que les membres du Bureau du T-PD ont transmis leurs commentaires qui ont été pris en considération et intégrés par le CDMSI dans le projet de Recommandation et le projet d'exposé des motifs correspondant.

12. Par ailleurs, près de trente contributions ont été reçues, provenant de différentes régions du monde et de représentants du secteur privé (compagnies de télécommunication et fournisseurs d'accès à Internet), d'organisations de la société civile, de la communauté technique et du monde académique. Ces contributions saluaient pour la plupart les travaux du Conseil de l'Europe sur le projet de guide et contenaient des commentaires et propositions de changement au projet.

13. Le CDMSI, à sa 4e réunion tenue du 3 au 6 décembre 2013, a examiné les propositions du MSI-DUI concernant un projet de recommandation du Comité des Ministres aux Etats membres sur un guide des droits de l'homme pour les utilisateurs d'internet. Il a pris note des consultations précitées avec les diverses parties prenantes et a finalisé le projet de recommandation sur la base des commentaires finaux envoyés par email.

Commentaires sur la Recommandation CM/Rec(2014)6 du Comité des Ministres aux Etats membres sur un guide des droits de l'homme pour les utilisateurs d'internet

14. L'objectif de cette recommandation est de promouvoir l'exercice et la protection des droits de l'homme et des libertés fondamentales sur internet dans l'ensemble des Etats membres du Conseil de l'Europe. L'accès des individus et des communautés à internet, et une meilleure utilisation de ce média, requièrent la mise en œuvre d'efforts pour les informer et leur donner les moyens d'exercer pleinement leurs droits et leurs libertés dans les environnements en ligne. Cet objectif a été affirmé par la Déclaration du Comité des Ministres sur des principes de la gouvernance de l'internet de 2011, qui souligne sa vision d'une approche d'internet basée sur les droits de l'homme et centrée sur les individus pour donner aux utilisateurs les moyens d'exercer leurs droits et leurs libertés sur internet, et qui constitue un principe de gouvernance d'internet.

15. Le Guide, qui est annexé à cette recommandation, donne quelques informations de référence sur des droits de l'homme choisis de la CEDH, ainsi que d'autres normes pertinentes du Conseil de l'Europe. Il met l'accent sur des droits et libertés spécifiques ainsi que les normes de droit international liées, concernant notamment le droit à la liberté d'expression, à la liberté de réunion et d'association, le droit au respect de la vie privée et protection des données personnelles, les droits de l'enfant et le droit à un recours effectif. Il a été rédigé en un langage accessible aux utilisateurs. Afin de conserver sa simplicité au texte, le MSI-DUI a décidé de ne pas faire référence au langage juridique strict relatif aux obligations des Etats membres en droit international, incluant la jurisprudence de la Cour

16. Les droits de l'homme et les libertés fondamentales sont garantis par divers instruments du Conseil de l'Europe qui s'appliquent aux environnements en ligne et hors ligne, et de ce fait pas exclusivement à internet. Les droits de l'homme et les libertés fondamentales sont notamment consacrés par la CEDH, telle qu'elle est interprétée par la Cour dans sa jurisprudence. Plusieurs

conventions et d'autres instruments non contraignants du Conseil de l'Europe fournissent des explications et orientations complémentaires aux utilisateurs d'internet. Le MSI-DUI a estimé qu'il été nécessaire, afin de permettre aux utilisateurs d'internet de mieux comprendre leurs droits et libertés, d'expliquer dans un langage simple les normes pertinentes de droit international du Conseil de l'Europe et des Nations Unies.

Préambule

17. Le préambule énonce les raisons qui ont conduit le Comité des Ministres à adopter la recommandation à ses Etats membres. L'hypothèse de la recommandation est que la responsabilité de protéger les droits de l'homme et les libertés fondamentales incombe aux Etats membres du Conseil de l'Europe, et ce, conformément à la CEDH telle qu'interprétée par la Cour européenne des droits de l'homme. D'autres instruments juridiquement contraignants du Conseil de l'Europe s'appliquent également, et notamment la Convention sur la cybercriminalité (ci-après la « Convention de Budapest »), la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201, ci-après la « Convention de Lanzarote ») et la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108, ci-après la « Convention 108 »).

18. D'autres normes non contraignantes adoptées par le Comité des Ministres fournissent aux Etats membres des orientations sur les questions relatives à internet, et notamment : la Recommandation CM/Rec(2007)16 du Comité des Ministres aux Etats membres sur des mesures visant à promouvoir la valeur de service public d'internet ; la Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet ; la Recommandation CM/Rec(2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage ; la Recommandation CM/Rec (2011)7 du Comité des Ministres aux Etats membres sur une nouvelle conception des médias ; la Recommandation CM/Rec(2012)4 du Comité des Ministres aux Etats membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux ; et la Recommandation CM/Rec(2012)3 du Comité des Ministres aux Etats membres sur la protection des droits de l'homme dans le contexte des moteurs de recherche.

19. Le deuxième paragraphe du préambule spécifie que les obligations des Etats en vue de respecter, de protéger et de promouvoir les droits de l'homme comprennent celle d'exercer un contrôle en ce sens sur les entreprises privées. Cette affirmation découle de l'article 1 de la CEDH, en vertu duquel les Etats membres doivent reconnaître à toute personne relevant de leur juridiction les droits et libertés définis dans la Convention. Cela inclut la protection contre les violations des droits de l'homme par les acteurs non étatiques et exige d'adopter des mesures appropriées pour empêcher ces atteintes, et lorsqu'elles se produisent, d'enquêter à leur sujet, d'en punir les auteurs et de les réparer par le biais de lois et de mesures. La Cour a affirmé dans ses arrêts que les Etats ont pour obligation positive la protection des droits et des libertés fondamentales des individus sur internet, et plus précisément la liberté d'expression,[5] la protection des enfants et des jeunes,[6] la protection de la moralité et des droits des autres,[7] la lutte contre les discours racistes ou xénophobes, contre la discrimination et la haine raciale[8]. En outre, la Cour a jugé que la responsabilité des Etats était engagée pour n'avoir pas protégé leurs citoyens des incidences préjudiciables sur leurs droits et libertés découlant d'actes d'entreprises privées.[9] Le deuxième paragraphe souligne aussi le principe de l'indivisibilité et l'universalité des droits de l'homme en s'appuyant sur la Déclaration de Vienne proclamée lors du sommet conférence de chefs d'Etat et de gouvernement des Etats membres du Conseil de l'Europe qui a eu lieu le 9 octobre 1993.

[5] Voir Özgür Gündem c. Turkey, n° 23144/93, § 42-46.
[6] K.U. c. RU, n° 2872/02.
[7] Pay c. RU, n° 32792/05.
[8] Féret c. Belgique n°15615/07.
[9] López Ostra c. Espagne, n° 16798/90, § 44-58; Taşkin et Autres c. Turquie; Fadeyeva c. la Fédération de Russie. Dans l'affaire Khurshid Mustafa et Tarzibachi c. Suède n° 23883/06, la Cour européenne des droits de l'homme a conclu que l'interprétation par une juridiction nationale d'un acte privé (contrat) engageait la responsabilité de l'Etat défendeur, en élargissant le champ de la protection prévue par l'article 10 à des restrictions imposées par des personnes privées.

20. Le troisième paragraphe du préambule réaffirme la valeur de service public d'internet énoncée dans la Recommandation CM/Rec(2007)16.[10] Considérant le rôle important que joue internet dans les activités quotidiennes des utilisateurs et la nécessité de garantir leurs droits sur internet, la recommandation souligne que les utilisateurs ne doivent pas subir de restriction illégale, non-nécessaire et disproportionnée dans l'exercice de leurs droits et libertés.

21. Le quatrième paragraphe du préambule définit l'objectif de la recommandation d'aider les utilisateurs à comprendre et exercer effectivement leurs droits de l'homme en ligne, y compris l'accès à des recours effectifs. Informer les utilisateurs des risques qui pèsent sur leurs droits et libertés fondamentales, et sur leurs possibilités en matière de recours, est donc important. L'affirmation concernant les possibilités offertes par internet en matière de transparence et de responsabilité dans la gestion des affaires publiques indique que l'un des objectifs de la recommandation est de donner aux individus et aux communautés la possibilité de participer à la vie démocratique.

Dispositif de la recommandation

22. Le paragraphe 5 affirme un principe essentiel des normes du Conseil de l'Europe relatives à la gouvernance d'internet est que les droits de l'homme et les libertés fondamentales s'appliquent de manière égale dans les environnements en ligne et hors ligne[11]. Cette approche a également été affirmée par le Conseil des droits de l'homme des Nations Unies dans sa Résolution de 2012 sur « La promotion, la protection et la jouissance des droits de l'homme sur l'internet ». La promotion de l'application du Guide viendra par conséquent renforcer la protection des droits de l'homme et des libertés fondamentales, conformément aux normes existantes en matière de droits de l'homme.

23. Le sous-paragraphe 5.1, contient une recommandation aux Etats membres sur la promotion du Guide que devrait être assurée non seulement par les institutions publiques, mais également par le secteur privé. Cette promotion pourrait inclure la publication du Guide, mais également sa diffusion sur des supports imprimés ou des adaptations en format électronique. Les autorités publiques concernées pourraient aussi le mettre en ligne sur leurs sites web. Le secteur privé pourrait être encouragé à faire de même.

24. Le sous-paragraphe 5.2, réaffirme que l'exercice des droits de l'homme et des libertés fondamentales sur internet peut faire l'objet de restrictions poursuivant un but légitime et nécessaires dans une société démocratique, ainsi que le prévoient les articles pertinents de la CEDH. Pour garantir le respect de ces conditions, le Comité des Ministres recommande à ses Etats membres d'évaluer, d'examiner périodiquement et, le cas échéant, de supprimer les restrictions à l'exercice des droits de l'homme et des libertés fondamentales sur internet.

25. Le sous-paragraphe 5.3, appelle les Etats membres à intensifier leurs efforts pour assurer le droit à un recours effectif, notamment en promouvant une coordination et une coopération renforcée entre des institutions, des entités (par exemple les autorités de régulation des communications électroniques) et des communautés en ce qui concerne le traitement des plaintes déposées par les utilisateurs d'internet. La recommandation reconnaît également qu'il existe dans les Etats membres une grande diversité de dispositifs de recours, comme les autorités de protection des données, les médiateurs, les procédures judiciaires ou encore les permanences téléphoniques. Les Etats membres pourraient aussi procéder à une évaluation des dispositifs en place dans leur juridiction et rassembler les informations pertinentes dans un inventaire des mécanismes de recours qui soit facile d'utilisation. De telles informations pourraient être diffusées en accompagnement du Guide, par exemple sous la forme d'une annexe. Ceci peut constituer une des actions de suivi qui pourraient être prises une fois la Recommandation adoptée.

26. De par sa nature, internet fonctionne par l'envoi et la réception de demandes d'information à travers les frontières, et donc sans considération des frontières. Cela signifie que, dans les Etats membres, les droits de l'homme et les libertés fondamentales sur internet peuvent être exposés aux agissements d'acteurs étatiques et non étatiques par-delà les frontières du Conseil de l'Europe. La liberté d'expression et l'accès à l'information, ainsi que le respect du caractère privé des données

[10] Recommandation CM/Rec(2007)16 du Comité des Ministres aux Etats membres sur des mesures visant à promouvoir la valeur de service public de l'Internet.
[11] Voir la Déclaration du Comité des Ministres sur des principes de la gouvernance de l'internet, principe 1 « Droits de l'homme, démocratie et Etat de droit ».

personnelles peuvent par conséquent faire l'objet d'ingérences. Par conséquent, le sous-paragraphe 5.4, recommande une coordination entre les Etats membres et non membres du Conseil de l'Europe, ainsi qu'avec les acteurs non étatiques.

