Cyber : Pour et contre le terrorisme

Auteur : Naedenoen, Nathaël
Promoteur(s) : Flore, Daniel
Faculté : Faculté de Droit, de Science Politique et de Criminologie
Diplôme : Master en droit, à finalité spécialisée en droit privé
Année académique : 2023-2024
URI/URL : http://hdl.handle.net/2268.2/19750

LIÈGE université
Droit, Science Politique & Criminologie

Département de Droit

Cyber : Pour et contre le terrorisme

Nathaël NAEDENOEN

Travail de fin d'études

Master en droit à finalité spécialisée en droit privé

Année académique 2023-2024

Recherche menée sous la direction de :

Monsieur Daniel FLORE

Professeur

RESUME

Cette étude a pour but de voir, à l'heure actuelle, sur la scène internationale, comment l'utilisation des outils informatiques peut obtenir la qualification de terroriste, et en parallèle, quels outils ou mécanismes informatiques peuvent être utilisés par les autorités pour lutter contre le terrorisme, dans quelles limites et avec quelles difficultés.

La première partie abordera donc les difficultés de définition tant du terrorisme que du cybercrime. Et dès lors, a fortiori, les difficultés liées au concept de cyberterrorisme, incluant aussi bien les attaques contre ou par le biais d'un système informatique, telles que visées par la directive (UE) 2017/541, que les contenus à caractère terroriste en ligne, comme définis à l'article 2, 7) du règlement (UE) 2021/784. Nous parlerons aussi de la provocation publique à commettre une infraction terroriste, telle que visée par l'article 5 de la directive 2017/541 et 5 de la convention du Conseil de l'Europe pour la prévention du terrorisme de 2005.

Une deuxième partie de l'exposé se penchera sur les instruments disponibles à l'heure actuelle dans la lutte contre le terrorisme, plus particulièrement sur le plan procédural. Principalement, ce sont les moyens contenus dans la directive (UE) 2017/541 et le règlement (UE) 2021/784 qui seront abordés. En effet, ces deux instruments prévoient des mesures spécifiques pour traiter des infractions à caractère terroriste. Les sanctions spécifiques prévues par ces instruments seront aussi succinctement mentionnées. Les pouvoirs d'enquête digitale consacrés par la convention de Budapest seront également synthétisés à cette occasion et ses protocoles seront brièvement passés en revue. Pour finir, nous dirons un mot de l'e-evidence package de l'Union européenne et de l'utilisation de l'IA. Eu égard à l'objet de cette étude, seuls les moyens d'action digitaux seront pris en compte, les moyens d'action standards ne seront pas abordés.

Enfin, dans la dernière partie de l'exposé, le conflit entre la réaction face au cyberterrorisme et les droits fondamentaux sera synthétisé au regard de ce qui précède. Ce sera également l'occasion de parler de la différence entre l'hacktivisme et le cyberterrorisme ainsi que du RGPD. Nous aborderons donc principalement les questions liées à la liberté d'expression et au droit à la vie privée, au regard de la jurisprudence de la Cour européenne des droits de l'Homme et de la Cour de justice de l'Union européenne.

L'objectif final est ainsi de voir, selon l'état actuel de la législation internationale, comment la qualification terroriste se combine aux moyens d'action technologiques dans la lutte contre le terrorisme, et ce dans le respect des droits fondamentaux.

REMERCIEMENTS

Merci au Professeur Flore d'avoir accepté de promouvoir mon travail.

Merci aussi tout particulièrement à Keyla Lubembo et Julian Ernotte de m'avoir relu, soutenu et encouragé tout au long de ce travail.

TABLE DES MATIERES

INTRODUCTION

À l'heure d'Internet, tant les actes de criminalité que les moyens d'y répondre évoluent. Le terrorisme et la lutte contre le terrorisme ne font pas exception.

Cette recherche tentera donc de déterminer quelle est l'utilisation du cyberespace qui peut être qualifiée de terroriste et quels moyens digitaux sont mis à disposition, même de manière générale, pour lutter contre le terrorisme. Le but ultime sera de voir comment, au vu des limites imposées par les droits fondamentaux, la qualification terroriste et les moyens d'action actuels se combinent pour lutter contre le terrorisme dans le cyberespace.

Pour ce faire, il s'agira dès lors, dans un premier temps, de définir les concepts de terrorisme, de cybercriminalité ainsi que de cyberterrorisme sous toutes ses facettes, et ce tant d'un point de vue criminologique que légal. L'objectif sera de faire un cliché de l'état de la doctrine et de la législation en la matière. Nous verrons particulièrement les difficultés à définir ces différents concepts.

Ce premier chapitre sera divisé en quatre parties, la première partie sera consacrée aux difficultés liées à la définition du terrorisme, la deuxième à celles liées au concept de cybercrime et la troisième aux difficultés propres au cyberterrorisme. Enfin, la dernière partie présentera les actes en ligne qui reçoivent la qualification terroriste par le droit européen.

Étant donné l'objet de cette étude, nous parlerons surtout de la qualification terroriste d'actes commis dans le cyberespace. Le thème de ce travail étant le droit pénal international et européen, et le droit international, en tous cas des Nations Unies, n'ayant apporté pour l'instant aucune réponse satisfaisante au terrorisme dans la sphère digitale, nous nous concentrerons principalement sur la législation européenne en la matière. Nous parlerons principalement de la directive 2017/541 relative à la lutte contre le terrorisme, qui attribue la qualification terroriste à des actes de cybercriminalité, et le règlement 2021/784 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, qui vise surtout à réprimer la propagande terroriste en ligne. Pour ce qui est de la provocation publique à commettre une infraction terroriste, nous évoquerons les articles 5 de la directive 2017/541 et 5 de la convention du Conseil de l'Europe de 2005.

Dans un deuxième temps, nous présenterons les différents moyens d'action à disposition de la lutte contre le terrorisme. Pour ce faire, nous diviserons les moyens présentés dans ce deuxième chapitre en sept parties.

La première partie portera sur les moyens à disposition pour lutter contre la provocation et le contenu terroriste en ligne, la deuxième sur les moyens de lutte contre les cyberattaques terroristes.

La troisième partie sera consacrée à l'enquête digitale plus générale, telle qu'elle est régie par la convention de Budapest. Celle-ci n'est pas spécifiquement liée au terrorisme, mais peut quand même s'appliquer en cas de cyberattaque, et ce même si la qualification terroriste n'est pas rencontrée.

Les quatrième et cinquième parties présenteront brièvement les protocoles additionnels de la convention de Budapest. Le premier protocole vise l'incrimination du racisme et de la

xénophobie en ligne tandis que le deuxième, plus général mais pas encore entré en vigueur, vise à renforcer la coopération en matière de preuves électroniques.

Dans la sixième partie, nous présenterons l'« e-evidence package » de l'Union européenne, constitué d'une directive et d'un règlement relatifs aux moyens de preuve électronique.

Enfin, la septième partie introduira succinctement l'utilisation de l'IA, qui peut permettre de faciliter la réaction à l'encontre du contenu à caractère terroriste, mais qui engendre également de nombreux défis.

Pour finir, le dernier chapitre relèvera les limites qui sont imposées, tant à la qualification terroriste qu'aux moyens de lutte, par les droits fondamentaux.

En effet, l'attribution de la qualification terroriste est limitée par la liberté d'expression. Cela a surtout une incidence sur la provocation et les contenus terroristes en ligne. La limite apportée par la liberté d'expression a fait l'objet de la jurisprudence tant de la Cour européenne des droits de l'Homme que de la Cour de justice de l'Union européenne. Nous ferons référence à ces arrêts, mais nous nous limiterons à quelques exemples seulement.

La liberté d'expression peut aussi entrer en compte, mais dans une moindre mesure, dans le cas des cyberattaques. En effet, à côté des cyberattaques terroristes, on retrouve également des cyberattaques qui sont le fait d'hacktivistes, prônant la liberté d'expression pour commettre des actes de cybercriminalité en signe de protestation, en raison de leurs idéologies. Nous mentionnerons donc les rapprochements entre le cyberterrorisme, en tant qu'acte de cybercriminalité, et l'hacktivisme, mais également les points de divergence entre les deux concepts.

En ce qui concerne les limites aux pouvoirs d'enquête, la plus notable est celle qui découle du droit à la vie privée. En effet, les moyens technologiques actuels permettent une surveillance et une récolte d'informations beaucoup plus importante que par le passé. Il faut dès lors accroître d'autant plus la vigilance pour éviter de tomber dans des ingérences arbitraires ou illégales dans la vie privée des citoyens. La Cour européenne des droits de l'Homme est ainsi intervenue dans sa jurisprudence pour rappeler à l'ordre les États en leur imposant des limites dans la collecte d'informations, notamment en vertu des principes de subsidiarité, nécessité et proportionnalité, ainsi qu'en rappelant l'obligation de prévoir des moyens de recours. La Cour de justice de l'Union européenne a également fourni de la jurisprudence en ce sens. Quelques exemples parmi les plus pertinents seront évoqués.

Pour clôturer ce chapitre, le RGPD sera brièvement mentionné en ce qu'il peut limiter l'échange de données entre les États.

CHAPITRE I : QUALIFICATION TERRORISTE DES ACTES EN LIGNE

A. Difficultés de définition du terrorisme

Depuis son apparition, le terme de terrorisme a été controversé dans les discussions entre les États et à l'heure actuelle, il n'existe toujours aucun consensus. En effet, seules des conventions visant certaines formes d'actes de terrorisme ont été prises sur la scène internationale, sans aucune définition générale[1].

Cette controverse venait d'une part, de la volonté des États occidentaux d'écarter le « terrorisme d'État », en temps de guerre comme en temps de paix, autrement dit, les actions des forces armées, et d'autre part, de la volonté des États du Tiers-Monde d'écarter la qualification de terroriste des mouvements de libération nationale[2].

Certains critères ont néanmoins pu être retirés en combinant la nature violente de certains actes avec les objectifs poursuivis par les auteurs, mais ces critères restent variables en fonction des États et des systèmes juridiques, puisque les éléments définitionnels diffèrent d'un instrument à l'autre[3].

Outre l'utilisation de la terreur comme instrument, il est notamment possible de pointer deux éléments essentiels du terrorisme, un élément téléologique, à savoir dans le but spécifique de troubler l'ordre public ou renverser l'ordre constitutionnel, et un élément structurel, à savoir des actes perpétrés par une organisation criminelle ou un groupe[4]. Ce dernier élément est toutefois contesté à cause des nouvelles manifestations terroristes, telles que les « lone wolves[5] »[6].

Étant donné la variété de dimensions que peut prendre le terrorisme, des définitions trop complexes et précises ne prendraient pas en compte toutes les hypothèses possibles en cette matière, tandis que des définitions trop larges manquent à réserver la qualification de terroriste aux seules infractions qui menacent réellement la société[7].

Sur le plan international, au départ, quelques actes spécifiques, comme les détournements d'avions ou les atteintes au matériel nucléaire, étaient réprimés par des conventions internationales, sans grande définition du terrorisme.