27. Au sous-paragraphe 5.5, conscient que cela est nécessaire, le Comité des Ministres recommande aux Etats membres d'encourager le secteur privé à s'engager dans un véritable dialogue concernant l'exercice de la responsabilité sociale des entreprises avec les pouvoirs publics pertinents ainsi que avec la société civile. Un principe fondamental des Principes directeurs relatifs aux entreprises et aux droits de l'homme[12] est que les entreprises devraient respecter les droits de l'homme, autrement dit qu'elles doivent éviter de porter atteinte aux droits de l'homme d'autrui et prendre des mesures contre les incidences préjudiciables sur les droits de l'homme dans lesquelles elles sont impliquées. La transparence et l'obligation des acteurs du secteur privé de rendre des comptes sont mises en avant comme des moyens essentiels de faire la preuve de leur responsabilité, tout comme leur active promotion du Guide et sa diffusion. Les fournisseurs d'accès à internet et les fournisseurs de contenus pourraient par exemple faire référence au Guide dans les conditions générales d'utilisation de leurs services.

28. Le sous-paragraphe 5.6, du dispositif reconnaît le rôle majeur que peut jouer la société civile dans la promotion du Guide et la surveillance du respect de ses dispositions. Il en découle la recommandation aux Etats membres de encourager les organisations de la société civile et les activistes pourraient aider à la diffusion et à l'application du Guide, et l'utiliser comme outil pour prôner la mise en œuvre des normes en matière de droits de l'homme et leur respect.

Annexe à la Recommandation CM/Rec(2014)6

Introduction

29. Le Guide s'adresse directement à l'utilisateur. Il est un outil pour tous ceux qui ne possèdent pas les connaissances spécialisées sur internet qui peuvent être acquises au moyen de l'enseignement ou de la formation. Il est notamment axé sur la capacité de l'utilisateur à gérer ses activités sur internet (par exemple, son identité et ses données personnelles). L'utilisateur doit être pleinement informé au sujet des choix qu'il peut faire sur internet, avec des répercussions éventuelles sur ses droits et libertés, et des conséquences découlant du consentement donné à ces choix. Il doit pouvoir comprendre les limitations imposées à ses droits et avoir connaissance des dispositifs de recours à sa disposition.

30. Le Guide se fonde sur la CEDH et la jurisprudence de la Cour européenne des droits de l'homme. Il s'appuie aussi sur d'autres normes juridiquement contraignantes du Conseil de l'Europe. D'autres instruments sont également pris en considération, et notamment certaines déclarations et recommandations du Comité des Ministres. Le Guide est sans préjudice de l'applicabilité des instruments juridiques sur lesquels il se fonde. Les droits et libertés énoncés dans le Guide s'appliquent en vertu des instruments juridiques sur la base desquels ils ont été définis. Le Guide se réfère aux normes en vigueur en matière de droits de l'homme et aux mécanismes d'application existants et ne proclame pas de nouveaux droits de l'homme ni de nouvelles libertés fondamentales. Le Guide n'est pas un recueil exhaustif des normes en matière de droits de l'homme, pas plus qu'il n'en fournit une explication normative. De plus amples clarifications sur les restrictions et ingérences aux droits de l'homme, ainsi que des orientations sur l'aide à apporter aux utilisateurs en matière de violence et d'abus sur internet, mériteraient notamment d'être examinées afin de permettre aux utilisateurs de mieux comprendre leurs droits et de se protéger, ainsi que de protéger les autres.

[12] Principes directeurs relatifs aux entreprises et aux droits de l'homme : mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations Unies (A/HRC/17/31), adoptés par le Conseil des droits de l'homme par la Résolution « Les droits de l'homme et les sociétés transnationales et autres entreprises » A/HRC/RES/17/4. Les principes directeurs prévoient en particulier que les Etats sont tenus d'appliquer des lois tendant à exiger des entreprises qu'elles respectent les droits de l'homme, ou qui ont cet effet, et, périodiquement, d'évaluer la validité de ces lois et de combler les éventuelles lacunes ; de faire en sorte que les autres lois et politiques régissant la création et l'exploitation courante des entreprises, comme le droit des sociétés, n'entravent pas mais favorisent le respect des droits de l'homme par ces entités ; de fournir des orientations effectives aux entreprises sur la manière de respecter les droits de l'homme dans toutes leurs activités ; d'inciter les entreprises à faire connaître la façon dont elles gèrent les incidences de leur activité sur les droits de l'homme, et de les y contraindre, le cas échéant.

Toutefois, le Guide pourra être mise à jour pour suivre les nouvelles normes du Conseil de l'Europe et la jurisprudence de la Cour à mesure que la technologie évolue.

Accès et non-discrimination

31. Le Guide met en avant les principes et considérations qui sont jugés intrinsèquement liés et généralement applicables à l'ensemble des droits de l'homme et des libertés fondamentales qu'il contient, y compris l'accès à internet et le principe de non-discrimination.

32. Bien que l'accès à internet ne soit pas encore formellement reconnu comme étant un droit de l'homme (des différences étant à noter dans les contextes nationaux, y compris au niveau de la législation interne et des politiques), il est considéré comme étant une condition essentielle et un catalyseur de la liberté d'expression et d'autres droits et libertés[13]. Par conséquent, le fait de couper l'accès à internet d'un utilisateur pourrait avoir des effets préjudiciables sur l'exercice de ses droits et libertés, voire être assimilé à une restriction de son droit à la liberté d'expression, y compris le droit de recevoir et de communiquer des informations. La Cour a déclaré qu'internet est devenue l'un des moyens principaux de l'exercice du droit à la liberté d'expression et d'information. La liberté d'expression ne s'applique pas seulement aux contenus de l'information, mais également aux moyens de sa diffusion, dans la mesure où toute restriction imposée à cette dernière porte nécessairement atteinte au droit de recevoir et de communiquer des informations. De telles ingérences sont acceptables sous réserve uniquement de répondre aux conditions énoncées à l'article 10, paragraphe 2 de la CEDH, tel qu'interprété par la Cour.[14] Une mesure susceptible d'influer sur l'accès des individus à internet engage la responsabilité de l'État en vertu de l'article 10.[15]

33. Dans ce contexte, le Guide affirme que l'accès à internet des utilisateurs ne devrait pas être coupé contre leur volonté, hormis par décision judiciaire. Toutefois, cela ne doit pas être compris comme empêchant l'exercice légitime de mesures de déconnexion telles que celles découlant d'obligations contractuelles. Les consommateurs ne s'acquittant pas du règlement du coût du service peuvent voir leur accès à internet interrompu. Une telle mesure devrait néanmoins être de dernier ressort. Les enfants peuvent par ailleurs se voir privés de l'accès à internet au titre de l'exercice de l'autorité parentale sur l'utilisation faite d'internet, selon l' âge et le degré de maturité de l'enfant concerné.

34. Les utilisateurs d'internet devraient disposer de voies de recours effectives contre les mesures de déconnexion à internet lorsqu'elles n'ont pas été décidées par un tribunal. Cela implique que les fournisseurs de services à internet informent leurs utilisateurs des motifs et des fondements juridiques des mesures de déconnexion et des procédures permettant de contester de telles mesures et de réclamer le rétablissement du plein accès à l'internet. Ces demandes devraient être traitées dans un délai raisonnable. Qui plus est, tout utilisateur d'internet, dans l'exercice de son droit à un jugement équitable, devrait pouvoir demander un réexamen des mesures de déconnexion par une autorité administrative et/ou judiciaire compétente. Ces aspects de la procédure régulière sont résumés dans la dernière section du Guide, intitulée « Voies de recours ».

35. Les actions ou mesures positives qui peuvent être prises par les pouvoirs publics pour garantir que tout un chacun soit connecté à internet est un autre aspect de la question de l'accès à internet. Le Comité des Ministres du Conseil de l'Europe a recommandé à ses Etats membres de promouvoir la valeur de service public d'internet.[16] Celle-ci est comprise comme étant « le fait pour les

[13] Le Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, a souligné qu'internet est devenu un outil indispensable pour combattre les inégalités, pour accélérer le développement, pour permettre à l'homme de s'accomplir, pour faciliter l'accès à l'information, mais aussi permettre la participation active des citoyens dans la construction d'une société démocratique. Assurer un accès universel à l'Internet devrait donc devenir une priorité pour tous les États. Tout Etat devrait donc développer une politique concrète et efficace, en consultation avec tous les segments de la société, y compris le secteur privé et les ministères gouvernementaux concernés, afin de faire en sorte qu'internet soit largement disponible, accessible et abordable pour tous. « En tant que catalyseur de l'exercice du droit à la liberté d'opinion et d'expression, Internet facilite la réalisation de bien d'autres droits de l'homme. » http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf .

[14] Voir note 2 ci-dessus, § 50. Voir aussi Autronic AG c. Suisse (n+ 12726/87). Dans l'affaire Khurshid Mustafa et Tarzibachi c. Suède n° 23883/06, la Cour européenne des droits de l'homme a conclu que l'interprétation par une juridiction nationale d'un acte privé (contrat) engageait la responsabilité de l'Etat défendeur, en élargissant le champ de la protection prévue par l'article 10 à des restrictions imposées par des personnes privées.

[15] Voir note 2 ci-dessus, § 53.

[16] Voir note 9 ci-dessus, CM/Rec(2007)16, section II.

personnes de compter de manière significative sur l'Internet comme un outil essentiel pour leurs activités quotidiennes (communication, information, savoir, transactions commerciales) et de l'attente légitime qui en découle que les services de l'Internet soient accessibles et abordables financièrement, sécurisés, fiables et continus ». Cette section informe l'utilisateur qu'il doit pouvoir bénéficier d'un accès à internet qui soit abordable et non discriminatoire.

36. La teneur du droit d'accéder à internet est liée au droit de recevoir et de transmettre des informations sur internet, comme mentionné dans l'article 10 de la CEDH.[17] Le Comité des Ministres du Conseil de l'Europe a affirmé que tous les usagers d'internet devraient avoir le plus large accès possible à tout contenu, application ou service de leur choix sur internet, qu'ils leur soient offerts ou non à titre gratuit, en choisissant les appareils jugés les plus appropriés de leur choix. Il s'agit d'un principe général habituellement appelé « neutralité de réseau » qui devrait s'appliquer quels que soient l'infrastructure ou le réseau utilisés pour la connexion internet.[18]

37. Les pouvoirs publics devraient fournir des efforts raisonnables pour faciliter l'accès à internet par des catégories spécifiques d'individus, comme les personnes vivant dans des zones isolées ou les personnes handicapées. Cela se fonde sur le principe du service communautaire universel énoncé dans la Recommandation Rec(99)14 sur le service universel communautaire relatif aux nouveaux services de communication et d'information.[19] Le Guide souligne que les utilisateurs vivant dans des zones rurales ou enclavées, ou encore à faibles revenus ou avec des besoins particuliers ou des handicaps doivent pouvoir attendre des pouvoirs publics qu'ils prennent des mesures spéciales pour faciliter leur accès à internet.

38. Les attentes de personnes atteintes de handicap de bénéficier d'un accès équivalent et non discriminatoire à celui dont jouissent les autres utilisateurs d'internet découlent d'instruments du Conseil de l'Europe qui recommandent aux Etats membres de prendre des mesures pour promouvoir la fourniture d'équipements adaptés pour l'accès à internet et aux TIC par les personnes handicapées[20]. Les Etats membres devraient promouvoir un accès abordable en gardant à l'esprit l'importance de la conception, du besoin de sensibiliser ces personnes ou groupes de personnes, du caractère approprié, attractif, adaptable et compatible des accès et services internet.[21]

39. Le principe de non-discrimination devrait s'appliquer aux relations des usagers avec les pouvoirs publics, les fournisseurs d'accès à internet, les fournisseurs de contenus et de services en ligne et d'autres sociétés, les utilisateurs ou groupes d'utilisateurs. Le paragraphe 4 paraphrase l'article 14 de la CEDH et l'article 1 du Protocole 12 de la CEDH, qui concernent tous deux l'interdiction de la discrimination.

Liberté d'expression et d'information

40. Cette section concerne le droit à la liberté d'expression tel que consacré par l'article 10 de la CEDH. La Cour a affirmé dans sa jurisprudence que l'article 10 est pleinement applicable à internet.[22] Le droit à la liberté d'expression inclut le droit d'exprimer librement ses opinions, ses visions et ses idées et de rechercher, recevoir et de communiquer des informations sans considération des frontières. Les utilisateurs d'internet devraient être libres d'exprimer leurs opinions politiques ainsi que leurs convictions religieuses et non religieuses. Ce dernier point correspond à l'exercice du droit à la liberté de pensée, de conscience et de religion tel que consacré par l'article 9 de la CDEH. Le droit à la liberté d'expression vaut non seulement pour les informations ou idées reçues avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent.[23]

[17] Voir note 2 ci-dessus, § 50.
[18] Déclaration du Comité des Ministres sur la neutralité du réseau, adoptée par le Comité des Ministres le 29 septembre 2010. Voir aussi la Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, article 8(4)g.
[19] Voir note 9 ci-dessus, CM/Rec(2007)16, annexe, section II ; Recommandation No. R (99)14 sur le service universel communautaire relatif aux nouveaux services de communication et d'information, principe 1.
[20] Ibid.
[21] Voir note 9 ci-dessus, CM/Rec(2007)16, annexe, section II.
[22] Voir note 2 ci-dessus, § 50.
[23] Handyside c. le Royaume-Uni, arrêt du 7 décembre 1976, série A, n° 24, § 49.

41. Il doit y avoir un juste équilibre entre l'exercice du droit à la liberté d'expression et d'information par les utilisateurs d'internet et le droit à la protection de la réputation. La Cour a affirmé dans plusieurs affaires qu'il s'agit d'un droit protégé par l'article 8 de la CEDH qui concerne le droit au respect de la vie privée.[24] La Cour a conclu que, par principe, les droits garantis en vertu des articles 8 et 10 devaient faire l'objet d'un même respect. S'agissant de la mise en balance du droit à la liberté d'expression et du droit au respect de la vie privée, les critères qui s'avèrent pertinents sont les suivants : la contribution à un débat d'intérêt général, la notoriété de la personne visée et l'objet du reportage, le comportement antérieur de la personne concernée, le mode d'obtention des informations et leur véracité, le contenu, la forme et les répercussions de la publication, et la gravité de la sanction imposée.[25] C'est pourquoi le Guide spécifie que l'utilisateur d'internet devrait tenir dûment compte de la réputation d'autrui, notamment de leur droit à la vie privée.

42. Le discours de haine, en revanche, est une forme d'expression qui ne peut bénéficier de la protection de l'article 10 de la CEDH. La Cour a jugé que certaines formes d'expression qui incitent à la haine ou nient les valeurs fondamentales de la CEDH sont exclues des protections prévues à l'article 10 de ladite Convention.[26] En la matière, la Cour applique l'article 17 de la CEDH. Bien qu'il n'existe pas de définition universellement acceptée du discours de haine, le Comité des Ministres du Conseil de l'Europe a affirmé que l'expression « discours de haine » couvre toutes les formes d'expression qui propagent, incitent à, promeuvent ou justifient la haine raciale, la xénophobie, l'antisémitisme ou d'autres formes de haine fondées sur l'intolérance, y compris l'intolérance qui s'exprime sous forme de nationalisme agressif et d'ethnocentrisme, de discrimination et d'hostilité à l'encontre des minorités, des immigrés et des personnes issues de l'immigration.[27] Le deuxième paragraphe de la section sur la liberté d'expression offre aux utilisateurs des informations concises formulées en langage simple sur la question d'application de l'Article 10 de la CEDH aux discours d'haine. Ce paragraphe n'essaye pas d'expliquer en des termes juridiques les applications différentes de l'article 10 et l'article 17 de la CEDH car on considère que cela serait plus approprie d'être inclus dans l'exposé des motifs de la recommandation en raison du caractère juridique de cette distinction.

43. Les utilisateurs ont le droit d'obtenir et de communiquer des informations sur internet, et notamment de créer des contenus, ainsi que de réutiliser et de diffuser des contenus en se servant d'internet. La Cour a examiné la relation entre la protection de la propriété intellectuelle et la liberté d'expression en relation à des affaires de condamnation pénale pour violation du droit d'auteur. La Cour a considéré ces condamnations comme des ingérences dans l'exercice du droit à la liberté d'expression qui, pour se justifier, doivent être prévues par la loi, poursuivre le but légitime de protéger les droits des autres et être considérées comme nécessaires dans une société démocratique.[28] Le partage ou le fait d'autoriser autrui à partager des fichiers sur internet, même des matériels protégés par le droit d'auteur ou à des fins commerciales, sont couverts par le droit de recevoir et de communiquer des informations, comme le prévoit l'article 10 de la CEDH.[29] Ce droit n'étant pas absolu, il convient de mettre en balance d'une part l'intérêt de partager des informations et, d'autre part, l'intérêt de protéger les droits du détenteur des droits d'auteur. La Cour a souligné que la propriété intellectuelle bénéficie de la protection accordée par l'article 1 du Protocole 1 à la CEDH. Il s'agit donc de mettre en balance deux intérêts concurrents protégés par la CEDH.

44. La recommandation du Comité des Ministres à ses Etats membres de promouvoir la valeur de service public d'internet inclut des conseils spécifiques sur les mesures et les stratégies concernant la liberté de communication et la création sur internet, indépendamment des frontières. Il conviendrait notamment de prendre des mesures pour faciliter, le cas échéant, les « réutilisations » de contenus, autrement dit l'utilisation de ressources numériques existantes, pour créer d'autres contenus ou services d'une façon compatible avec le respect des droits de propriété intellectuelle.[30]

[24] Chauvy et Autres, n° 64915/01, § 70; Pfeifer c. Autriche, n° 12556/03, § 3 ; et Polanco Torres et Movilla Polanco c. Espagne, n° 34147/06, § 40.
[25] Delfi As c. Estonie, n° 64569/09, § 78-81 (l'affaire a été renvoyée devant la Grande Chambre de la Cour); Axel Springer AG c. Allemagne n° 39954/08, § 89-95 et Von Hannover c. Allemagne (n° 2), n° 40660/08 et 60641/08, § 108-113.
[26] Féret c. Belgique n° 15615/07; Garaudy c. France n° 65831/01, 24.06.2003, décision de recevabilité; Leroy c. France n° 36109/03; Jersild c. Danemark n° 15890/89; Vejdeland et Autres c. Suède (n° 1813/07).
[27] Recommandation No. R (97) 20 du Comité des Ministres aux Etats membres sur le « discours de haine ».
[28] Neij et Sunde Kolmisoppi c. Suède n° 40397/12. Voir aussi Ashby Donald et Autres c. France, n° 36769/08, § 34.
[29] Ibid.
[30] Voir CM/Rec(2007)16, annexe, section III, deuxième tiret.

45. Le paragraphe 4 fournit un aperçu des conditions que les restrictions de la liberté d'expression doivent respecter. Les Etats membres ont une obligation première, en vertu de l'article 10 de la CEDH, de ne pas entraver la communication d'information entre les individus, qu'il s'agisse de personnes physiques ou morales. La Cour a affirmé que l'exercice effectif du droit à la liberté d'expression peut également requérir des mesures positives de protection, y compris dans la sphère des relations entre individus. La responsabilité de l'Etat peut être engagée s'il n'édicte pas la législation interne appropriée.[31] Une violation de la CEDH peut également être établie dans le cas où l'interprétation par une juridiction nationale d'un acte juridique, qu'il s'agisse d'un contrat privé, d'un document public, d'une disposition statutaire ou d'une pratique administrative, apparaitrait abusive, arbitraire, discriminatoire ou, plus globalement, incohérente avec les principes sous-jacents de la CEDH.[32]

46. La liberté d'expression, parce qu'elle n'est pas un droit absolu, peut faire l'objet de restrictions. Les ingérences dans la liberté d'expression doivent être considérées comme toute forme de restriction émanant d'une autorité exerçant des attributions publiques ou de la fonction publique, comme les tribunaux, les bureaux des procureurs, la police, tout organe chargé de l'application de la loi, les services de renseignement, les conseils au niveau local ou central, les services gouvernementaux, les instances décisionnelles de l'armée et les structures professionnelles publiques.

47. Conformément à l'article 10, paragraphe 2 de la CEDH, toute ingérence doit être prévue par la loi. Cela signifie que la loi doit être accessible, claire et suffisamment précise pour permettre aux individus de réguler leurs comportements. La loi doit aussi prévoir des garanties suffisantes contre les mesures restrictives abusives, y compris un contrôle effectif par un tribunal ou un autre organe de règlement indépendant.[33] Toute ingérence doit aussi poursuivre un but légitime dans l'intérêt de la sécurité nationale, de l'intégrité territoriale ou de la sécurité publique, de la prévention des troubles à l'ordre public et de la criminalité, de la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire. Cette liste est exhaustive, mais son interprétation et sa portée évoluent avec la jurisprudence de la Cour. Une ingérence doit également être nécessaire dans une société démocratique, ce qui signifie qu'il faut prouver qu'elle correspond à un besoin social impérieux, qu'elle poursuit un but légitime et qu'elle représente le moyen le moins restrictif d'y parvenir.[34] Ces conditions doivent être résumées dans un langage compréhensible par l'utilisateur, autrement dit toute restriction à la liberté d'expression ne doit pas être arbitraire et doit poursuivre un objectif conforme à la CEDH tels que, entre autre, la protection de la sécurité nationale ou de l'ordre public, de la santé publique ou de la morale et doit respecter la législation en matière de droits de l'homme.

48. Des informations plus détaillées sur des garanties que doivent être apportées aux utilisateurs d'internet en cas de restrictions au droit à la liberté d'expression en ligne sont présentées dans les paragraphes suivantes de l'exposé des motifs de la recommandation. Le blocage et le filtrage sont des exemples de restrictions qui peuvent être assimilées à des violations de la liberté d'expression. Cela est basé sur des principes généraux établis par la Cour ainsi que d'autres normes pertinentes adoptées par le Comité des Ministres.[35]

49. Des mesures générales de blocage ou de filtrage ne devraient être prises par les pouvoirs publics que si le filtrage concerne un contenu spécifique et clairement identifiable, sur la base d'une décision au sujet de l'illégalité de ce contenu prise par une autorité nationale compétente et qui peut être réexaminée par un tribunal ou une entité de régulation indépendante et impartiale, en accord avec les dispositions de l'article 6 de la CEDH.[36] Les pouvoirs publics devraient veiller à ce que tous les filtres soient évalués avant et pendant leur mise en œuvre, afin de vérifier que les effets du filtrage sont en adéquation avec l'objectif de la restriction et donc justifiés dans une société démocratique, afin d'éviter tout blocage injustifié des contenus.[37]

---

[31] Vgt Verein gegen Tierfabriken c. Suisse, n° 24699/94, § 45.
[32] Voir Khurshid Mustafa et Tarzibachi c. Suède n° 23883/06 § 33; Plaand Puncernau c. Andorre, n° 69498/01, § 59, ECHR 2004-VIII
[33] Voir note 2 ci-dessus, § 64.
[34] Ibid., § 66-70.
[35] Recommandation CM/Rec(2008)6 sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet, voir annexe, partie III, ii. Voir aussi, note 1 ci-dessus.
[36] Ibid. CM/Rec(2008)6, voir annexe, partie III, iv.
[37] Ibid.