---

[1] F. DUBUISSON, « La définition du "terrorisme" : débats, enjeux et fonctions dans le discours juridique », *Confluences Méditerranée*, 2017/3 (n°102), p. 31.
[2] F. DUBUISSON, *Ibidem*, p. 31.
[3] F. DUBUISSON, *Ibidem*, p. 34.
[4] A. PASTRANA SANCHEZ, « A critical concept of terrorism for criminal prosecution », *INECS*, 2022, n°17, article 6, pp. 12 – 13.
[5] En général, il s'agit d'immigrants de seconde génération qui se radicalisent d'eux-mêmes via internet et agissent individuellement ou en coordination avec d'autres de même nature, de manière autonome, mais poursuivant la même idéologie jihadiste. Cfr A. PASTRANA SANCHEZ, *Ibidem*, p. 10.
[6] A. PASTRANA SANCHEZ, *Ibidem*, p. 14.
[7] N. BOISTER, *An introduction to transnational criminal law*, 2e éd., New York, Oxford, 2018, p. 107.

En 1997, la convention internationale pour la suppression des attentats terroristes à l'explosif a fait un premier pas en incriminant la participation au groupe terroriste[8].

En 1999, ensuite, la convention internationale pour la suppression du financement du terrorisme est intervenue pour prévenir et contrer le financement qui ne doit ainsi plus être en relation directe avec une infraction terroriste[9].

Au sein de l'Union européenne, plus spécifiquement, une convention européenne sur la suppression du terrorisme de 1977 a permis de faciliter les extraditions, particulièrement en supprimant l'exception d'infraction politique dans les cas de terrorisme[10].

Du point de vue des droits humains, la qualification terroriste est très importante puisqu'elle entraîne des procédures et sanctions spécifiques, fort attentatoires aux droits fondamentaux. Or, seules quelques expressions de ces droits se retrouvent dans les conventions susmentionnées[11]. Et l'ambiguïté, selon le conseil des droits humains de l'ONU, peut entraîner des restrictions illégitimes de liberté[12].

Malgré ces difficultés, sur le plan criminologique, une sorte de consensus semble se dessiner sur au moins trois conditions nécessaires à la qualification terroriste[13], à savoir la poursuite d'un objectif politique, la volonté d'intimider plus que de faire des victimes directes et une asymétrie de pouvoir.

B. Difficultés de définition du cybercrime

Le cybercrime désigne tant les actes qui s'attaquent à des structures informatiques ou des données que les actes qui usent de systèmes informatiques pour commettre des infractions[14] ou encore le contenu informatique qui constitue en lui-même une infraction[15]. Il est également possible, selon certains, de faire une distinction entre deux grandes catégories, les crimes cyberfacilités, autrement dit les infractions classiques qui se sont étendues ou déplacées en ligne, et les crimes cyberdépendants, où la technologie est essentielle à l'infraction[16].

Dans cette matière, la principale difficulté est de mettre en balance la protection contre les cybercrimes et la protection contre les atteintes injustifiées aux droits fondamentaux[17].

---

[8] N. BOISTER, *Ibidem*, p. 112.
[9] N. BOISTER, *Ibidem*, p. 113.
[10] N. BOISTER, *Ibidem*, p. 113.
[11] N. BOISTER, *Ibidem*, p. 122.
[12] N. BOISTER, *Ibidem*, p. 123.
[13] M. INNES et M. LEVI, « Making and managing terrorism and counter-terrorism : the view from criminology », *the Oxford handbook of criminology* (7e éd.), A. Liebling, S. Maruna, L. McAra (dir.), New York, Oxford, 2023, p. 657.
[14] N. BOISTER, *An introduction to transnational criminal law*, 2e éd., New York, Oxford, 2018, p. 188.
[15] N. BOISTER, *Ibidem*, p. 193.
[16] B. COLLIER et A. HUTCHINGS, « Cybercrime : A social ecology », *the Oxford handbook of criminology* (7e éd.), A. Liebling, S. Maruna, L. McAra (dir.), New York, Oxford, 2023, p. 457.
[17] N. BOISTER, *Op. Cit.*, p. 189.

La plus grande avancée législative dans ce domaine est certainement la convention de Budapest du Conseil de l'Europe, adoptée en 2001, qui a permis de poser le cadre de l'incrimination matérielle des cybercrimes. Toutefois, cette convention ne définit pas le cybercrime en tant que tel, elle ne fait qu'énumérer différentes catégories d'infractions cybercriminelles.

Cette convention couvre de nombreux domaines, mais depuis son adoption, force est de constater que les cybercrimes ont évolué et que la convention n'est donc plus tout à fait suffisante à couvrir tous les actes de cybercrime, notamment avec l'avènement de l'IA. À une expansion du champ d'application de la convention s'opposent toutefois les droits fondamentaux, et notamment la possibilité que cette extension soit un moteur pour la censure et une limitation de la liberté d'expression[18].

Au niveau de l'ONU, malgré des appels à travailler à la répression des cybercrimes depuis 2001, aucun accord n'a pu être trouvé pour l'adoption d'une convention. En effet, les désaccords concernaient essentiellement les problèmes de souverainetés, comme l'accès à des systèmes informatiques d'un autre pays ou la possibilité de donner des injonctions à des entités qui se trouvent matériellement sur le territoire d'un autre État, ainsi que les inquiétudes relatives aux droits humains. À cela s'ajoute le fait que, selon certains, la convention de Budapest serait suffisante et pourrait servir de cadre puisqu'elle est ouverte aux pays non-membres du Conseil de l'Europe[19].

C. Difficultés de définition du cyberterrorisme

Le cyberterrorisme peut être défini selon l'auteur ou selon les actes commis, mais pose des difficultés étant donné l'imprécision liée à la notion tant de terrorisme que de cybercrime[20].

Si c'est l'auteur qui est utilisé pour définir le terrorisme, par son identité et son intention, outre le fait que la qualification terroriste n'a pas de caractéristiques claires et des critères communément admis, le cyberterrorisme rencontre la difficulté majeure de l'anonymat en ligne[21].

Quant à la qualification par l'acte, elle pose également un problème lorsque la définition du terrorisme retenue est celle de l'action violente entraînant des effets psychologiques disproportionnés par rapport aux effets physiques. En effet, une action dans le cyberespace a rarement des effets physiques conséquents[22], bien que l'évolution actuelle de la technologie, et notamment l'*Internet of Things*, puisse radicalement changer la donne. Le critère de la violence serait dès lors difficile à remplir. En outre, les actes terroristes sont souvent indiscriminés et frappent des populations civiles de manière disproportionnée. Or, des opérations criminelles dans le cyberespace sont rarement de grande envergure ; elles frappent le plus souvent des acteurs spécifiques pour des motifs économiques, ou alors sont

[18] N. BOISTER, *Op. Cit.*, p. 196.
[19] N. BOISTER, *Op. Cit.*, p. 198.
[20] O. KEMPF, "Le cyberterrorisme : un discours plus qu'une réalité », *Hérodote*, 2014/1-2 (n°152-153), p. 83.
[21] O. KEMPF, *Ibidem*, p. 84.
[22] O. KEMPF, *Ibidem*, p. 85.

basiques, et consistent en de simples dénis de service ou *spamming*, avec des effets mineurs[23]. Il en découle ainsi également une absence quasi certaine d'effets psychologiques disproportionnés[24].

La plupart des auteurs définissent néanmoins le cyberterrorisme comme l'utilisation de la technologie digitale ou de la communication à travers les ordinateurs pour causer des dommages ou forcer un changement social contre la population civile sur base d'idéologies ou d'opinions politiques. Par exemple, en 2001, l'Institut National de Justice des États-Unis l'a défini assez largement comme l'attaque préméditée et politiquement motivée contre des systèmes, programmes ou données informatiques, pour rompre l'infrastructure politique, sociale ou physique de la cible. Selon cette définition, la violence physique n'est pas nécessaire, une simple atteinte économique ou la peur provoquée par une telle attaque informatique sont suffisantes à la qualification de terroriste[25].

Les cyberattaques représentent aussi potentiellement un nouveau moyen d'action pour le terrorisme, qui pourraient à l'avenir permettre d'atteindre à la vie ou de produire de sévères dégâts économiques. Cependant, la plupart des gouvernements et auteurs ont peine à qualifier terroriste les cyberattaques étant donné qu'elles n'ont, jusqu'à présent, pas produit de dommages physiques et psychologiques aussi importants que les attentats[26].

De multiples exemples peuvent pourtant être donnés de la possibilité pour des groupes de hackers de supporter des objectifs terroristes. Par exemple, en 1997, le groupe « Libération Tigers of Tamil Eelam » fut responsable de bombardements de courriels envers les ambassades du Sri Lanka, envoyant près de 800 mails par jour pour perturber les communications. En 2001, peu après les attentats du 11 septembre, un groupe de hackers associé à Al-Qaeda avait menacé des sites web gouvernementaux américains. À partir de là, un jihad électronique a commencé en ligne, distribuant des manuels et outils d'hacking pour promouvoir et coordonner des cyberattaques contre des sites web, comme celui du Vatican ou encore de grandes banques américaines[27].

En outre, le concept de cyberterrorisme peut désigner la radicalisation à travers la technologie ou encore son financement. Cela pose moins de difficultés dès lors qu'il n'y a pas besoin d'effets physiques ou psychologiques pour attribuer la qualification terroriste.

Le cyberespace est donc profitable au terrorisme en ce qu'il permet la communication et la propagande, sans frontières. Il permet également de mieux préparer les actions terroristes sur le terrain[28].

Pour l'instant, les définitions proposées viennent d'auteurs de différentes spécialisations, de sorte qu'elles n'optent pas toujours pour le même point de vue[29]. Une certaine confusion

---

[23] O. KEMPF, *Ibidem*, p. 87.
[24] O. KEMPF, *Ibidem*, p. 88.
[25] T.J. HOLT, G.W. BURRUSS et A.M. BOSSLER, *Policing Cybercrime and Cyberterror*, Durham, C.A.P., 2015, p. 10.
[26] Y. JEWKES et M. YAR, *Handbook of Internet Crime*, Cullompton, Willan, 2009, p. 198.
[27] Y. JEWKES et M. YAR, *Ibidem*, p. 199.
[28] O. KEMPF, *Op. Cit.*, p. 94.
[29] E. LUIIJF, « Definitions of Cyber Terrorism », *Cyber Crime and Cyber Terrorism Investigator's Handbook*, B. Akhgar, A. Staniforth et F. Bosco (dir.), Watham, Elsevier, 2014, p. 11.

règne également du fait que le terme de « cyberterrorisme » est utilisé pour toute utilisation du cyberespace par des terroristes et groupes terroristes[30].

En définitive, comme vu précédemment, la définition tant du terrorisme que du cybercrime fait l'objet de difficultés. Il est donc d'autant plus difficile de définir le cyberterrorisme que les concepts qui le précèdent ne sont pas toujours clairs[31].

Pour l'attaque terroriste en ligne, une définition qui pourrait néanmoins être proposée serait l'utilisation, la préparation ou la menace d'une action destinée à causer un changement d'ordre social, à créer un climat de peur ou d'intimidation parmi le public, ou à influencer les décisions politiques du gouvernement ou d'une organisation internationale, dans l'intention de promouvoir une cause politique, religieuse, raciale ou idéologique, en affectant l'intégrité, la confidentialité ou l'accessibilité d'informations, de systèmes d'information et de réseaux, ou par des actions non autorisées affectant le contrôle technologique d'information et communication de procédés du monde physique, et qui implique ou cause violences, dommages ou mort de personnes, dommages à une propriété, de sérieux risques pour la santé et la sécurité du public, une sérieuse perte économique, une sérieuse brèche pour la sécurité écologique ou pour la stabilité politique et sociale et la cohésion nationale[32].