50. Les mesures prises pour bloquer un site précis ne doivent pas être utilisées arbitrairement comme moyen d'opérer un blocage général de l'information sur internet. Elles ne doivent pas avoir pour effet collatéral de rendre inaccessibles de grandes quantités d'informations, restreignant ce faisant substantiellement les droits des utilisateurs.[38] Elles doivent être prévues par la loi. Il devrait y avoir une surveillance stricte de la portée du blocage et un contrôle juridictionnel effectif afin d'éviter tout abus de pouvoir.[39] Le contrôle juridictionnel d'une telle mesure devrait évaluer les intérêts concurrents en jeu, ménager un équilibre entre eux et déterminer si une mesure de moins grande portée pourrait être envisagée pour bloquer l'accès à un contenu spécifique d'internet.[40] Les obligations et principes susmentionnés n'empêchent pas l'installation de filtres pour la protection des mineurs, notamment dans des endroits où les mineurs ont accès à internet tels que les écoles ou les bibliothèques.[41]

51. Le filtrage et la désindexation de contenus internet par des moteurs de recherche comportent le risque de violer la liberté d'expression des utilisateurs. Les moteurs de recherche ont la liberté d'explorer et d'indexer les informations diffusées sur internet. Ils ne devraient pas être tenus d'exercer un contrôle proactif de leurs réseaux et services afin de déceler un éventuel contenu illicite et ne devraient pas non plus réaliser des activités préalables de filtrage ou de blocage sans qu'il leur soit ordonné de le faire par une ordonnance judiciaire ou par une autorité compétente. La désindexation ou le filtrage de sites web spécifiques à la demande des pouvoirs publics devraient être transparents, étroitement ciblés et réexaminés à intervalles réguliers sous réserve du respect du droit à une procédure régulière.[42]

52. Cette section identifie également quelques-unes des garanties qu'il faudrait assurer aux utilisateurs lorsque des restrictions s'appliquent, en insistant notamment sur les informations à leur fournir et sur les possibilités de remettre ces restrictions en question. Cela est mentionné dans la recommandation du Comité des Ministres sur les mesures relatives au blocage et aux filtres internet.[43] Les utilisateurs d'internet devraient recevoir des informations indiquant quand le filtrage a été activé et expliquant pourquoi tel ou tel contenu a été filtré, afin qu'ils puissent comprendre comment et selon quels critères le filtrage opère (par exemple listes noires, listes blanches, blocage de mots clés, classement du contenu, désindexation ou filtrage de certains sites web ou contenus spécifiques par les moteurs de recherche). Ils devraient aussi recevoir des conseils clairs et concis sur le contournement manuel d'un filtre actif, à savoir l'instance à contacter quand le blocage d'un contenu s'avère injustifié et les motifs qui peuvent autoriser le contournement d'un filtre pour un type spécifique de contenu ou d'URL. Les utilisateurs devraient également disposer de voies de recours et de réparation facilement accessibles, y compris la suspension des filtres lorsque l'utilisateur affirme qu'un contenu a été bloqué de façon injustifiée.

53. Il est possible que des sociétés, comme les réseaux sociaux, suppriment des contenus créés et mis à disposition par des utilisateurs d'internet. Ces sociétés peuvent aussi désactiver le compte d'utilisateurs (par exemple, le profil d'un utilisateur ou sa présence sur les réseaux sociaux) en justifiant leur décision par le non-respect des conditions générales d'utilisation de leurs services. De telles mesures peuvent constituer une ingérence dans le droit à la liberté d'expression et celle de recevoir ou de communiquer des informations, à moins que ne soient réunies les conditions prévues à l'article 10, paragraphe 2, telles qu'interprétées par la Cour européenne des droits de l'homme.[44]

54. Conformément aux Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme (qui ne sont pas un instrument contraignant en soi), les entreprises ont en effet une responsabilité de respecter les droits de l'homme, ce qui les oblige à éviter d'engendrer ou de contribuer à des incidences négatives sur les droits de l'homme, et à prévoir ou à collaborer au redressement de telles incidences. Par contre, l'obligation de protéger et d'assurer un accès à un

[38] Voir note 2 ci-dessus, § 52; 66- 68. Déclaration sur la liberté de communication sur l'Internet, Comité des Ministres.
[39] Ibid., § 64. Association Ekin c. France, n° 39288/98.
[40] Ibid., § 64-66.
[41] Voir Déclaration sur la liberté de communication sur l'Internet, principe 3.
[42] Voir Recommandation CM/Rec(2012)3 du Comité des Ministres aux Etats membres sur la protection des droits de l'homme dans le contexte des moteurs de recherche, annexe, partie III.
[43] Voir CM/Rec(2008)6, voir annexe, partie I; Ibid., CM/Rec(2012)3, annexe, partie III.
[44] Recommandation CM/Rec (2011)7 du Comité des Ministres aux Etats membres sur une nouvelle conception des médias, § 7, annexe, § 15; 44-47; 68 -69 ; Recommandation CM/Rec(2012)4 du Comité des Ministres aux Etats membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux, § 3.

recours effectif incombe essentiellement aux Etats. Cela a été évoqué par le paragraphe 5 de section sur la liberté d'expression. La responsabilité sociale des fournisseurs de services en ligne englobe l'engagement à lutter contre les propos haineux et d'autres contenus incitant à la violence ou à la discrimination. Les fournisseurs de services en ligne devraient porter une attention particulière à l'utilisation, et à leur réaction à de tels propos d'un point de vue éditorial, d'expressions à caractère raciste, xénophobe, antisémite, misogyne, sexiste (y compris à l'égard des personnes LGBT) ou autre.[45] Ces fournisseurs devraient également aider les utilisateurs à signaler tout contenu ou opinion et/ou comportement pouvant être considérés illicites.[46]

55. Le Guide alerte les utilisateurs d'internet sur le fait que les fournisseurs de services en ligne qui hébergent des contenus créés par les utilisateurs peuvent exercer différents niveaux de contrôle éditorial sur le contenu de leurs services.[47] Sans préjudice de leur indépendance éditoriale, ils devraient faire en sorte que le droit des utilisateurs d'internet de rechercher, de recevoir et de diffuser des informations ne soit pas bafoué, en vertu de l'article 10 de la CEDH.[48] Cela signifie que toute restriction appliquée à des contenus générés par les utilisateurs devrait être spécifique, justifiée pour permettre la restriction et communiquée à l'utilisateur concerné.

56. L'utilisateur d'internet devrait pouvoir prendre une décision éclairée sur le fait d'utiliser ou non le service en ligne. Dans la pratique, l'utilisateur devrait être pleinement informé de toute mesure prévue concernant la suppression de contenus créés par lui ou la désactivation de son compte, avant que celle-ci ne soit prise[49]. L'utilisateur d'internet devrait avoir accès à des informations claires et précises (formulées dans une langue qu'il comprenne) sur les faits et motifs motivant la prise de mesures pour la suppression d'un contenu et la désactivation d'un compte. Cela inclut les dispositions juridiques sur lesquelles elles sont basées ainsi que d'autres éléments utilisés pour évaluer la proportionnalité et la légitimité du but visé. Il devrait aussi pouvoir demander un réexamen de la décision de supprimer un contenu et/ou de désactiver un compte, dans un délai raisonnable et assorti de la possibilité de porter plainte contre la décision auprès d'une autorité judiciaire et/ou administrative compétente.

57. Le sixième sous-paragraphe concerne la question de l'anonymat. Celle-ci se fonde sur la jurisprudence de la Cour européenne des droits de l'homme, la Convention de Budapest et d'autres instruments du Comité des Ministres. La Cour a examiné la question de la confidentialité des communications sur internet dans une affaire où un État membre du Conseil de l'Europe a manqué à son obligation d'obliger un fournisseur de service internet à révéler l'identité d'une personne qui avait publié une annonce indécente concernant un mineur sur un site de rencontres par internet. La Cour a estimé que, bien que la liberté d'expression et la confidentialité des communications soient des considérations primordiales, et que les utilisateurs de télécommunications et de services sur internet doivent avoir la garantie que leur intimité et leur liberté d'expression sont respectées, cette garantie ne peut être absolue et doit parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui. L'État a l'obligation positive de prévoir un cadre permettant de concilier les différents intérêts à protéger dans ce contexte.[50]

58. La Convention de Budapest ne pénalise pas l'utilisation des technologies informatiques aux fins de communications anonymes. Selon son rapport explicatif, « la modification des données de trafic aux fins de faciliter les communications anonymes (comme dans le cas des activités des systèmes de réexpédition anonyme) ou la modification des données aux fins d'assurer la protection des communications (chiffrement, par exemple) sont considérées comme assurant la protection légitime de la vie privée et, de ce fait, sont considérées comme étant réalisées de façon légitime. Toutefois, les Parties [à la Convention] peuvent incriminer certains actes abusifs se rapportant aux

[45] Ibid., CM/Rec(2011)7, § 91.
[46] Ibid., CM/Rec(2012)4, II/10.
[47] Ibid., CM/Rec(2011)7, § 18; 30-31.
[48] Ibid., CM/Rec(2011)7, § 7, 2e tiret.
[49] Voir le rapport intitulé : « *Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users* », de Erica Newland, Caroline Nolan, Cynthia Wong et Jillian York, disponible à: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Final_Report_on_Account_Deactivation_and_Content_Removal.pd.f
[50] K.U. c. Finlande, n° 2872/02, § 49.

communications anonymes, comme dans le cas de la falsification des données d'un en-tête de paquet visant à dissimuler l'identité de l'auteur d'une infraction ».[51]

59. Le Comité des Ministres du Conseil de l'Europe a affirmé le principe de l'anonymat dans sa Déclaration sur la liberté de la communication sur l'internet.[52] En conséquence, afin d'assurer une protection contre les surveillances en ligne et de favoriser l'expression libre d'informations, les Etats membres du Conseil de l'Europe devraient respecter la volonté des usagers d'internet de ne pas révéler leur identité. Toutefois, le respect de l'anonymat n'empêche pas les Etats membres de prendre des mesures pour retrouver la trace de ceux qui sont responsables d'actes délictueux, conformément à la législation nationale, à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et aux autres traités internationaux dans le domaine de la justice et de la police.

Réunion, association et participation

60. Le droit à la liberté de réunion et d'association est inscrit dans la Convention européenne des droits de l'homme (article 11). Il renvoie aussi aux principes établis par la Cour européenne des droits de l'homme concernant la protection du discours politique, qui prévoient notamment une marge d'appréciation réduite en vertu de l'article 10, paragraphe 2 de la CEDH, pour les restrictions aux discours politiques ou aux débats sur des questions d'intérêt public.[53]

61. L'utilisateur d'internet a le droit de se réunir et de s'associer pacifiquement avec d'autres personnes en utilisant internet. Cela inclut le fait de constituer, de rejoindre, de mobiliser et de participer à des groupes de la société ou des associations ou des syndicats en utilisant les outils mis à disposition par internet. Cela inclut par exemple la signature d'une pétition pour participer à une campagne, ou toute autre forme d'action civique. L'utilisateur devrait avoir la liberté de choisir les outils lui permettant d'exercer ses droits, comme des sites web, des applications ou d'autres services. L'exercice de ce droit n'est pas conditionné à la reconnaissance formelle de ces groupes ou associations par les pouvoirs publics.

62. Le droit d'émettre des protestations s'applique également en ligne et hors ligne. Les protestations qui ont des conséquences pour le grand public, comme des perturbations ou des blocages d'accès à des bâtiments, entrent dans le cadre de l'exercice de la liberté de réunion conformément à l'article 11 de la CEDH. Toutefois, il peut y avoir des exceptions, notamment lorsque de telles actions provoquent des interruptions de services en ligne, comme l'accès non autorisé à un site web particulier ou à un espace en ligne en accès restreint, ou la manipulation de contenus numériques sans autorisation. Enfin, il est important d'informer l'utilisateur que des protestations en ligne qui engendreraient des perturbations peuvent ne pas être aussi librement acceptées.

63. Internet est devenu un outil grâce auquel les citoyens peuvent participer activement à la construction et au renforcement de sociétés démocratiques. Le Comité des Ministres a recommandé aux Etats membres de concevoir et de mettre en œuvre des stratégies de démocratie en ligne, de participation et d'administration en ligne en utilisant les technologies de l'information et de la communication (TIC) dans les débats et processus démocratiques, dans les relations entre les pouvoirs publics et la société civile, mais aussi dans la fourniture de services publics.[54]

64. Cela inclut la liberté de participer aux débats publics au niveau local, national ou mondial, aux initiatives législatives et à l'observation citoyenne des processus décisionnels, y compris le droit de signer des pétitions au moyen le cas échéant de l'utilisation des TIC. La base en est les recommandations du Comité des Ministres à ses Etats membres d'encourager l'utilisation des TIC par les citoyens (notamment les forums en ligne, blogues, débats politiques en ligne, messageries instantanées et autres formes de communication entre citoyens) pour engager des débats démocratiques, des actions militantes et des campagnes en ligne, faire valoir leurs préoccupations, leurs idées et leurs initiatives, promouvoir le dialogue et la délibération avec des représentants et le gouvernement, et pour contrôler l'action des fonctionnaires et des responsables politiques sur les questions d'intérêt public.

[51] Convention de Budapest sur la cybercriminalité, article 2, rapport explicatif, § 62.
[52] Voir Déclaration sur la liberté de communication sur l'Internet, principe 7.
[53] Wingrove c. Royaume-Uni, 25 novembre 1996, § 58, rapports 1996-V.
[54] Voir CM/Rec(2007)16, annexe, partie I.

Protection de la vie privée et des données personnelles

65. Le droit au respect de la vie privée et familiale est garanti par l'article 8 de la Convention européenne des droits de l'homme. Ce droit a ensuite été interprété par la jurisprudence de la Cour, et complété et renforcé par la Convention 108.

66. La notion de vie privée ne se prête pas à une définition exhaustive. La Cour a souligné que l'article 8 englobe un large éventail d'intérêts, et notamment le droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance, y compris par courrier électronique, téléphone[55] et courriels sur le lieu de travail. Le droit au respect de la vie privée fait référence au droit de la personne à son image,[56] par exemple au moyen de photographies ou de clips vidéo. Il englobe aussi le droit à l'identité et au développement personnel, le droit de nouer et de développer des relations avec ses semblables. Les activités de nature professionnelles ou commerciales sont également incluses.[57]

67. De nombreuses activités des utilisateurs d'internet impliquent une forme ou une autre de traitement automatisé des données à caractère personnel, et notamment : l'utilisation de navigateurs, du courrier électronique, de la messagerie instantanée ou de la téléphonie sur internet, de protocoles, des réseaux sociaux, des moteurs de recherche ou de services de stockage de données « dans les nuages » (« cloud computing »). La Convention 108 couvre toutes les opérations effectuées sur internet, comme la collecte, le stockage, l'altération, l'effacement, et la récupération ou la diffusion de données à caractère personnel.[58]

68. Il existe des règles et des principes qui doivent être respectés par les pouvoirs publics et par les entreprises impliquées dans le traitement des données à caractère personnel. Il est nécessaire que l'utilisateur soit conscient et comprenne quelles sont les données personnelles traitées et comment, et s'il peut prendre des mesures à ce sujet, par exemple pour demander la rectification ou la suppression des données. En vertu de la Convention 108, les données à caractère personnel doivent être obtenues et traitées loyalement et licitement, et enregistrées pour des finalités déterminées et légitimes. Elles doivent être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, exactes et si nécessaire mises à jour, conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées.[59]

69. L'accent est placé sur deux principes spécifiques du traitement des données personnelles : la licéité du traitement et le consentement [explicite] de l'utilisateur. L'utilisateur doit être informé que les données ne peuvent être traitées que dans les cas prévus par la loi ou auxquels il a consenti, par exemple en acceptant les conditions d'utilisation d'un service sur internet.

70. Le consentement libre, spécifique, éclairé et explicite (non-équivoque) de la personne concernée pour le traitement de ses données sur internet est actuellement en discussion en vue de son intégration dans la Convention 108.[60] Le consentement éclairé est évoqué dans la Recommandation CM/Rec(2012)4 du Comité des Ministres aux Etats membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux. Les services de réseaux sociaux, en particulier, devraient demander le consentement éclairé des utilisateurs lorsqu'ils souhaitent diffuser ou partager leurs données avec d'autres catégories de personnes ou d'entreprises ou les utiliser à des finalités autres que celles spécifiées lors de leur collecte initiale. Pour obtenir le consentement des usagers, ils devraient pouvoir obtenir qu'ils consentent à élargir l'accès par des tiers à leurs données personnelles (par exemple, lorsque des applications tierces sont exploitées sur le réseau social). De la même façon, les utilisateurs devraient pouvoir retirer leur consentement.

[55] Klass et Autres c. Allemagne, n° 5029/71, § 41.
[56] Von Hannover c. Allemagne (n° 2), n° 40660/08 et 60641/08, § 108-113 ; Sciacca c. Italie, n° 50774/99, § 29.
[57] Rotaru c. Roumanie (n° 28341/95); P.G. et J.H. c. RU (n° 44787/98); Peck c. RU (n° 44647/98); Perry c. RU (n° 63737/00); Aman c. Suisse (n° 27798/95).
[58] Voir Convention 108, article 2.
[59] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n°108, art. 8).
[60] Le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel (STCE n°108) a fait plusieurs propositions pour moderniser cette convention (T-PD(2012)4Rev3_en). L'une de ces propositions met l'accent sur le consentement de la personne dont les données personnelles sont traitées en tant que condition préalable à ce traitement. « Chaque Partie prévoit que le traitement de données ne peut être effectué que si la personne concernée a donné son consentement de manière [explicite, non- équivoque], spécifique, libre et éclairée, ou si ce traitement est prévu par le droit. ».

71. Il est important de noter la Recommandation CM/Rec(2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage. Il s'agit en l'occurrence d'une technique de traitement automatisé des données qui consiste à appliquer un « profil » à une personne physique, notamment afin de prendre des décisions à son sujet ou d'analyser ou de prévoir ses préférences, comportements et attitudes personnels. Par exemple, les données personnelles d'un usager d'internet peuvent être collectées et traitées dans le contexte de son interaction avec un site web ou une application ou encore dans celui des activités de navigation au fil du temps sur différents sites (par exemple, en collectant des informations sur les pages et contenus visités, l'heure des visites, l'objet des recherches, ce qui a été cliqué). Les « cookies » sont l'un des moyens employés pour suivre les activités de navigation des usagers, en stockant et récupérant des informations sur un périphérique de ce dernier. La Recommandation envisage le droit des utilisateurs d'internet à donner leur consentement pour l'utilisation des données à caractère personnel aux fins de profilage, ainsi que le droit de retirer leur consentement.[61]

72. Le droit à l'information des utilisateurs d'internet concernant le traitement de leurs données personnelles est mentionné dans plusieurs instruments du Conseil de l'Europe. La Convention 108 prévoit que la personne concernée puisse connaître l'existence du traitement de ses données personnelles par toute personne physique ou morale, les principales finalités du traitement, ainsi que l'identité et la résidence habituelle ou le principal établissement de l'entité de traitement, et obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'enregistrement ou non de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible.[62]

73. Il est également fait référence à l'information des utilisateurs dans la Recommandation CM/Rec(2012)4 du Comité des Ministres aux Etats membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux. Les utilisateurs d'internet sur les réseaux sociaux devraient être informés dans un langage clair et compréhensible de tout changement apporté aux conditions générales d'utilisation des services des fournisseurs. Cela concerne d'autres actions, comme l'installation d'applications tierces qui comportent un risque pour le droit au respect de la vie privée des utilisateurs ; la loi qui s'applique aux services des réseaux sociaux et au traitement de leurs données à caractère personnel ; les conséquences d'un accès illimité à leurs profils et communications (dans le temps et géographiquement), en particulier en expliquant clairement la différence entre communication privée et communication publique, ainsi que les conséquences de rendre une information publiquement disponible, y compris l'accès sans restriction à leurs données par des tiers ; et la nécessité d'obtenir le consentement préalable d'autres personnes avant de publier des données à caractère personnel sur elles, y compris des contenus audio et vidéo, dans les cas où ils ont élargi l'accès des informations au-delà du cercle restreint des contacts qu'ils ont eux-mêmes sélectionnés. Les utilisateurs d'internet doivent aussi recevoir des informations spécifiques sur la logique qui sous-tend le traitement des données à caractère personnel pour son profilage et les finalités du profilage.