D. Qualification légale

Au niveau européen, la directive (UE) 2017/541[33], en son article 3.1.d), érige en infraction terroriste le fait de causer des destructions massives à une installation gouvernementale ou publique, y compris à un système informatique, et son article 3.1.i) en fait de même pour l'atteinte illégale à l'intégrité d'un système. Cette qualification donne ainsi accès aux outils d'enquête et de confiscation (art. 20). Cette directive reprend et précise la décision-cadre du Conseil de 2002 relative à la lutte contre le terrorisme[34].

Par ailleurs, l'article 3.1.i) vise les infractions contenues aux articles 4 et 5 de la directive 2013/40/EU[35], autrement dit, l'interférence illégale avec un système ou des données, mais pas l'interception de données ou l'accès à des systèmes d'information. La qualification ne s'étend pas non plus aux outils pour commettre les infractions susmentionnées.

Or, l'interception de données et l'accès à des systèmes pourraient être utilisés par des groupes terroristes pour accéder à des données sensibles et s'en servir ensuite pour commettre des infractions en dehors de la sphère informatique. De plus, étendre la qualification aux outils pour commettre des infractions informatiques pourrait permettre d'intervenir bien plus tôt dans le processus. Le seul tempérament à cela est l'article 4 de la directive 2017/541 qui

[30] E. LUIIJF, *Ibidem*, p. 13.
[31] E. LUIIJF, *Ibidem*, p. 14.
[32] E. LUIIJF, *Ibidem*, p. 15-16.
[33] Directive (EU) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil, *J.O.U.E.*, L 88/6, 31 mars 2017.
[34] Décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme, *J.O.U.E.*, L 164, 22 juin 2002.
[35] Directive 2013/40/EU du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, *J.O.U.E.*, L 218/8, 14 août 2013.

incrimine les infractions liées à un groupe terroriste, en ce compris la fourniture d'informations ou de moyens matériels en sachant que cela contribuera aux activités criminelles du groupe terroriste. Encore faut-il pour cela identifier un lien avec le groupe terroriste, ce qui n'est pas nécessairement chose aisée dans le cyberespace.

En ce qui concerne la propagande terroriste en ligne, la même directive, en son article 21, prévoit des mesures pour lutter contre les contenus en ligne de provocation publique à commettre une infraction terroriste, complétée par le règlement (UE) 2021/784[36].

Le règlement (UE) 2021/784 définit le contenu à caractère terroriste en son article 2 (7), comme le matériel qui incite à la commission d'infractions visées à l'article 3, §1er, points a) à i) de la directive (UE) 2017/541, que ce soit directement ou indirectement, en sollicitant une personne ou un groupe à commettre, contribuer ou participer à ces infractions ou en fournissant des instructions, et même lorsque cela ne constituerait qu'une menace.

L'article 5 de la directive 2017/541 prévoit aussi l'interdiction de la provocation publique à commettre une infraction terroriste, en visant expressément la diffusion en ligne ou hors ligne. L'article 6 incrimine également le recrutement pour le terrorisme, autrement dit, solliciter une personne pour commettre l'une des infractions énumérées dans la directive.

L'article 5 de la convention du Conseil de l'Europe pour la prévention du terrorisme de 2005[37] ne vise pas expressément la provocation en ligne, mais est neutre dans ses termes, de sorte que la publication en ligne de contenu tendant à inciter à commettre des infractions terroristes peut être inclus. L'article 6 de la convention incrimine aussi le recrutement pour le terrorisme.

Lorsque l'on compare l'article 5 de la directive 2017/541 et l'article 5 de la convention du Conseil de l'Europe, même si les deux sont globalement assez similaires, il est possible de noter que la directive précise que la diffusion peut être en ligne ou hors ligne, ce que ne fait pas la convention. En outre, la directive précise que la glorification des actes terroristes est également visée, ce que ne fait pas non plus la convention. Par ailleurs, la convention prévoit que la provocation doit être commise « illégalement », ce qui n'est pas le cas de la directive. La directive de l'Union européenne est donc plus précise que la convention du Conseil de l'Europe.

L'article 7 de la convention de Varsovie, en ce qu'il vise le fait de donner des instructions « pour d'autres méthodes et techniques spécifiques en vue de commettre une infraction terroriste ou de contribuer à sa commission », pourrait aussi inclure la mise à disposition d'instructions pour commettre des cyberattaques. L'article 7 de la directive 2017/541 incrimine également en son article 7 le fait de dispenser un entraînement au terrorisme, en ce compris le fait de fournir des instructions en rapport avec toute méthode ou technique spécifique permettant de commettre un des infractions énumérées à l'article 3, §1er, a) à i) ou contribuer à l'une de ces infractions. L'article 8 de la directive prévoit également que le fait de recevoir intentionnellement un entraînement terroriste soit incriminé. Aucun article similaire

[36] Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, *J.O.U.E.*, L 172/79, 17 mai 2021.
[37] Convention du Conseil de l'Europe pour la prévention du terrorisme, *STCE* n° 196, Varsovie, 16 mai 2005, en vigueur le 1er juin 2007.

ne peut être trouvé dans la convention du Conseil de l'Europe, mais cela est prévu à l'article 3 du protocole additionnel à la convention du Conseil de l'Europe[38]

Malheureusement, il faudrait, pour que ces différents articles de la convention du Conseil de l'Europe et de son protocole additionnel s'appliquent aux cyberattaques, que celles-ci soient inclues dans la définition d'infraction terroriste. Ce n'est pas le cas puisque l'article 1 de la convention pour la prévention du terrorisme ne vise que les infractions qualifiées terroristes par les Traités listés en annexe et aucun de ces Traités ne permet de qualifier de terroristes des cyberattaques.

En revanche, certaines cyberattaques, nous l'avons vu, sont inclues dans la directive 2017/541. Ainsi, les articles ci-dessus sont applicables également lorsque la provocation, le recrutement ou l'entraînement se font en vue de commettre des cyberattaques terroristes.

À noter que l'Union européenne est partie à la convention du Conseil de l'Europe pour la prévention du terrorisme et à son protocole additionnel depuis 2018, par deux décisions du Conseil du 4 juin 2018, une pour la convention elle-même[39] et une pour le protocole additionnel[40].

[38] Protocole additionnel à la convention du Conseil de l'Europe pour la prévention du terrorisme, *STCE* n°217, Riga, 22 octobre 2015, en vigueur le 1er juillet 2017.
[39] Décision (UE) 2018/889 du Conseil du 4 juin 2018 relative à la conclusion, au nom de l'Union européenne, de la convention du Conseil de l'Europe pour la prévention du terrorisme, *J.O.U.E.*, L 159/1, 22 juin 2018.
[40] Décision (UE) 2018/890 du Conseil du 4 juin 2018 relative à la conclusion, au nom de l'Union européenne, du protocole additionnel à la convention du Conseil de l'Europe pour la prévention du terrorisme, *J.O.U.E.*, L 159/15, 22 juin 2018.

CHAPITRE II : POUVOIRS D'INVESTIGATION ET DE SANCTION

A. Provocation et contenu terroriste en ligne

1) Moyens procéduraux

Pour contrer le contenu de provocation publique en ligne, l'article 21 de la directive 2017/541 prévoit que les États membres prennent des mesures pour ôter le contenu en ligne qui constitue une provocation publique à commettre une infraction terroriste telle que définie à l'article 5 et qui est hébergé sur son territoire.

La majeure difficulté sera alors de savoir ce que signifie l'hébergement sur le territoire. En effet, cela change radicalement la donne si l'on situe le service d'hébergement dans le pays où se trouvent les serveurs contenant les fichiers ou dans tout pays sur lequel le contenu est visible et disponible.

L'article 21 impose tout de même aux États membres de s'efforcer, à tout le moins, de rendre inaccessible le contenu sur son territoire.

Cette disposition a été complétée par le règlement 2021/784, qui fait explicitement référence aux infractions définies par la directive 2017/541. L'article 1er, §2 de ce règlement précise qu'il s'applique aux fournisseurs de services d'hébergement qui proposent des services dans l'Union, quel que soit leur lieu d'établissement principal, du moment qu'ils diffusent des informations au public.

L'article 3 du règlement 2021/784 permet alors les injonctions de retrait pour retirer ou bloquer l'accès aux contenus dans tous les États membres. Cette injonction est adressée à l'établissement principal du fournisseur de services d'hébergement ou son représentant légal. Si cet établissement principal n'est pas situé dans l'État membre qui émet l'injonction et qu'il n'y a pas de représentant légal, un palliatif consiste à soumettre simultanément une copie de l'injonction à l'État membre sur lequel le fournisseur de service possède son établissement principal ou là où son représentant légal réside, selon la procédure détaillée à l'article 4.

L'article 5 prévoit en outre que les fournisseurs de service d'hébergement exposés à du contenu terroriste incluent dans leurs termes et conditions et appliquent des mesures pour contrer l'utilisation de leurs services pour la diffusion de contenu terroriste en ligne. Ils doivent en outre prendre des mesures spécifiques pour protéger leurs services. L'article 5 §2 donne des exemples de mesures et le §3 établit certains standards.

Toutefois, les fournisseurs de services cloud et de communication électronique, tels que définis par la directive (EU) 2018/1972, sont exclus du champ d'application de ce règlement[41].

Afin de permettre un réexamen administratif ou un contrôle juridictionnel, ou encore le traitement de réclamations, mais également pour la prévention et la détection ainsi que des

[41] G. DE GREGORIO, « Fighting Terrorism Online : Censorship, Platforms and Freedom of Expression across the Atlantic », *Virtual Freedoms, Terrorism and the Law*, G. De Minico et O. Pollicino (dir.), New York, Routledge, 2021, p. 104-105.

enquêtes et poursuites, les fournisseurs de services doivent conserver les contenus retirés et les données connexes pour un minimum de six mois voire plus, à la demande de l'autorité ou de la juridiction compétente, conformément à l'article 6.

Plusieurs obligations sont également faites aux fournisseurs de services, notamment de transparence (art. 7) et de responsabilité (art. 9 et 10).

L'article 14 prévoit également un mécanisme d'échange d'informations, de coordination et de coopération entre les fournisseurs de services, les autorités compétentes et Europol. L'article 15 oblige en outre les fournisseurs à établir des points de contact pour la réception des injonctions.

La décision du Conseil sur l'échange d'informations et la coopération concernant les infractions terroristes[42], qui s'appliquait pour les infractions de la décision-cadre 2002/475/JAI, remplacée par la directive 2017/541, s'applique également. Cette décision prévoit notamment la fourniture d'informations concernant les infractions terroristes à Eurojust, Europol et aux États membres (art. 2). Elle prévoit également la mise en place d'équipes communes d'enquête (art. 3) et la possibilité de faire des demandes d'entraide judiciaire et d'exécution de décisions judiciaires (art. 4).