74. Les utilisateurs d'internet devraient pouvoir exercer un contrôle sur leurs données personnelles, comme l'expose la Convention 108, et notamment faire valoir leur droit de rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit, et leur droit de disposer d'un recours s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement, comme évoqué précédemment.[63]

75. La Recommandation CM/Rec(2012)3 du Comité des Ministres aux Etats membres relative à la protection des droits de l'homme dans le contexte des moteurs de recherche fait référence à plusieurs mesures que peuvent prendre les fournisseurs pour protéger la vie privée de leurs utilisateurs. Cela inclut la protection des données à caractère personnel contre tout accès illicite de tiers à ces dernières et des mécanismes appropriés de notification des cas de violation de sécurité des données. Ces mesures devraient comprendre le cryptage de bout en bout (end-to-end) des communications entre utilisateurs et fournisseurs de moteurs de recherche. La corrélation croisée des données provenant de différents services/plateformes appartenant à un fournisseur de moteurs de

[61] Recommandation CM/Rec(2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, section 5.
[62] Convention 108, article 8.
[63] Ibid, article 8.

recherche ne doit être possible que sous réserve d'un consentement non-équivoque de l'utilisateur pour ce service particulier. Les utilisateurs doivent pouvoir avoir accès, corriger ou effacer les données les concernant qui ont été collectées pendant l'utilisation des services, y compris tout profil créé à des fins de marketing direct par exemple.[64]

76. Les réseaux sociaux devraient aussi apporter leur aide aux utilisateurs pour la gestion et la protection de leurs données, en particulier au moyen de :

- *la configuration des paramètres par défaut de leur profil*, pour limiter l'accès de tiers à des contacts qu'ils ont eux-mêmes identifiés et sélectionnés. Cela inclut des réglages de leurs paramètres et la sélection du niveau d'accès public à leurs données ;

- *la protection élevée des données sensibles*, comme l'accès aux données biométriques ou à la reconnaissance faciale qui ne devrait pas être activé par défaut ;

- *la protection des données à caractère personnel* contre tout accès illicite par des tiers, y compris des mesures de cryptage de bout en bout (end-to-end) des communications entre l'utilisateur et les réseaux sociaux. Les utilisateurs devraient être informés des violations de la sécurité de leurs données à caractère personnel afin qu'ils puissent prendre des mesures préventives, comme changer leur mot de passe et surveiller de près leurs opérations financières (par exemple, lorsque les réseaux sociaux disposent de leurs informations bancaires ou des numéros de leur carte de crédit) ;

- *le respect de la vie privée dès la conception (« privacy by design »),* qui concerne la nécessité de protéger les données à caractère personnel dès la phase de conception de leurs produits ou services et d'évaluer en permanence les incidences sur la vie privée de toute modification apportée à des services existants ;

- *la protection des personnes qui n'utilisent pas les réseaux sociaux*, en s'abstenant de collecter et de traiter leurs données à caractère personnel et leurs données biométriques. Il importe que les utilisateurs soient conscients de leurs obligations à l'égard d'autres personnes et, tout particulièrement, du fait que la publication de données à caractère personnel de tiers devrait respecter les droits de ces derniers.[65]

77. Avant la clôture de leur compte, les utilisateurs devraient être en mesure de transférer, aisément et librement et dans un format exploitable, les données qu'ils ont téléchargées vers un autre service ou un outil périphérique. Une fois la résiliation validée, toutes les données relatives à l'utilisateur du compte concerné devraient être définitivement supprimées du support de stockage du service de réseau social. De plus, les utilisateurs d'internet devraient avoir la possibilité de faire des choix éclairés sur leur identité en ligne, y compris, l'utilisation d'un pseudonyme. Lorsqu'un service de réseau social exige une identité réelle pour s'enregistrer sur son site, la diffusion de l'identité des utilisateurs sur internet devrait être facultative. Cela n'empêche pas pour autant les autorités chargées de l'application de la loi d'avoir accès à la véritable identité d'un internaute lorsque cela s'avère nécessaire, et sous réserve de conformité aux garanties juridiques appropriées garantissant le respect des droits et des libertés fondamentales.

78. Dans le cadre du profilage, l'utilisateur devrait pouvoir s'opposer à l'exploitation de ses données personnelles aux fins de profilage et s'opposer à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative prise sur la seule base d'un profilage, à moins que la loi l'autorise et précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée, notamment en lui permettant de faire valoir son point de vue et à moins que la décision ait été prise dans le cadre de l'exécution d'un contrat auquel la personne concernée est partie et que les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée soient mises en place.[66]

[64] Voir CM/Rec(2012)3, et notamment l'annexe, partie II.
[65] Ibid.
[66] Recommandation CM/Rec(2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, section 5.

79. Les droits des usagers d'internet ne sont pas absolus d'où le libellé « en règle générale » au troisième sous-paragraphe. Des restrictions sont autorisées lorsqu'elles sont prévues par la loi et constituent une mesure nécessaire dans une société démocratique : (a) à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales ; et (b) à la protection des personnes concernées ou des droits et libertés d'autrui. Des restrictions à l'exercice des droits peuvent être prévues par la loi pour les fichiers automatisés de données à caractère personnel utilisés à des fins de statistiques ou de recherches scientifiques, lorsqu'il n'existe manifestement pas de risques d'atteinte à la vie privée des personnes concernées.[67]

80. L'interception concerne l'écoute, le contrôle ou la surveillance du contenu des communications, et l'obtention du contenu soit directement au moyen de l'accès au système informatique et de son utilisation, soit indirectement, au moyen de l'emploi de dispositifs d'écoute. L'interception peut aussi consister en un enregistrement des données.[68] Le droit au respect de la confidentialité de sa correspondance et de ses communications est garanti par l'article 8 de la CEDH, qui a été par la suite interprété par la Cour européenne des droits de l'homme. Le concept de correspondance couvre les courriels et les télécommunications,[69] ainsi que les courriels envoyés dans le contexte professionnel[70]. Il faut espérer que l'interprétation va évoluer pour rester en phase avec des progrès technologiques qui pourraient faire entrer dans la sphère de la protection de l'article 8 d'autres formes de communication sur internet, comme les courriels (dans un contexte plus large), la messagerie instantanée et d'autres encore.

81. Certains des principes généraux affirmés dans la juridiction de la Cour concernant l'interception et la surveillance des communications dans des affaires en relation ou pas avec internet et impliquant des ingérences par les pouvoirs publics sont mentionnés ci-dessous. Ces principes fournissent des orientations générales et des références en vue d'une future éventuelle application aux communications par internet.

82. L'interception de la correspondance et des télécommunications constitue une ingérence dans le respect au droit de la vie privée et est soumise aux conditions prévues à l'article 8, paragraphe 2 de la CEDH. L'existence même d'une législation permettant la surveillance des télécommunications peut être considérée comme une ingérence dans le droit à la vie privée. Une loi qui institue un système de surveillance, en vertu duquel tous les individus dans le pays peuvent être concernés par une surveillance de leurs courriels et télécommunications, touche directement tous les utilisateurs ou utilisateurs potentiels des services postaux et de télécommunication nationaux. La Cour a donc accepté que, dans certaines conditions, un individu puisse se prétendre victime d'une violation occasionnée par la simple existence de mesures secrètes ou d'une législation les permettant, sans devoir alléguer qu'il a lui-même fait l'objet de telles mesures.[71]

83. L'interception doit respecter les principes de la base légale et être nécessaire dans une société démocratique dans l'intérêt de la sûreté publique, du bien-être économique du pays, de la défense de l'ordre et de la prévention des infractions pénales, de la protection de la santé ou de la morale, ou de la protection des droits et libertés d'autrui, comme prévu à l'article 8 de la CEDH. La Cour européenne des droits de l'homme a développé les principes généraux ci-après établissant les exigences auxquelles doit satisfaire la législation prévoyant des mesures de surveillance des correspondances et des communications par les autorités publiques.

[67] Convention 108, article 9.
[68] Voir le rapport explicatif de la Convention de Budapest, § 53.
[69] Association pour l'intégration européenne et les droits de l'homme et Ekmidzhiev c. Bulgarie (n° 62540/00) § 58; Klass et Autres c. Allemagne n° 5029/71; Malone c. Royaume-Uni, n° 8691/79 et Weber et Saravia c. Allemagne, n° 54934/00.
[70] Voir Copland c. RU, n° 62617/00.
[71] Klass et Autres, n° 5029/71, § 30-38; Malone c. Royaume-Uni, n° 8691/79§ 64; et Weber et Saravia c. Allemagne n° 54934/00, § 78 et 79, Association pour l'intégration européenne et les droits de l'homme et Ekmidzhiev c. Bulgarie (n° 62540/00), § 58, § 69-70.

- *Prévisibilité* – La loi doit être accessible à l'intéressé qui doit pouvoir prévoir les conséquences de son application à son cas. La loi doit user de termes assez clairs et précis pour indiquer de manière adéquate aux citoyens en quelles circonstances et sous quelles conditions elle habilite les autorités à recourir à une ingérence secrète et potentiellement dangereuse dans le droit au respect de la vie et de la correspondance privées.[72]

- *Garanties minimales pour l'exercice du pouvoir discrétionnaire par les pouvoirs publics* – La loi doit contenir des dispositions détaillées sur (i) la nature des infractions susceptibles de donner lieu à un mandat d'interception ; (ii) la définition des catégories de personnes susceptibles d'être mises sur écoute ; (iii) la fixation d'une limite à la durée de l'exécution de la mesure ; (iv) la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ; et (v) les précautions à prendre pour la communication des données à d'autres parties ; et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements.[73]

- *Contrôle et réexamen par des autorités compétentes* – La Cour requiert l'existence de garanties adéquates et suffisantes contre les abus.[74]

84. La jurisprudence de la Cour en matière de vie privée sur le lieu de travail a estimé que les appels téléphoniques passés par un employé sur le lieu de travail sont couverts par le droit au respect de la vie et de la correspondance privée. Les courriels envoyés du lieu de travail ainsi que les informations découlant de la surveillance de l'usage qu'une personne fait de l'internet devraient être protégés en vertu de l'article 8 de la CEDH. En l'absence d'une mise en garde de possible surveillance en la matière, l'employé peut attendre de manière raisonnable que sa vie privée soit respectée en ce qui concerne les appels téléphoniques, les courriels et l'usage d'internet sur le lieu de travail.[75] L'utilisateur peut obtenir de l'aide auprès des autorités de protection des données, ou d'autres autorités compétentes dans les Etats membres.

85. Les autorités de protection des données, qui existent dans la plupart des pays européens, ont un rôle essentiel d'investigation, d'intervention, de sensibilisation ou plus généralement dans la réparation de l'ingérence dans le traitement des données personnelles. Ceci indépendamment du rôle premier de l'Etat de garantir la protection des données à caractère personnel dans le cadre plus large de leur obligation de protéger le droit au respect de la vie privée et familiale.

Education et connaissances générales

86. Le droit à l'instruction est consacré par l'article 2 du Protocole 1 à la CEDH. La Recommandation CM/Rec(2007)16 du Comité des Ministres aux Etats membres sur des mesures visant à promouvoir la valeur de service public d'internet encourage la création, l'utilisation et l'accès aux contenus pédagogiques, culturels et scientifiques sous forme numérique, afin de veiller à ce que toutes les cultures puissent s'exprimer et accéder à internet dans toutes les langues, y compris autochtones.[76] Les usagers doivent avoir librement accès sur internet aux œuvres culturelles et aux travaux de recherche financés à partir de fonds publics.[77] Il conviendrait de garantir, dans le cadre de limites raisonnables, l'accès libre aux éléments de patrimoine numérique relevant du domaine public. Des conditions peuvent être établies à l'accès au savoir dans des cas très spécifiques, afin de rémunérer les détenteurs de droits pour le travail accompli, dans les limites admissibles du droit à la protection de la propriété intellectuelle.

[72] Malone c. Royaume-Uni, n° 8691/79 § 67; Valenzuela Contreras c. Espagne, arrêt du 30 juillet 1998, rapports 1998-V, p. 1925, § 46 (iii); et Khan c. Royaume-Uni, n°35394/97, § 26, Association pour l'intégration européenne et les droits de l'homme et Ekmidzhiev c. Bulgarie, n° 62540/00, § 71.
[73] Voir Kruslin c. France, n° 11801/85, § 33; Huvig c. France, n° 11105/84, § 32; Amann c. Suisse, n°27798/95, § 56; Weber et Saravia c. Allemagne, n° 54934/00§ 93; Association pour l'intégration européenne et les droits de l'homme et Ekmidzhiev c. Bulgarie (n° 62540/00), § 76.
[74] Ibid., n° 62540/00, § 77.
[75] Copland c. RU, n° 62617/00, § 41, 42.
[76] Voir aussi, CM/Rec(2007)16, section IV.
[77] Ibid.