Au niveau du Conseil de l'Europe, qui incrimine également la provocation publique à commettre une infraction terroriste dans son article 5, l'article 15 de la convention n°196 prévoit un devoir d'enquête, ainsi que de prendre des mesures pour assurer la présence de la personne suspecte pour les poursuites ou l'extradition, toutefois accompagné du droit pour la personne soumise à l'enquête de prendre contact avec un représentant de l'État dont elle a la nationalité, ou tout autre État apte à protéger ses droits. L'article 17 prévoit une coopération internationale la plus large possible. L'article 18 prévoit l'obligation de poursuivre en cas de refus d'extrader et l'article 19 prévoit la possibilité de l'extradition, combiné à l'article 20 qui exclut la clause d'exception politique. Seule la clause de discrimination, autrement dit la requête d'extradition pour des considérations de race, de religion ou autres, reste opposable à l'extradition selon l'article 21. L'article 22 prévoit également une information spontanée entre les États.

Le protocole additionnel prévoit en outre un échange d'informations rapide, avec un point de contact disponible 24 heures sur 24 et 7 jours sur 7, en son article 7. Et l'article 9 du protocole rend toute la convention de Varsovie applicable, sauf l'article 9 sur les infractions accessoires.

Sanctions

La directive 2017/541, en son article 15 concernant les personnes physiques, prévoit que les États membres prennent les mesures nécessaires pour que les infractions terroristes soient passibles de sanctions pénales effectives, proportionnées et dissuasives, en ce compris l'article 5. Rien de plus n'est prévu pour la provocation publique à commettre une infraction terroriste.

[42] Décision 2005/671/JAI du Conseil du 20 septembre 2005 relative à l'échange d'informations et à la coopération concernant les infractions terroristes, *J.O.U.E.*, L 253/22, 29 septembre 2005.

S'agissant des personnes morales, l'article 17 de la directive impose aux États membres de prendre les mesures nécessaires pour qu'une personne morale soit tenue pour responsable de toute infraction terroriste commise pour son compte par toute personne, qu'elle ait agi individuellement ou en tant que membre d'un organe de la personne morale et qui exerce une fonction dirigeante en son sein, lorsque cette infraction est fondée sur un pouvoir de représentation, ou encore lorsque la personne a suffisamment d'autorité pour prendre des décisions ou pour exercer un contrôle au sein de la personne morale.

La personne morale doit également pouvoir être tenue responsable, selon le §2, lorsque le défaut de surveillance ou de contrôle a rendu possible la commission de l'infraction pour son compte par une personne soumise à son autorité.

Cette disposition n'exclut pas les poursuites contre les personnes physiques auteures, instigatrices ou complices.

Concernant les sanctions, l'article 18 impose de prévoir des mesures pour que les personnes morales responsables sur base de l'article 17 soient passibles de sanctions effectives, proportionnées et dissuasives, incluant des amendes pénales ou non, et éventuellement d'autres sanctions, comme l'exclusion du bénéfice d'un avantage ou d'aides publiques, l'interdiction temporaire ou définitive d'exercer une activité commerciale, un placement sous surveillance judiciaire, une mesure judiciaire de dissolution ou encore la fermeture temporaire ou définitive d'établissements ayant servi à commettre l'infraction.

Selon l'article 18 du règlement 2021/784, les fournisseurs de service d'hébergement qui ne satisfont pas à leurs obligations établies par le règlement doivent être soumis à pénalité. En cas de persistance dans les manquements, le §3 prévoit même une pénalité jusqu'à 4% du chiffre d'affaires global de l'année précédente.

Du point de vue du Conseil de l'Europe, l'article 10 de la convention de Varsovie prévoit une responsabilité des personnes morales qui participent aux infractions, ce qui est donc plus restrictif que la directive, et ne parle que de mesures « nécessaires » pour établir la responsabilité, laissant ainsi une large marge de manœuvre aux États. Pour les personnes physiques, l'article 11, comme la directive, indique simplement la prise de mesures nécessaires pour rendre passible de peines effectives, proportionnées et dissuasives.

B. Cyberattaque terroriste

1) Moyens procéduraux

Au sein de l'Union européenne, l'article 3, i) de la directive 2017/541 fait référence aux articles 4 et 5 de la directive 2013/40/UE.

Cette directive 2013/40/UE prévoit un échange d'informations en son article 13, au moyen d'un point de contact permanent.

Dans un rayon plus large que l'Union, la convention de Budapest sera applicable pour les États qui l'auront ratifiée de sorte que l'enquête digitale au sens large sera possible. Celle-ci est détaillée plus loin.

2) Sanctions

Au sein de l'Union européenne, la directive 2017/541 ne vise les articles 4 et 5 de la directive 2013/40/UE qu'à condition que les sanctions de l'article 9, §3 ou §4 soient applicables.

L'article 9, §3 prévoit que le maximum d'emprisonnement soit d'au moins trois ans lorsque l'atteinte à un système ou aux données est commise de manière intentionnelle et qu'un grand nombre de systèmes sont touchés au moyen d'un des outils énumérés à l'article 7.

L'article 9, §4, quant à lui, prévoit que le maximum d'emprisonnement soit au minimum de 5 ans lorsque l'atteinte est commise dans le cadre d'une organisation criminelle, qu'elle cause un préjudice grave ou qu'elle soit commise contre un système d'information d'une infrastructure critique.

La convention de Budapest est applicable en dehors de l'Union, mais celle-ci ne prévoit qu'une incrimination et pas de peine minimale. L'article 13 impose seulement des sanctions effectives, proportionnées et dissuasives, incluant des peines privatives de liberté.

C. Enquête digitale de manière générale – Convention de Budapest

Comme vu au précédent chapitre, quand bien même la qualification terroriste ne pourrait pas s'appliquer, il reste que les cyberattaques font l'objet d'une incrimination à part, que l'on peut retrouver notamment dans la convention de Budapest[43]. Cette convention prévoit de nombreux moyens d'investigation et est neutre dans ses termes de sorte qu'elle s'applique aux technologies tant actuelles que futures[44].

L'article 14 de la convention prévoit en effet que les États parties à la convention appliquent les pouvoirs et procédures aux fins d'enquêtes pénales, tant à l'égard des infractions mentionnées par elle que pour toute autre infraction pénale commise au moyen d'un système informatique, ainsi qu'à la collecte de preuves électroniques pour toute infraction pénale. Toutefois, le §3 de ce même article permet aux Parties de limiter certaines des mesures.

L'article 15 limite en outre les pouvoirs et procédures au respect des droits de l'Homme et des libertés fondamentales, ainsi qu'au principe de proportionnalité.

L'Union européenne a également facilité la production et la préservation des données par un règlement (EU) 2023/1543 du 12 juillet 2023[45], afin de donner un meilleur accès aux preuves électroniques.

---

[43] Convention sur la cybercriminalité*, STE* n°185, Budapest, 23 novembre 2001, en vigueur le 1er juillet 2004.

[44] Conseil de l'Europe, *Convention sur la cybercriminalité : protocole sur la xénophobie et le racisme et deuxième protocole sur le renforcement de la coopération et de la divulgation de preuves électroniques*, rapports explicatifs et notes d'orientation, disponible sur www.coe.int/cybercrime, décembre 2023, §6, p. 200.

[45] Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale, *J.O.U.E.*, L 191/118, 28 juillet 2023.

1) Conservation rapide de données informatiques stockées

L'article 16 de la convention de Budapest permet aux États Parties d'ordonner ou d'imposer la conservation de données, y compris relatives au trafic, stockées par un système informatique lorsqu'elles sont susceptibles de perte ou de modification.

Cela s'applique à tout type de données.

2) Conservation et divulgation rapides de données relatives au trafic

L'article 17 de la convention de 2001 permet de conserver les données de trafic uniquement et d'en assurer la divulgation rapide aux autorités compétentes, pour permettre l'identification des fournisseurs de services et de la voie de transmission de la communication.

3) Injonction de produire

L'article 18 de la convention sur la cybercriminalité prévoit des mesures pour ordonner soit à une personne sur son territoire de communiquer des données informatiques en sa possession ou sous son contrôle, soit à un fournisseur de services offrant des prestations sur son territoire de communiquer les données, en sa possession ou sous son contrôle, relatives aux abonnés et concernant les services fournis, à l'exclusion des données de trafic ou de contenu (§3).

4) Perquisition et saisie de données informatiques stockées

Conformément à l'article 19 de la convention de Budapest, les États doivent adopter des mesures pour habiliter les autorités à perquisitionner ou accéder à un système informatique et aux données qui y sont stockées ou à un support de stockage informatique qui se trouve sur son territoire.

Le §4 de cet article prévoit une mesure particulière, qui est d'ordonner à toute personne connaissant le fonctionnement du système ou les mesures de protection des données qu'il contient de fournir les informations nécessaires pour permettre la saisie des données informatiques. Cela doit bien évidemment s'apprécier au regard du droit de ne pas s'incriminer.

5) Collecte en temps réel de données informatiques

Concernant les données relatives au trafic, l'article 20 enjoint les Parties à adopter des mesures pour habiliter ses autorités compétentes à collecter ou enregistrer, ou à obliger un fournisseur de services à collecter ou enregistrer ou prêter son concours aux autorités pour collecter ou enregistrer en temps réel les données relatives au trafic associées à des communications spécifiques transmises sur son territoire.

Le §3 prévoit en outre d'imposer le secret de la procédure au fournisseur de services qui aura prêté son concours à l'enquête. Il s'agit d'une exception notable au RGPD, particulièrement à l'égard du principe de transparence.

Pour ce qui est des données relatives au contenu, l'article 21 prévoit les mêmes mesures que l'article 20 mais uniquement pour des infractions graves à définir en droit interne.

La conformité de l'application de ces articles par rapport aux droits fondamentaux a fait l'objet d'un examen par la Cour européenne des droits de l'homme que nous aborderons dans la dernière partie de cet exposé.

6) Entraide en matière de mesures provisoires

En matière de coopération, l'article 29 permet aux États de demander à d'autres Parties d'ordonner ou imposer la conservation rapide de données sur leur territoire. La double incrimination n'est en principe pas requise, mais une Partie peut, au sens du §4, refuser la demande de conservation dans le cas où il est raisonnable de penser que la double incrimination ne sera pas remplie au moment de la divulgation. Les autres causes de refus sont lorsque la demande est de nature politique ou porte sur une infraction de nature politique, ou encore si cela pourrait porter atteinte à la souveraineté, sécurité, à l'ordre public ou autres intérêts essentiels de l'État. Selon la définition du terrorisme adoptée par chaque État, la motivation politique du terrorisme pourrait potentiellement faire échec à une telle demande.

L'article 30, ensuite, permet la divulgation rapide de données conservées, lorsqu'au cours de l'application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre État a participé à la transmission de la communication. Les données qui peuvent être divulguées doivent être suffisantes concernant le trafic pour identifier le fournisseur de service et la voie de communication. Les causes de refus sont les mêmes que pour l'article 29.

7) Entraide concernant les pouvoirs d'investigation

L'article 31 de la convention de Budapest prévoit la possibilité pour une Partie de demander à une autre de perquisitionner ou accéder, saisir, obtenir et divulguer des données se trouvant sur son territoire, y compris les données conservées conformément à l'article 29. Cela doit être fait aussi rapidement que possible lorsque les données sont susceptibles d'être perdues ou modifiées ou lorsque d'autres instruments internationaux prévoient une coopération rapide.

L'article 32 permet en outre à une Partie, sans autorisation, d'accéder à des données ouvertes au public, quelle que soit la localisation géographique des données, et d'accéder ou recevoir au moyen d'un système informatique situé sur son territoire des données informatiques stockées situées dans un autre État en obtenant le consentement légal et volontaire de la personne légalement autorisée à divulguer ces données.

Lors de la collecte en temps réel de données relatives au trafic, l'article 33 impose aux Parties de s'entraider, selon les conditions et procédures de droit interne, au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel serait disponible pour une affaire analogue au niveau interne.

La même chose est prévue pour l'interception de données relatives au contenu dans la mesure des traités et lois internes applicables pour la collecte ou l'enregistrement en temps réel de telles données relatives au contenu de communications spécifiques.

Enfin, l'article 35 prévoit un réseau 24/7, qui est un point de contact joignable 24h sur 24, 7 jours sur 7, désigné par la Partie pour assurer une assistance immédiate dans les investigations concernant les infractions pénales liées à des systèmes et données informatiques ou pour recueillir des preuves sous forme électronique d'une infraction pénale.

D. Incrimination du racisme et de la xénophobie – Premier protocole additionnel

Le premier protocole additionnel à la convention de Budapest[46] renforce la convention sur la cybercriminalité en prévoyant une incrimination spécifique visant le contenu raciste et xénophobe.

Son article 3 prévoit ainsi que les États parties au protocole érigent en infraction la diffusion et autres formes de mise à disposition du public, par des moyens informatiques, du matériel raciste et xénophobe. Ce matériel est défini par l'article 2 comme tout écrit, image ou représentation d'idées ou de théories, qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes en raison de la race, de la couleur, de l'ascendance, l'origine ethnique ou national, ou encore de la religion.

L'article 4 établit des mesures contre la menace d'une infraction pénale grave et l'article 5 à l'insulte en public avec une motivation raciste ou xénophobe.

Plus largement, l'article 6 incrimine également le matériel qui nie, minimise, approuve ou justifie des actes de génocide ou autres crimes contre l'humanité.

L'aide et la complicité sont également incriminés par l'article 7.

Ce Traité est entré en vigueur le 1 mars 2006 après avoir reçu 5 ratifications.

Puisqu'il vise le discours de haine, il se peut que ce protocole soit utilisé pour incriminer la propagande terroriste en ligne, là où le règlement européen trouve ses limites géographiques. Cela devra s'apprécier selon les circonstances de fait, en fonction du message, pour voir si celui-ci peut s'interpréter comme étant contre une race, une couleur, une ascendance, une origine ethnique ou nationale ou encore une religion, ou si seules des idées politiques ou un ordre social sont remises en cause, celles-ci n'étant pas visées.

[46] Protocole additionnel à la convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, *STE* n° 189, Strasbourg, 28 janvier 2003, en vigueur le 1er mars 2006.

E. Preuves électroniques – Deuxième protocole additionnel

Le deuxième protocole additionnel à la convention de Budapest[47] prévoit de renforcer la coopération entre les États signataires. Cependant, ce protocole n'est pas encore en vigueur, étant donné que son article 16 prévoit un minimum de 5 signatures pour son entrée en vigueur, et qu'à l'heure actuelle, seuls deux États l'ont ratifié.

En cas d'entrée en vigueur, l'article 5 de ce protocole prévoit une coopération la plus large possible et détaille l'ensemble des mesures prévues.

Ainsi, les articles 6 et 7 ont pour objet de renforcer la coopération directe avec les fournisseurs et entités sur le territoire d'une autre partie, peu importe qu'il existe un traité ou arrangement d'entraide avec des législations uniformes ou réciproques entre les Parties.

Les articles 8 et 9 prévoient des procédures de renforcement de la coopération pour la divulgation de données informatiques.

L'article 10 prévoit des mesures d'entraide d'urgence.

Pour finir, les articles 11 et 12 prévoient des procédures en l'absence d'accords internationaux applicables, à savoir le recueil de dépositions de témoins ou d'experts par vidéoconférence (article 11) et des équipes communes d'enquêtes et enquêtes communes (art. 12).

Cela peut s'avérer particulièrement utile, notamment dans le cas des services cloud, puisqu'il ne serait plus nécessaire de passer par les autorités de l'État sur lequel sont établis les fournisseurs de service.

En effet, le Groupe sur les preuves dans le nuage, créé en 2015 après l'examen des dispositions d'entraide par le T-CY[48] en décembre 2014, avait conclu en 2016 que les trop nombreux terminaux, services et utilisateurs ne permettait d'enregistrer qu'une très faible portion de preuves de la cybercriminalité, rendant les enquêtes impossibles, de sorte que la plupart des victimes ne pourront pas obtenir justice. Les principales difficultés que le Groupe a identifié sont le cloud, la territorialité et la compétence, ainsi que la difficulté d'obtenir un accès efficace aux preuves électroniques et à leur divulgation[49].

Au vu de ces résultats, les Parties ont alors convenu de prendre des mesures pour renforcer la coopération et la capacité des autorités judiciaire d'obtenir des preuves électroniques, c'est ce qui a donné naissance deuxième protocole additionnel[50].

Un premier point de réforme est la création d'un mécanisme simplifié d'ordres ou demandes aux fournisseurs de services de produire des informations sur les abonnés et données de trafic, afin de remplacer les demandes d'entraide trop longues et contraignantes[51].

---

[47] Deuxième Protocole additionnel à la convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques, *STE* n°224, Strasbourg, 12 mai 2022.
[48] Comité de la Convention sur la cybercriminalité.
[49] Conseil de l'Europe, *Convention sur la cybercriminalité : protocole sur la xénophobie et le racisme et deuxième protocole sur le renforcement de la coopération et de la divulgation de preuves électroniques*, rapports explicatifs et notes d'orientation, disponible sur www.coe.int/cybercrime, décembre 2023, §10, p. 201.
[50] Conseil de l'Europe, *Ibidem*, §11, p. 202.
[51] Conseil de l'Europe, *Ibidem*, §23, p. 204.

Un deuxième point est alors la possibilité d'obtenir directement auprès d'un fournisseur de service, sans passer par une demande d'entraide, la divulgation de données relatives aux abonnés, étant donné qu'elles sont les plus recherchées mais également indispensables pour les enquêtes liées à la cybercriminalité et autres crimes impliquant des preuves électroniques. Idem pour les données relatives au trafic qui doivent pouvoir faire l'objet d'une divulgation rapide pour remonter à la source d'une communication[52].

Pour éviter que la cybercriminalité ne soit facilitée par des domaines créés ou exploités à des fins criminelles, il était également important de mettre en place un dispositif pour obtenir des informations auprès de fournisseurs de services d'enregistrement de noms de domaine[53].

Le protocole visait aussi à combler les lacunes dans la disponibilité des moyens de coopération tels que les visioconférences ou les équipes communes d'enquête dans certains Parties à la convention[54].

Puisque la mise en œuvre et l'application des pouvoirs et procédures doivent être soumises à des conditions et des garanties, il a également été nécessaire d'ajouter un article à ce sujet pour protéger les droits de l'homme et libertés fondamentales. D'autant plus que la protection des données a pris un essor considérable dans les constitutions et obligations internationales des Parties à la convention[55].

F. E-Evidence Package

Au niveau de l'Union européenne, des dispositions similaires au second protocole additionnel à la convention de Budapest ont été prises. Il s'agit de ce qu'on appelle communément l' « e-evidence package », composé d'un règlement[56] et d'une directive[57].

Ces nouveaux instruments ont notamment pour objet de créer un ordre européen de production, autorisant ainsi les autorités judiciaires à obtenir des preuves électroniques directement d'un fournisseur de service ou de son représentant légal d'un autre État membre, qui sera alors obligé de répondre dans un délai de 10 jours, voire 8 heures en cas d'urgence[58].

En parallèle, un ordre européen de préservation est crée pour permettre aux autorités judiciaires de requérir d'un fournisseur de services ou son représentant légal de préserver des

---

[52] Conseil de l'Europe, *Ibidem*, §23, p. 204.
[53] Conseil de l'Europe, *Ibidem*, §23, p. 205.
[54] Conseil de l'Europe, *Ibidem*, §23, p. 205.
[55] Conseil de l'Europe, *Ibidem*, §23, p. 206.
[56] Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale, *J.O.U.E.*, L 191/118, 28 juillet 2023.
[57] Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales, *J.O.U.E.*, L 191/181, 28 juillet 2023.
[58] Commission européenne, *E-evidence – cross-border access to electronic evidence : Improving cross-border access to electronic evidence*, disponible sur https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en#documents, consulté le 12 mai 2024.

données spécifiques en vue d'une demande de production via l'assistance légale mutuelle, un ordre européen de production ou un ordre européen d'investigation[59].

Ces instruments prévoient également des garde-fous pour protéger les droits fondamentaux. Les personnes dont les données sont demandées bénéficiera donc de garanties et de remèdes légaux. Un système de notification des autorités de l'État membre sur lequel est établi le fournisseur de service requis sera également mis en place et celui-ci pourra, dans quatre hypothèses, empêcher la production des données. Une procédure spécifique devant un juge ou une Cour est également prévue en cas de conflit de lois[60].

Un système d'IT décentralisé est également créé pour permettre une communication sécurisée et fiable entre les autorités judiciaire[61].

Pour permettre le bon fonctionnement de ces instruments, les fournisseurs de service ont l'obligation de désigner un établissement ou un représentant légal au sein de l'Union. Imposer un tel système harmonisé permettra en outre d'améliorer la certitude et la clarté des règles de droits pour toutes les entreprises et fournisseurs de service[62].

Cependant, il faut mentionner que bien que les nouvelles règles soient entrées en vigueur le 17 août 2023, la directive ne s'applique que depuis le 17 février 2024 et le règlement ne s'appliquera qu'à partir du 17 août 2026. Aussi, les effets concrets de ce pack sur les preuves électroniques restent à découvrir[63].

G. Utilisation de l'IA

Une autre solution envisageable pour contrer l'utilisation du cyberespace à des fins terroristes serait d'utiliser l'intelligence artificielle. En effet, il serait assez intéressant, particulièrement pour les fournisseurs de services d'hébergement, d'utiliser l'IA afin de traiter de larges quantités de données et analyser le contenu afin d'identifier les contenus à caractère terroriste de manière automatique et permanente, moyennant peu de ressources humaines. Cela permettrait également d'augmenter la réactivité des fournisseurs de services, notamment face aux demandes judiciaires de retrait de contenu, spécialement dans l'heure comme requis par le règlement 2021/784 en son article 3[64].

Cependant, l'utilisation de l'IA pose des difficultés en raison des risques de biais et de discrimination, ce qui pourrait contrevenir à la liberté d'expression[65].