87. Les utilisateurs d'internet doivent avoir la capacité d'acquérir les informations de base, l'éducation, les savoirs et les savoir-faire nécessaires à l'exercice de leurs droits de l'homme sur internet. Ce principe s'inscrit dans le droit-fil des normes du Comité des Ministres du Conseil de l'Europe qui promeut la maîtrise de l'informatique comme condition essentielle à l'accès à l'information, à l'exercice des droits culturels et au droit à l'éducation par l'intermédiaire des TIC.[78]

88. Les programmes et les initiatives de formation à internet permettent aux utilisateurs de porter un regard critique sur la justesse et la fiabilité des contenus sur internet. Le Comité des Ministres a recommandé aux Etats membres du Conseil de l'Europe de faciliter l'accès aux équipements TIC, de promouvoir pour tous, en particulier les enfants, la formation permettant de travailler avec un large éventail de TIC et de procéder à une analyse critique de la qualité des informations, notamment celles qui sont susceptibles de leur être préjudiciables.[79]

Les enfants et les jeunes

89. Les enfants et les jeunes ont le droit d'exprimer librement leur opinion, de participer à la société et de contribuer aux prises de décision sur les affaires qui les concernent au moyen d'internet et des autres TIC. Ce principe est fondé sur les normes du Comité des Ministres en vertu desquelles tous les enfants et les jeunes de moins de 18 ans devraient avoir le droit, les moyens, la place, la possibilité et, si nécessaire, le soutien d'exprimer librement leurs opinions, d'être entendus et de contribuer aux prises de décision sur les affaires les concernant, leurs opinions étant dûment prises en considération eu égard à leur âge, à leur degré de maturité et à leur capacité de compréhension. Le droit à la participation des enfants et des jeunes s'applique pleinement dans les environnements en ligne, sans discrimination aucune pour des motifs comme la race, l'appartenance ethnique, la couleur, le sexe, la langue, la religion, les opinions politiques ou autres, l'origine nationale ou sociale, la fortune, le handicap, la naissance, l'orientation sexuelle ou toute autre situation.[80]

90. Les enfants et les jeunes devraient recevoir des informations adaptées à leur âge et à leur situation, notamment à travers les réseaux sociaux ou autres médias, sur les possibilités qui s'offrent à eux d'exercer leurs droits. Ils devraient avoir parfaitement connaissance de la portée de leur participation, y compris les limites à leur engagement, des résultats attendus et réels de leur participation et de la façon dont leurs opinions ont finalement été prises en compte.[81] Lorsqu'ils estiment que leur droit à la participation a été bafoué, ils devraient avoir accès à des possibilités de réparation et des voies de recours effectives grâce à des mécanismes de plaintes et à des procédures administratives et judiciaires adaptés aux enfants, y compris une assistance et un soutien dans leur usage.[82]

91. Les enfants et les jeunes utilisateurs devraient pouvoir utiliser internet en toute sécurité et dans le respect de leur vie privée. Ils devraient recevoir des informations et une formation de la part de leurs enseignants, éducateurs et parents. Leurs connaissances en la matière s'entendent comme la maîtrise des outils d'accès à l'information, le développement de l'analyse critique des contenus qu'ils véhiculent et l'appropriation des compétences utiles en vue d'un usage créatif, ainsi que des formations destinées aux enfants et à leurs éducateurs afin qu'ils utilisent internet et les technologies de l'information et de la communication de façon positive et responsable.[83]

[78] Comité des Ministres, Déclaration sur les droits de l'homme dans la société de l'information, CM(2005)56 final 13 mai 2005.
[79] Ibid.
[80] Recommandation CM/Rec(2012)2 du Comité des Ministres aux Etats membres sur la participation des enfants et des jeunes de moins de 18 ans.
[81] Ibid.
[82] Voir Recommandation CM/Rec(2011)12 du Comité des Ministres aux Etats membres sur les droits de l'enfant et les services sociaux adaptés aux enfants et aux familles, Lignes directrices du Conseil de l'Europe sur une justice adaptée aux enfants.
[83] Recommandation Rec(2006)12 du Comité des Ministres aux Etats membres sur la responsabilisation et l'autonomisation des enfants dans le nouvel environnement de l'information et de la communication.

92. Le droit des enfants au respect de la vie privée a été examiné dans le cadre d'affaires portées devant la Cour européenne des droits de l'homme. Le bien-être physique et psychologique des enfants est un aspect essentiel de leur droit au respect de leur vie privée. Les Etats membres ont l'obligation positive de garantir le respect effectif de ce droit.[84] La Cour considère que la dissuasion efficace d'actes graves mettant en péril les valeurs fondamentales et les aspects essentiels de la vie privée exige des dispositions et des enquêtes pénales effectives.[85]

93. Il est important de comprendre que les contenus que les enfants et les jeunes génèrent ou utilisent sur internet ou les contenus que d'autres créent les concernant (par exemple, photos, vidéos, textes ou tout autre contenu) ou encore les traces de ces contenus (fichiers journaux, archives, manipulations effectuées) peuvent avoir une durée de vie importante ou être accessibles en permanence. Cela est susceptible de porter atteinte à leur dignité, à leur sécurité et à leur vie privée, ou encore de les rendre vulnérables, maintenant ou plus tard dans leur vie. Il convient donc de leur donner à eux, ainsi qu'à leurs parents, tuteurs, professeurs ou aux personnes responsables d'eux, les moyens de comprendre et de faire face à cette réalité, ainsi que de protéger leur vie privée en ligne. Il est à cette fin important que des conseils pratiques sur la façon d'effacer des informations personnelles soient disponibles. Le Comité des Ministres du Conseil de l'Europe a en la matière fourni des lignes directrices à ses Etats membres en affirmant qu'il convient de veiller à ce qu'aucun historique des contenus générés par des enfants sur internet, susceptible de porter atteinte à leur dignité, à leur sécurité et à leur vie privée ou de les rendre vulnérables, maintenant ou à un stade ultérieur de leur vie, ne soit accessible de façon durable ou permanente, excepté dans le cadre de la lutte contre les infractions.[86] Par conséquent, les Etats membres sont invités à étudier ensemble, et le cas échéant avec d'autres parties prenantes, la faisabilité de retirer ou de supprimer ce type de contenu – y compris ses traces (fichiers journaux, archives, manipulations effectuées) – dans un délai raisonnablement court.[87] Le sous-paragraphe 3 ne s'applique néanmoins pas aux contenus créés par la presse ou les éditeurs et relatifs aux enfants et jeunes. La première phrase de cette disposition du Guide précise en effet que sont visés les contenus que les enfants et les jeunes génèrent ou utilisent sur internet ou les contenus que d'autres créent les concernant.

94. En ce qui concerne les contenus et comportements préjudiciables en ligne, l'enfant a droit à une aide spéciale et à une assistance adaptée à son âge et à sa situation, en particulier eu égard au risque de préjudice lié à la pornographie en ligne, la représentation humiliante et stéréotypée des femmes, la représentation et la glorification de la violence et de l'automutilation, en particulier les suicides, les propos humiliants, discriminatoires ou racistes, ou l'apologie de tels propos, la sollicitation aux fins d'abus sexuels, le recrutement des enfants victimes de la traite des êtres humains, l'intimidation, la traque et d'autres formes de harcèlement, qui sont susceptibles d'être nuisibles au bien-être physique, émotionnel et psychologique des enfants.[88] Les enfants et les jeunes utilisateurs d'internet devraient par conséquent être informés, d'une manière adaptée à leur âge et d'autres circonstances particulières, des types de contenus et de comportements illicites.

95. Les enfants et les jeunes devraient pouvoir signaler les contenus et les comportements qui présentent un risque de préjudice et recevoir des conseils et un soutien d'une manière qui respecte leur droit à la confidentialité et à l'anonymat. Cela vaut particulièrement dans le contexte des réseaux sociaux. Le Comité des Ministres du Conseil de l'Europe a recommandé à ses Etats membres de prendre des mesures en la matière,[89] notamment de protéger les enfants et les jeunes des contenus préjudiciables, et plus précisément de :

- préciser clairement les types de contenus ou de partage de contenus ou de comportements susceptibles de porter atteinte aux dispositions légales applicables ;

[84] K.U. c. Finlande n°2872/02, § 40, 41.
[85] X et Y c. Pays-Bas, § 23-24 et 27; August c. Royaume-Uni n° 36505/02; et M.C. c. Bulgarie, n° 39272/98, § 150 ; K.U. c. Finlande, n° 2872/02, § 46.
[86] Déclaration du Comité des Ministres du Conseil de l'Europe sur la protection de la dignité, de la sécurité et de la vie privée des enfants sur l'internet.
[87] Ibid.
[88] Recommandation CM/Rec(2009)5 du Comité des Ministres aux Etats membres visant à protéger les enfants contre les contenus et comportements préjudiciables et à promouvoir leur participation active au nouvel environnement de l'information et de la communication.
[89] Voir CM/Rec(2012)4 , annexe, II, § 10.

- développer des politiques éditoriales de telle sorte que des contenus ou des comportements puissent être définis comme « inappropriés » selon les conditions générales d'utilisation du service de réseau social, tout en veillant à ce que cette approche ne limite pas le droit à la liberté d'expression et d'information ;

- créer des mécanismes aisément accessibles visant à signaler tout contenu ou comportement inapproprié ou apparemment illicite sur des réseaux sociaux ;

- réagir avec diligence à toute plainte concernant le harcèlement ou la sollicitation en ligne.[90]

96. Les enfants et les jeunes devraient être informés des risques d'atteinte à leur bien-être physique et psychologique, y compris l'exploitation et les abus sexuels en ligne qui requièrent une protection spéciale. Il y est fait référence dans la Convention de Lanzarote du Conseil de l'Europe et dans la jurisprudence de la Cour, qui reconnaît que les Etats ont l'obligation positive d'assurer la protection des enfants en ligne.[91]

97. En vertu de la Convention de Lanzarote, l'enfant devrait être protégé contre son recrutement en vue de participer à des spectacles pornographiques, sa participation forcée à de tels spectacles ou tout acte visant à faciliter sa participation auxdits spectacles accessibles ou disponibles sur internet (par exemple par des webcams, dans des forums de discussion ou des jeux en ligne).[92] Il devrait aussi être protégé des sollicitations par l'intermédiaire d'internet ou d'autres TIC à des fins d'activités sexuelles avec un enfant qui, conformément aux dispositions pertinentes du droit national, n'a pas atteint l'âge légal pour entretenir des activités sexuelles, ou de production de pornographie infantile.[93]

98. Les enfants devraient être encouragés à participer à l'élaboration et à la mise en œuvre des politiques, des programmes publics ou autres portant sur la lutte contre l'exploitation et les abus sexuels concernant des enfants dans les environnements en ligne.[94] Ils devraient avoir accès à des dispositifs adaptés à leur âge pour signaler les allégations d'exploitation et d'abus sexuels sur internet et déposer plainte par le biais de services d'information, comme les lignes d'assistance par téléphone et par internet. Ils devraient bénéficier de conseils et d'aide pour l'utilisation de ces services d'une manière qui respecte leur droit à la confidentialité et à l'anonymat.[95]

Voies de recours

99. Le droit à un recours effectif est garanti par l'article 13 de la CEDH. Toute personne dont les droits et libertés ont été restreints ou violés sur internet a droit à un recours effectif.