[59] Commission européenne, *Ibidem*.
[60] Commission européenne, *Ibidem*.
[61] Commission européenne, *Ibidem*.
[62] Commission européenne, *Ibidem.*
[63] Commission européenne, *Ibidem*.
[64] S. BIANCHI et al., « Artificial Intelligence to Counter Cyber-Terrorism », *IC3,* Vol. X, 2023, p. 16.
[65] S. BIANCHI, *Ibidem*, p. 17.

Le tout nouveau projet de règlement européen sur l'intelligence artificielle[66] y répond par son article 14 qui impose au déployeur[67] un contrôle humain lors de l'utilisation de systèmes d'IA à haut risque[68], proportionnellement aux risques, au niveau d'autonomie et au contexte d'utilisation du système d'IA. Ce règlement n'est toutefois pas encore entré en vigueur de sorte que son efficacité reste à voir en pratique.

Les problèmes majeurs qui demeurent dans l'utilisation de l'IA sont le manque de transparence qui touche ces systèmes, ainsi que l'imprévisibilité des résultats produits par l'IA et le manque d'explicabilité[69].

[66] Règlement (UE) 2024/… du Parlement européen et du Conseil du … établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), cor01, 16 avril 2024.

[67] Défini par l'article 3, 4) comme : « une personne physique ou morale, une autorité publique, une agence ou un autre organisme utilisant sous sa propre autorité un système d'IA, sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel. »

[68] Tel que défini aux annexes II et III.

[69] R. MONTASARI, *Countering Cyberterrorism : The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*, Cham, Springer, 2023, p. 69.

CHAPITRE III : LIMITES LIÉES AUX DROITS FONDAMENTAUX

A. Limites de la qualification terroriste

1) Liberté d'expression

Cette liberté a été inscrite pour la première fois à l'article 19 de la Déclaration universelle des Droits de l'Homme. Les principaux éléments de cette liberté sont la liberté d'opinion, des médias et de communication. Elle est garantie par divers traités des Nations Unies et du Conseil de l'Europe. On la retrouve également à l'article 10 (1) de la convention européenne des Droits de l'Homme[70].

Des restrictions peuvent toutefois s'imposer à cette liberté, mais uniquement selon les règles internationales. Ainsi, la convention internationale sur les droits civils et politiques considère que des circonstances telles que l'état d'urgence permettent de déroger à la liberté d'expression, à condition que l'État reste constant dans ses obligations internationales, que ces dérogations soient prévues par la loi et nécessaires pour le respect des droits ou de la réputation d'autrui ou pour la protection de la sécurité nationale, l'ordre public ou encore pour la santé et la moralité publique[71].

Dans le cadre du contre-terrorisme, les articles 5 de la convention internationale des droits civils et politiques et 17 de la convention européenne des Droits de l'Homme prévoient expressément des restrictions à la liberté d'expression en ce qu'il s'agit d'exploiter les droits humains pour promouvoir la haine ou avec pour objectif d'outrepasser les droits d'autrui[72].

Concernant l'utilisation d'internet pour promouvoir le terrorisme, non seulement la qualification terroriste de la propagande est souvent subjective, mais la propagande en elle-même n'est pas une activité prohibée en soi, de sorte que la question du conflit de la qualification terroriste avec la liberté d'expression se pose particulièrement[73].

La liberté d'expression n'est heureusement pas un droit absolu, de sorte qu'elle peut être restreinte en respectant les principes de légalité, proportionnalité et non-discrimination, particulièrement lorsque cette liberté est utilisée pour inciter à la discrimination, l'hostilité ou la violence. La principale difficulté reste alors de situer la limite à partir de laquelle la glorification et l'incitation au terrorisme n'est plus acceptable, ce qui varie fortement selon les pays, en fonction des différences culturelles et du background législatif[74].

Il est aussi malaisé de contrôler le nombre exorbitant de contenus publiés sur Internet. Dès lors, les opportunités de propagande se sont multipliées et diversifiées pour finir par toucher le monde entier. De plus, tant le terrorisme que le cyberespace présentent une dimension

---

[70] N. LAITALA, *Hacktivism and cyberterrorism: Human rights issues in state responses*, thèse, Prof. Z. Kedzia (dir.), Adam Mickiewicz University, 19 juin 2012, p. 13.
[71] N. LAITALA, *Ibidem*, p. 15.
[72] N. LAITALA, *Ibidem*, p. 16.
[73] UNODC Report, *The use of the Internet for terrorist purposes*, United Nations Office, New York, 2012, p. 3 et 4.
[74] UNODC Report, *Ibidem*, p. 13-14.

internationale. Or, le manque d'accord international sur la qualification terroriste rend difficile la détermination de la limite à la liberté d'expression dans le cyberespace[75].

C'est ainsi que l'on peut trouver des divergences dans la notion de liberté d'expression, notamment entre l'Union européenne, où la liberté d'expression reçoit la limite de l'abus de droit de l'article 54 de la Charte des droits fondamentaux, et les États-Unis, où, au contraire, la liberté d'expression est quasi absolue et ne peut être limitée qu'en de rares occasions[76].

La limitation de la liberté d'expression en ligne n'est pas seulement l'apanage des autorités publiques puisque les plateformes en ligne peuvent être amenées à modérer elles-mêmes le contenu publié, sur base de leurs conditions de service. Et l'utilisation de moyens automatiques pour gérer les contenus soulève d'autant plus de questions au regard des droits humains[77]. C'est pour cela que la Commission européenne est intervenue, pour rétablir la balance entre les différents intérêts, mais en se focalisant sur la transparence de la modération et les moyens de s'opposer aux décisions de modération[78]. Cela a été matérialisé par l'article 15 du règlement sur les services numériques[79].

La directive 2017/541, comme vu précédemment, impose également aux fournisseurs de service d'hébergement de coopérer avec les autorités judiciaires et de respecter plusieurs obligations relatives au contenu terroriste en ligne. Mais comme l'a précisé la Cour de justice de l'Union européenne dans un arrêt *Sabam v. Netlog*[80], il faut garder à l'esprit l'article 15 de la directive e-Commerce[81] qui interdit aux États d'imposer une surveillance généralisée. Dès lors, imposer aux fournisseurs d'hébergement un mécanisme de filtre pour surveiller activement toutes les données relatives aux utilisateurs de leurs services serait interdit[82].

Il reste que le discours de haine en lui-même n'a pas de définition précise et il est difficile de le distinguer de la simple critique[83]. Cela est d'autant plus vrai aux États-Unis, particulièrement dans le cyberespace, où le Web est vu comme un terrain neutre pour la diffusion des idées et, par conséquent, mérite une protection[84].

Pour déterminer, en Europe et au sein du Conseil de l'Europe en tous cas, la ligne de démarcation entre la liberté d'expression et le discours de haine, il est possible de se référer aux arrêts rendus par la Cour européenne des droits de l'Homme en la matière. Par exemple,

---

[75] G. DE GREGORIO, « Fighting Terrorism Online : Censorship, Platforms and Freedom of Expression across the Atlantic », *Virtual freedoms, terrorism and the law*, G. De Minico et O. Pollicino (dir.), New York, Routledge, 2021, p. 96.
[76] G. DE GREGORIO, *Ibidem*, p. 101.
[77] G. DE GREGORIO, *Ibidem*, p. 115.
[78] G. DE GREGORIO, *Ibidem*, p. 116.
[79] Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), *J.O.U.E.*, L 277/1, 27 octobre 2022.
[80] C.J.U.E., arrêt *Sabam v. Netlog*, 16 février 2012, C-360/10, ECLI:EU:C:2012:85.
[81] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), *J.O.U.E.*, L 178, 17 juillet 2000.
[82] F. ABBONDANTE, « Freedom of Speech and Social Networks in the Age of Terrorism : A Comparative Analysis », *Virtual freedoms, terrorism and the law*, G. De Minico et O. Pollicino (dir.), New York, Routledge, 2021, p. 133.
[83] F. ABBONDANTE, *Ibidem*, p. 119.
[84] F. ABBONDANTE, *Ibidem*, p. 123.

dans l'arrêt *Leroy c. France*[85], la Cour a estimé que la limite à la liberté d'expression était justifiée par la défense de la sûreté publique et que la condamnation était proportionnée à la poursuite de cet objectif dans le cas d'une caricature. Ce raisonnement est toutefois critiquable selon certains puisque la Cour a alors validé la position du juge français qui était de considérer que l'intention de l'auteur n'entrait pas en compte dans l'établissement de l'infraction, alors que l'article 5 de la convention pour la prévention du terrorisme[86] y fait expressément référence[87]. L'article 5 de la directive 2017/541 prévoit également le critère de l'intention pour la qualification de provocation publique à commettre une infraction terroriste, tout comme la convention du Conseil de l'Europe.

Un autre exemple, cette fois plus mitigé, serait l'arrêt *Rouillan c. France*[88], dans lequel la Cour a estimé qu'en glorifiant les attentats terroristes à Paris et Seine-Saint-Denis de 2015, il s'agissait bien d'une incitation indirecte à l'usage de la violence terroriste. Cependant, même si l'ingérence des autorités judiciaires pouvait être justifiée par la nécessité, elle a tout de même considéré que la sanction était disproportionnée au regard de l'objectif[89].

Ce dernier arrêt est probablement celui qui a inspiré le législateur européen lorsqu'il a rédigé l'article 5 de la directive 2017/541, qui intègre la glorification des actes terroristes dans son incrimination de la provocation publique à commettre une infraction terroriste. Il s'agit là d'une nouveauté par rapport à la convention du Conseil de l'Europe de 2005.

Des controverses au sein même de sa jurisprudence apparaissent cependant puisque tantôt les juges semblent considérer qu'il suffit, pour limiter la liberté d'expression, que le danger soit suffisamment réel et préoccupant, tantôt ils semblent requérir un danger clair et présent[90]. En cas de simple glorification ou apologie, où l'évaluation du contexte est d'autant plus importante, la Cour semble laisser une plus grande marge de discrétion aux États Membres, même sans qu'il y ait d'incitation explicite à la violence[91].

2) Hacktivisme vs cyberterrorisme

Tant l'hacktivisme que le cyberterrorisme sont motivés par des raisons politiques, idéologiques ou religieuses. Les manifestations de telles idées s'exprimaient déjà avant l'ère d'Internet, notamment par des campagnes de lettres, mais le développement de la technologie a ouvert de plus en plus de possibilités d'exprimer ses opinions, particulièrement

---

[85] Cour eur. D.H., arrêt *Leroy c. France*, 2 octobre 2008, n°36109/03.
[86] Convention du Conseil de l'Europe pour la prévention du terrorisme, *STCE* n° 196, Varsovie, 16 mai 2005, en vigueur 1er juin 2007.
[87] F. DUBUISSON, *Lutte contre le terrorisme et liberté d'expression : Le cas de la répression de l'apologie du terrorisme*, Paris, Pedone, 2018, p. 12.
[88] Cour eur. D.H., arrêt *Rouillan c. France*, 23 juin 2022, n°28000/19.
[89] Cour eur. D.H., *Guide sur la jurisprudence de la Cour européenne des droits de l'Homme – Terrorisme*, disponible sur https://ks.echr.coe.int/web/echr-ks/terrorism, mis à jour le 31 août 2023, p. 23.
[90] G.M. TERUEL LOZANO, « Freedom of Expression behind the Incitement to Terrorism in a Globalised World by the Internet », *Virtual freedoms, terrorism and the law*, G. De Minico et O. Pollicino (dir.), New York, Routledge, 2021, p. 144.
[91] G.M. TERUEL LOZANO, *Ibidem*, p. 145.

aux travers des médias sociaux[92]. Cela devient plus problématique lorsque les médias sont utilisés pour organiser ou promouvoir la violence dans la vie réelle[93].

L'hacktivisme vise l'utilisation d'hacking pour promouvoir l'activisme ou exprimer des opinions. Un exemple est l'attaque par un individu se réclamant du Front de libération animale à l'encontre d'un site web de vente de fourrure et de cuir. Cet individu a pu avoir accès et détruire des données du site en signe de protestation en faveur de la cause animale. Ce faisant, l'hacker en question a également indiqué avoir eu accès aux informations de paiement des clients de l'entreprise et proféré des menaces sur cette base[94].

L'hacktivisme a donc pour objectif de provoquer un changement social[95], il s'agit d'attirer l'attention des médias et du public en perturbant le fonctionnement normal du réseau, par des techniques d'hacking[96].

Cela se rapproche dès lors fortement de la définition du cyberterrorisme que nous avons précédemment proposée, qui visait aussi à provoquer un changement social. La majeure différence entre les deux sera donc l'intention de provoquer la terreur[97].

Les deux notions étant extrêmement larges et floues, il est difficile de les distinguer clairement. Parmi les exemples concrets, on pourra néanmoins noter que la plupart des actes de cyberterrorisme sont qualifiés comme tels car ils viennent en support de groupe eux-mêmes qualifiés de terroristes[98].

De plus, bien que les deux partagent des méthodes et un but d'attirer l'attention, une grande différence qui peut être relevée est que la plupart des groupes hacktivistes évitent de causer des dommages permanents aux infrastructures et aux autres utilisateurs alors que les cyber-terroristes ont plutôt tendance à causer un maximum de dommages irréparables[99].

En tous les cas, les uns comme les autres restent soumis à la convention de Budapest et sont passibles de sanctions, mais la qualification de terrorisme permettra sans doute une plus grande intrusion et une plus grande facilité de réaction au regard de la liberté d'expression[100].

---

[92] T.J. HOLT, A.M. BOSSLER et K.C. SEIGRFRIED-SPELLAR, *Cybercrime and Digital forensics*, 3e éd., New York, Routledge, 2022, p. 375.
[93] T.J. HOLT, A.M. BOSSLER et K.C. SEIGRFRIED-SPELLAR, *Ibidem*, p. 376.
[94] T.J. HOLT, A.M. BOSSLER et K.C. SEIGRFRIED-SPELLAR, *Ibidem*, p. 377.
[95] P. LUDLOW, « What is a Hacktivist? », *Opinionator - The New York Times*, disponible sur https://archive.nytimes.com/opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist/?searchResultPosition=1, 13 janvier 2013.
[96] N. LAITALA, *Hacktivism and cyberterrorism : Human rights issues in state responses*, thèse, Prof. Z. Kedzia (dir.), Adam Mickiewicz University, 19 juin 2012, p. 25.
[97] T.J. HOLT, A.M. BOSSLER et K.C. SEIGRFRIED-SPELLAR, *Cybercrime and Digital forensics*, 3e éd., New York, Routledge, 2022, p. 378.
[98] T.J. HOLT, A.M. BOSSLER et K.C. SEIGRFRIED-SPELLAR, *Ibidem*, pp. 378 – 380.
[99] N. LAITALA, *Op. Cit.*, p. 70.
[100] N. LAITALA, *Op. Cit.*, p. 74.

B. Limites aux pouvoirs d'enquête

1) Droit à la vie privée

Pour contrer le terrorisme, il faut parfois user de surveillance et de récolte d'informations de manière poussée, de sorte qu'il faut particulièrement veiller à protéger les personnes contre les ingérences arbitraires ou illégales dans leur droit à la vie privée[101].

Il est arrivé à plusieurs reprises que la Cour européenne des droits de l'Homme rappelle que bien que les États aient la possibilité de restreindre le droit à la vie privée dans le cadre de la lutte contre le terrorisme, cela ne leur permet pas de soumettre leurs citoyens à la surveillance secrète de manière illimitée[102].

Ainsi, par exemple, dans un cas Szabo and Vissy v. Hungary[103], la Cour européenne des droits de l'Homme a rappelé qu'il fallait respecter les principes de subsidiarité, nécessité et proportionnalité, de même que la nécessité de prévoir un mécanisme de plainte pour les personnes concernées par la surveillance[104].

La Cour de justice de l'Union européenne a également rendu des arrêts très pertinents en matière d'enquête digitale liée au terrorisme. En effet, dans un arrêt *Digital Rights*[105], elle avait invalidé la directive 2006/24[106] en ce qu'elle imposait aux fournisseurs de service de conserver des métadonnées permettant de tirer des conclusions précises concernant la vie privée des personnes. Cette immixtion dans la vie privée, selon la Cour, devait alors être assortie de garanties suffisantes[107]. La Cour a également considéré que cela pouvait constituer une entrave à la liberté d'expression en ce qu'une telle possibilité d'intrusion dans l'intimité des personnes pouvait dissuader les individus d'utiliser les réseaux de communication[108].

Dans le même sens, la Cour européenne des droits de l'Homme, dans un arrêt *Big Brother Watch*[109] s'est trouvée inquiétée du fait que les services de renseignement pouvaient procéder à des recherches et analyses de métadonnées sans aucune restriction. Ainsi, selon la Cour, les garanties s'appliquant aux données de contenu devaient pouvoir s'appliquer aux

---

[101] UNODC, *The use of the Internet for terrorist purposes*, United Nations Office, New York, 2012, p. 14.
[102] D. DERENCINOVIC, « Europe at a Crossroads – Coutering Terrorism in the Surveillance Society », *Dealing with Terrorism*, M. Engelhart et S. Roksandic Vidlicka (eds.), Berlin, Duncker & Humblot, 2019, p. 9.
[103] Cour eur. D. H., arrêt *Szabo and Vissy c. Hongrie*, 12 janvier 2016, n°37138/14, §§ 64, 68, 78 – 81 et 241 - 243.
[104] D. DERENCINOVIC, *Op. Cit.*, p. 10 – 12.
[105] C.J.U.E., arrêt *Digital Rights Ireland*, 8 avril 2014, C-293/12 et C-594/12, ECLI:EU:C:2014:238.
[106] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.U.E.*, L 105/54, 13 avril 2006.
[107] S. BACLET LOUVET, « Contre-terrorisme et droits fondamentaux des internautes : la mise à l'épreuve des juridictions européennes », *État de droit et dispositifs juridiques de lutte contre le terrorisme*, M. Boumghar et L. Delabie (dir.), Paris, Mare & Martin, 2020, p. 216.
[108] K. TURKALJ, « Les enjeux de la réglementation sur la conservation des données de communications électroniques à la lumière de la jurisprudence de la Cour de justice de l'Union européenne », *Zbornik radova Pravnog fakulteta u Splitu*, god. 57, 1/2020, p. 70.
[109] Cour eur. D.H., arrêt *Big Brother Watch et a. c. Royaume-Uni,* 13 septembre 2018, n°58170/13, 62322/14 et 24969/15, § 355.

métadonnées. Elle opère donc une fusion entre ces types de données du point de vue des garanties[110].

La Cour de justice de l'Union européenne a par la suite reprécisé les critères permettant de déroger au droit à la vie privée dans un arrêt *Tele2Sverige*[111]. En effet, la Cour impose à la réglementation nationale de se fonder sur des éléments objectifs pour ne viser qu'un public dont les données sont susceptibles d'avoir un lien, au moins indirect, avec des actes de criminalité grave ou permettant de contribuer à la lutte contre cette criminalité ou de prévenir un risque grave pour la sécurité publique. Par cela, la Cour signifie qu'imposer des mesures de surveillance à l'ensemble de la population pour tous les moyens de communication électronique ne respecte pas les limites de nécessité et proportionnalité[112].

Plus récemment, la Cour semble cependant s'assouplir, tel qu'il ressort de son avis 1/15[113] concernant le système PNR, de collecte et de traitement de données à caractère personnel par les transporteurs aériens à l'occasion de l'enregistrement des passagers. Ce système met donc en place une surveillance de l'ensemble des voyageurs en ce qu'ils seraient tous concernés par la lutte contre le terrorisme[114].

Toutefois, bien que dans son avis la Cour reconnait qu'il s'agit d'une ingérence qui peut être justifiée par l'intérêt public, validant dès lors l'idée même de ce système, elle a tout de même fait remarquer que l'accord qui lui était soumis ne se limitait pas au strict nécessaire et n'établissait pas des règles suffisamment claires et précises, notamment concernant la protection des données sensibles et la limite de conservation[115].

2) RGPD

Le RGPD vient également limiter la coopération entre les États puisqu'il impose de réclamer des garanties suffisantes pour effectuer un échange de données avec un État tiers. Pour pallier cela, la Commission européenne peut prendre des décisions d'adéquation, afin de faciliter les échanges[116].

Comme démontré par les arrêts *Schrems I*[117] et *II*[118], rendus par la Cour de justice de l'Union européenne, qui ont invalidé deux décisions d'adéquation avec les États-Unis, les standards

---

[110] S. BACLET LOUVET, *Op. Cit.*, p. 218.
[111] C.J.U.E., arrêt *Tele2Sverige AB c. Post-och telestyrelsen* et *Secretary of State for the Home Department c. Tom Watson et a.,* 21 décembre 2016, C-203/15 et C-698/15, ECLI:EU:C:2016:970, § 111.
[112] S. BACLET LOUVET, *Op. Cit.*, p. 222.
[113] C.J.U.E., *Avis 1/15*, 26 juillet 2017, §§ 149 – 150.
[114] S. BACLET LOUVET, *Op. Cit.*, p. 224.
[115] R. SERRA CRISTOBAL, « Processing Personal Data on EU Cross-Border Movements to Fight Terrorism », *Virtual freedoms, terrorism and the law*, G. De Minico et O. Pollicino (dir.), New York, Routledge, 2021, p. 58.
[116] C. POULY, « La lutte contre le terrorisme et la protection de la vie privée : Surveillance de masse, une cruelle nécessité ? », *La lutte contre le terrorisme*, S. Jacopin et A. Tardieu (dir.), Paris, A. PEDONE, 2017, p. 240.
[117] C.J.U.E., *Maximillian Schrems v. Data Protection Commissioner*, 6 octobre 2015, C-362/14, ECLI:EU:C:2015:650.
[118] C.J.U.E., *Data Protection Commissioner* v. *Facebook Ireland, Maximillian Schrems*, 16 juillet 2020, C-311/18, ECLI:EU:C:2020:559.

européens, notamment en termes de proportionnalité pour la conservation des données à caractère personnelle, ne permettent pas un transfert libre de données.

En effet, la Cour a jugé que les États-Unis, en ce que les autorités judiciaires américaines étaient autorisées à accéder à des données personnelles sans aucune distinction, limitation ou exception en fonction d'un but précis, ne donnaient pas de garanties suffisantes pour que le transfert de données puissent se faire dans le respect du RGPD[119].

[119] C. POULY, *Op. Cit.*, p. 241.

CONCLUSION

Cela a été rapporté tout au long de cette étude, l'ère numérique apporte son lot de défis dans la lutte contre le terrorisme. En effet, si elle donne des moyens assez efficaces de lutter contre le terrorisme sous ses différentes formes, sur le plan international, le manque de consensus en fait surtout un allié des terroristes qui y trouvent une ressource fort utile à leur expansion et à leurs actions, mais surtout à leur propagande. Par ailleurs, la technologie peut s'avérer, comme nous l'avons vu, assez dangereuse pour les droits fondamentaux qui peuvent vite se retrouver bafoués par l'utilisation de la technologie au sein des autorités judiciaires.

Ainsi que nous l'avons vu dans la première partie, l'utilisation d'internet par les terroristes n'est à l'heure actuelle reconnue directement que par le droit de l'Union européenne de manière limitée. En effet, la qualification terroriste n'est donnée qu'à des actes de cybercriminalité très spécifiques.

La seconde partie a permis de démontrer que les moyens d'action dans la sphère digitale sont nombreux et peuvent être fort intrusifs.

C'est pour cette raison que les juridictions tentent d'y réintroduire les droits fondamentaux, ce qui a fait l'objet de notre troisième partie.

Dans la détermination de la limite des moyens d'enquête, la qualification terroriste est particulièrement utile, puisqu'elle permet de faire sauter de nombreux verrous. En effet, le terrorisme étant une menace grave pour sûreté nationale, les critères de proportionnalité sont beaucoup plus rapidement rencontrés lorsqu'un acte reçoit cette qualification. La Cour européenne des droits de l'Homme a ainsi jugé dans plusieurs affaires que le terrorisme était un danger public qui permettait l'application de l'article 15 de la convention européenne des droits de l'Homme, et donc des dérogations en cas d'état d'urgence[120].

Or, le terrorisme n'a pour l'instant pas reçu de définition légale à proprement dit. En effet, les sources de droit international se limitent le plus souvent à répertorier divers actes particuliers, sans jamais définir la notion de terrorisme en elle-même. Cela rend d'autant plus difficile l'octroi de la qualification terroriste aux actes commis dans le cyberespace puisque la cybercriminalité est elle-même à peine émergente et ne connait pas non plus de définition légale plus générale, elle vise également des actes spécifiques.

Pour l'application des divers instruments spécifiques au terrorisme que nous avons répertoriés au chapitre 2, cette difficulté est à prendre en compte.

Dans la provocation et le contenu terroriste, le règlement 2017/784 permet en effet des injonctions de retrait et une coopération renforcée des États pour ce faire, ainsi que des obligations de vigilance et de responsabilisation pour les fournisseurs de service d'hébergement. Mais cela est limité par la liberté d'expression telle qu'interprétée par la Cour européenne des droits de l'Homme et la Cour de justice de l'Union européenne, dont quelques exemples sont cités dans la dernière partie de ce travail. Le contexte est alors

[120] Nous renvoyons sur ce point au guide de la Cour européenne des droits de l'homme en la matière : Cour eur. D.H., *Guide sur l'article 15 de la Convention européenne des droits de l'homme – Dérogation en cas d'état d'urgence*, disponible sur https://ks.echr.coe.int/web/echr-ks/article-15, mis à jour le 31 août 2023.

hautement important pour définir les contenus qui peuvent recevoir la qualification terroriste ou non. La convention du conseil de l'Europe ayant des termes très similaires, la difficulté est la même. À mentionner dès lors que l'utilisation de l'IA pourrait s'avérer injuste dès lors qu'une évaluation humaine du contexte est indispensable.

Il en va de même, dans une moindre mesure, pour les actes de cybercriminalité, puisqu'on peut retrouver des manifestations en ligne similaires aux mouvements de protestation dans la vie réelle, qui sont les hacktivistes, dont la répression est malaisée puisque certains considèrent qu'il s'agit d'une simple manifestation d'idées qui doit être protégée par la liberté d'expression. Là aussi, les difficultés de définition des différents concepts sont à prendre en compte puisque la limite entre l'hacktivisme et le cyberterrorisme, ainsi que leurs limites par rapport à la liberté d'expression, s'en retrouve floutée.

Ces phénomènes étant relativement récents, il n'y a à l'heure actuelle que peu de jurisprudence pour permettre de déterminer les cas qui peuvent être classés dans le terrorisme et recevoir une plus grande dérogation par rapport aux droits fondamentaux.

Pour ce qui est de l'enquête digitale, elle aussi trouve ses limites. Les moyens technologiques actuels permettent une intrusion dans la vie privée beaucoup plus grande que par le passé puisque nombre de choses de la vie courante se font désormais de manière électronique. Cela engendre un amas de données gargantuesque qui peut révéler le moindre détail de la vie des personnes.

Avec l'avènement de l'IA, ces données peuvent être plus facilement scannées et engendrer une surveillance de masse hors de tout contrôle humain, entraînant des conséquences parfois injustes, notamment en cas de biais.

Les moyens d'enquête digitaux ont surtout été développés par la convention de Budapest, en 2001, de sorte qu'il existe beaucoup plus de jurisprudence à ce sujet. Mais la plupart de ces arrêts sont cependant récents puisque, depuis 2001, la technologie a encore fortement évolué et son utilisation s'est beaucoup étendue. Les possibilités sont devenues plus nombreuses et son contrôle beaucoup moins évident.

Le risque d'outrepasser le droit à la vie privée s'en trouve grandi. C'est pour cela qu'une fois encore la qualification terroriste revêt de l'importance puisqu'elle donne une plus grande marge de manœuvre du point de vue de la nécessité et de la proportionnalité.

Les divergences existantes en matière de notion de sécurité nationale engendrent également des difficultés dans la coopération entre les États, notamment au regard du RGPD. Cela se voit particulièrement avec les États-Unis, où les possibilités d'ingérence des pouvoirs publics en vertu de la sécurité nationale sont beaucoup plus étendues qu'en Europe. C'est ce qui a donné lieu à l'annulation de deux décisions d'adéquation par la Cour de justice de l'Union européenne dans les arrêts Schrems I et II. La nouvelle décision d'adéquation de juillet 2023 pourrait d'ailleurs bien déboucher sur un nouvel arrêt. Elle a déjà fait l'objet d'une requête de la part d'un parlementaire français et une adhésion de la part Maximilian Schrems à ce recours est pressentie pour la suite[121].

[121] M. BARCZENTEWICZ, « Schrems III : Gauging the Validity of the GDPR Adequacy Decision for the United States », *ICLE*, 25 septembre 2023, p. 2.

En définitive, les instruments présentés au cours de cette étude peuvent être considérés comme un bon début, lorsqu'ils sont interprétés au regard de la jurisprudence de la Cour européenne des droits de l'Homme et de la Cour de justice de l'Union européenne. Mais une mise à jour s'impose pour combler les lacunes qui existent du fait de l'absence de définition des différentes notions, notamment de terrorisme, de l'expansion de l'utilisation des services de cloud ou encore du développement de l'IA.

En effet, par exemple, comme nous l'avons vu, les services cloud et de communication ne sont pas visés par le règlement 2021/784 alors que ceux-ci prennent une ampleur considérable.

De plus, les actes visés par la directive 2017/541 ne concernent pas l'ensemble des actes répertoriés par la convention de Budapest, particulièrement en ce qui concerne les outils technologiques illégaux qui peuvent constituer un atout considérable pour le terrorisme.

À l'avenir, plus de recherches pourraient également être réalisées à propos de l'utilisation de l'IA, qui vient de faire ses débuts dans le droit européen avec l'AI Act et le Digital Services Act.

Par ailleurs, la relation de l'Europe avec les États-Unis en matière de droit de la protection des données personnelles est également appelée à évoluer dans un futur proche et pourra également être revue.

BIBLIOGRAPHIE

A. Doctrine

ABBONDANTE F., « Freedom of Speech and Social Networks in the Age of Terrorism : A Comparative Analysis », *Virtual freedoms, terrorism and the law*, G. De Minico et O. Pollicino (dir.), New York, Routledge, 2021, p. 119.

BACLET LOUVET S., « Contre-terrorisme et droits fondamentaux des internautes : la mise à l'épreuve des juridictions européennes », *État de droit et dispositifs juridiques de lutte contre le terrorisme*, M. Boumghar et L. Delabie (dir.), Paris, Mare & Martin, 2020.

BOISTER N., *An introduction to transnational criminal law*, 2e éd., New York, Oxford, 2018.

COHEN D., « Cyber terrorism : Case studies », *Cyber Crime and Cyber Terrorism Investigator's Handbook*, B. Akhgar, A. Staniforth et F. Bosco (dir.), Watham, Elsevier, 2014, pp. 165 – 174.

COLLIER B. et HUTCHINGS A., « Cybercrime : A social ecology », *the Oxford handbook of criminology* (7e éd.), A. Liebling, S. Maruna, L. McAra (dir.), New York, Oxford, 2023, pp. 456 – 478.

DE GREGORIO G., « Fighting Terrorism Online : Censorship, Platforms and Freedom of Expression across the Atlantic », *Virtual freedoms, terrorism and the law*, G. De Minico et O. Pollicino (dir.), New York, Routledge, 2021, pp. 95 – 117.

DERENCINOVIC D., « Europe at a Crossroads – Coutering Terrorism in the Surveillance Society », *Dealing with Terrorism*, M. Engelhart et S. Roksandic Vidlicka (eds.), Berlin, Duncker & Humblot, 2019, pp. 3 – 16.

DUBUISSON F., *Lutte contre le terrorisme et liberté d'expression : Le cas de la répression de l'apologie du terrorisme*, Paris, Pedone, 2018.

HOLT T.J., BURRUSS G.W. et BOSSLER A.M., *Policing Cybercrime and Cyberterror*, Durham, C.A.P., 2015.

HOLT T.J., BOSSLER A.M. et SEIGRFRIED-SPELLAR K.C., *Cybercrime and Digital forensics*, 3e éd., New York, Routledge, 2022.

INNES M. et LEVI M., « Making and managing terrorism and counter-terrorism : the view from criminology », *the Oxford handbook of criminology* (7e éd.), A. Liebling, S. Maruna, L. McAra (dir.), New York, Oxford, 2023, pp. 653 – 675.

JEWKES Y. et YAR M., *Handbook of Internet Crime*, Cullompton, Willan, 2009.

LAITALA N., *Hacktivism and cyberterrorism : Human rights issues in state responses*, thèse, Prof. Z. Kedzia (dir.), Adam Mickiewicz University, 19 juin 2012.

LUIIJF E., « Definitions of Cyber Terrorism », *Cyber Crime and Cyber Terrorism Investigator's Handbook*, B. Akhgar, A. Staniforth et F. Bosco (dir.), Watham, Elsevier, 2014, pp. 11 – 17.

MACDONALD S., JARVIS L. et LAVIS S. M., « Cyberterrorism Today ? Findings From a Follow-on Survey of Researchers », *Studies in Conflict & Terrorism*, New York, Routledge, 2022, 45:8, pp. 727-752.

MONTASARI R., *Countering Cyberterrorism : The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*, Cham, Springer, 2023.

POLLICINO