100. L'article 13 de la CEDH garantit l'existence en droit interne d'un recours permettant de se prévaloir des droits et libertés de la Convention tels qu'ils y sont consacrés. Cette disposition a donc pour conséquence d'exiger un recours interne habilitant à examiner le contenu d'un grief fondé sur la Convention et à offrir le redressement approprié.[96] Les Etats ont l'obligation positive de mener une enquête au sujet des allégations de violation des droits de l'homme qui doit être diligente, approfondie et effective. Les procédures suivies doivent permettre à l'organe compétent de décider du bien-fondé de la plainte de violation de la Convention et de sanctionner toute violation constatée, mais aussi de garantir l'exécution des décisions prises.[97]

[90] Ibid.
[91] K.U. c. Finlande n° 2872/02.
[92] Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, (STCE n° 201), article. 2; article 21, voir aussi le rapport explicatif sur ces articles.
[93] Ibid., article 23.
[94] Ibid., article 9/1.
[95] Ibid., article 13. Voir aussi Recommandation CM Rec(2011)12 du Comité des Ministres aux Etats membres sur les droits de l'enfant et les services sociaux adaptés aux enfants et aux familles, Lignes directrices du Conseil de l'Europe sur une justice adaptée aux enfants.
[96] Kaya c. Turquie, n° 22729/93, § 106.
[97] Smith et Grady c. RU, n° 33985/96 33986/96.

101. Une autorité nationale doit être chargée de se prononcer sur les allégations de violation des droits garantis par la CEDH.[98] Il doit exister une voie juridique spécifique par le biais de laquelle un individu doit pouvoir se plaindre du caractère déraisonnable du délai dans la détermination de ses droits.[99] L'autorité en question ne doit pas forcément être une instance judiciaire si elle présente une garantie d'indépendance et d'impartialité. Toutefois, ses pouvoirs et les garanties procédurales offertes devraient permettre de déterminer si tel ou tel recours est effectif.[100]

102. La procédure suivie par l'autorité nationale compétente devrait permettre une enquête effective en cas de violation. Elle devrait permettre à l'autorité compétente de se prononcer sur le bien-fondé de la plainte de violation des droits de la CEDH,[101] de sanctionner toute violation et de garantir à la victime que la décision prise sera exécutée.[102] Le recours doit être effectif en pratique et en droit et ne pas être conditionné à la certitude d'une issue favorable pour le plaignant.[103] L'ensemble des recours offerts par le droit interne peut remplir les exigences de l'article 13, même si aucun d'eux n'y répond en entier à lui seul.[104]

103. Des voies de recours effectives doivent être disponibles, connues, accessibles, abordables et permettre d'obtenir une réparation appropriée. Un recours peut également être obtenu directement auprès des fournisseurs d'accès à internet (bien qu'ils ne jouissent pas nécessairement d'une indépendance suffisante au titre de l'Article 13 de la CEDH), des pouvoirs publics et/ou d'autres institutions nationales des droits de l'homme. Les possibilités de réparation incluent une enquête, une explication par le fournisseur de service ou le prestataire en ligne, la possibilité de répondre à une affirmation jugée diffamatoire ou offensante, par exemple, le rétablissement du contenu créé par l'utilisateur qui a été supprimé par un fournisseur de service en ligne, et la reconnexion à internet de l'utilisateur lorsqu'il a été déconnecté, avec la compensation afférente.

104. Les Etats, dans le cadre de leurs obligations positives de protéger les particuliers contre les violations des droits de l'homme par des entreprises privées, devraient prendre les mesures nécessaires pour assurer que, lorsque de telles violations ont lieu, les victimes ont accès à des mécanismes judiciaires et non judiciaires.[105] Les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme spécifient que les sociétés devraient mettre en place des mécanismes de réclamation qui soient accessibles, prévisibles (prévoyant une procédure clairement établie assortie d'un calendrier indicatif pour chaque étape, et un descriptif précis des types de procédures et d'issues disponibles et des moyens de suivre la mise en œuvre), équitables (assurant un accès aux sources d'information, aux conseils et aux compétences), transparents et en capacité d'offrir des mesures de réparation qui soient pleinement compatibles avec les droits de l'homme internationalement reconnus.[106]

105. Les utilisateurs d'internet devraient avoir accès à des informations claires et transparentes concernant les moyens de recours à leur disposition. Ces informations pourraient être incluses dans les conditions d'utilisation du service ou d'autres lignes directrices et politiques des fournisseurs d'accès/de services internet. Les utilisateurs d'internet devraient disposer d'outils pratiques et accessibles leur permettant de contacter les fournisseurs d'accès/de services internet pour leur soumettre leurs problèmes. Ils devraient pouvoir solliciter des informations et demander réparation. Parmi les exemples de recours à la disposition des utilisateurs d'internet figurent les lignes d'assistance ou les permanences téléphoniques gérées par les fournisseurs de services internet ou les

[98] Silver et Autres c. RU, n° 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, § 113; Kaya c. Turquie, n° 22729/93, § 106.
[99] Kudla c. Pologne, n° 30210/96, § 157.
[100] Silver et Autres c. RU, n° 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, § 113; Kaya c. Turquie, n° 22729/93, § 106.
[101] Smith et Grady c. RU, n° 33985/96 33986/96, § 138.
[102] Iatridis c. Grèce, n° 31107/96, § 60.
[103] Kudla c. Pologne, n° 30210/96, §158.
[104] Silver et Autres c. RU, n°5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, § 113; Kudla c. Pologne, n° 30210/96, §157.
[105] Les questions de la responsabilité sociale des entreprises et des obligations positives de l'Etat de protéger les droits de l'homme sont expliquées aux paragraphes 19 et 28 de l'exposé des motifs.
[106] Voir les Principes directeurs relatifs aux entreprises et aux droits de l'homme mise en œuvre du cadre de référence « protéger, respecter et réparer » (A/HRC/17/31) adoptés par le Conseil des droits de l'homme par la Résolution « Les droits de l'homme et les sociétés transnationales et autres entreprises » A/HRC/RES/17/4, section III, principes 28-31.

associations de protection des consommateurs, vers lesquelles les utilisateurs d'internet peuvent se tourner en cas de violation de leurs droits ou des droits d'autres personnes. Des conseils devraient également être mis à disposition par les pouvoirs publics et/ou d'autres institutions nationales de droits de l'homme (médiateurs), les autorités de protection des données, les autorités de régulation des communications électroniques, les services d'aide aux particuliers, les associations de protection des droits de l'homme ou des droits numériques, ou les organisations de défense des consommateurs.

106. Les utilisateurs d'internet devraient être protégés de la cybercriminalité. Les Etats signataires de la Convention de Budapest se sont engagés à protéger les citoyens des activités criminelles et des infractions pénales commises sur internet. Les utilisateurs d'internet attendent raisonnablement d'être protégés contre les activités criminelles et les infractions pénales commises sur internet ou par l'utilisation d'internet.

107. L'accent est ici placé sur les atteintes à la confidentialité et à l'intégrité des systèmes et des données qu'ils contiennent, et sur les infractions commises par le biais de l'ordinateur. Les infractions en lien avec les contenus (pornographie infantile, violations du droit d'auteur) ne sont pas couvertes dans ce contexte, car il est considéré qu'elles sont traitées par les parties du Guide concernant les droits de l'enfant. Il est par ailleurs considéré que la protection des détenteurs de droits d'auteur concerne les intérêts de ces derniers plutôt que ceux des utilisateurs d'internet. De même, les interceptions et la surveillance des communications sont abordées dans la section sur la protection de la vie privée et des données personnelles.

108. Les utilisateurs d'intérêt ont un intérêt légitime à pouvoir diriger, exploiter et contrôler leurs systèmes informatiques sans perturbation ni entrave d'aucune sorte. Ils devraient être protégés de l'accès illégal à l'intégralité ou une partie quelconque de leur système informatique, y compris le matériel, les composantes, les données stockées du système installé, les répertoires, les données relatives au trafic et au contenu. Cela inclut aussi la protection contre les intrusions non autorisées dans les systèmes informatiques et les données qu'ils contiennent (piratage, infiltration ou autres formes d'intrusion) qui pourraient constituer des entraves pour les utilisateurs d'internet, comme l'accès à des données confidentielles (mots de passe, informations et secrets, etc.).[107]

109. Les utilisateurs d'internet devraient aussi bénéficier d'une protection contre les atteintes à l'intégrité des données contenues dans leur ordinateur par des programmes malveillants (par exemple, les virus et les chevaux de Troie).[108] Ils devraient aussi être protégées contre les ingérences dans le fonctionnement de leur ordinateur ou de leurs systèmes de télécommunication par l'introduction, le transfert, l'endommagement, l'effacement, l'altération ou la suppression de données informatiques,[109] par exemple par des programmes qui portent atteinte à des systèmes sous la forme d'un « déni de service », des codes malveillants, tels que les virus, qui interdisent ou ralentissent sensiblement le fonctionnement du système, ou les programmes qui envoient un énorme volume de courrier électronique à un destinataire afin de paralyser les fonctions de communication du système (spamming). Il peut s'agir d'une infraction administrative ou pénale, selon le droit interne.

110. Les utilisateurs d'internet devraient être protégés contre la falsification informatique, qui concerne la création non autorisée ou l'altération des données enregistrées de façon qu'elles acquièrent une valeur probante différente dans le déroulement de transactions juridiques, qui sont fondées sur l'authenticité des informations fournies par ces données.[110]

111. Les utilisateurs d'internet ont un intérêt légitime à bénéficier de la protection des actifs représentés ou gérés par des systèmes informatiques (fonds électroniques, dépôts). Ils devraient être protégés contre les fraudes informatiques qui occasionnent directement à l'utilisateur un préjudice économique ou matériel (argent et immobilisations corporelles ou incorporelles ayant une valeur économique), comme les fraudes à la carte de crédit.[111]

[107] Convention de Budapest sur la cybercriminalité, article 2, rapport explicatif, § 44-50.
[108] Ibid. article 4, rapport explicatif, § 60-61.
[109] Ibid. article 5, rapport explicatif, § 65-69.
[110] Ibid., article 7, rapport explicatif, § 81.
[111] Ibid., article 8, rapport explicatif, § 86-88.

112. Toute mesure de sécurité visant à assurer la protection des utilisateurs d'internet contre la cybercriminalité doit respecter pleinement les normes de la CEDH, notamment eu égard au droit au respect de la vie privée et de la vie familiale et au droit à la liberté d'expression.[112]

113. Les utilisateurs d'internet ont droit à un procès équitable, tel que consacré par l'article 6 de la CEDH. Cela renvoie à la détermination des droits civils et des obligations ou des chefs d'inculpation pénale eu égard aux activités des utilisateurs d'internet. En particulier, cela concerne les principes clés énoncés par la Cour européenne des droits de l'homme, et notamment le droit à ce que leur cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, le droit d'introduire une action en justice, le droit à un règlement final du différend, à un jugement raisonné et à l'exécution du jugement, le droit à une procédure contradictoire et à l'égalité des armes.

114. La Cour, bien que ce ne soit pas dans des affaires en relation avec internet, a établi des principes généraux eu égard à l'administration de la justice (indépendance, impartialité, compétence du tribunal) et à la protection du droit des parties (jugement équitable, égalité des armes et audience publique), ainsi que concernant l'efficience de l'administration de la justice (délai raisonnable).

115. L'utilisateur d'internet a un droit de recours individuel devant la Cour après l'épuisement des voies de recours internes disponibles et effectives, dans un délai de six mois[113] à compter de la date à laquelle une décision finale a été prise.

[112] Ibid. article 15.
[113] Ce délai serait quatre mois après l'entrée en vigueur du Protocole n° 15 de la CEDH.

PREMS 70414

FRA

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il compte 47 États membres, dont 28 sont également membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE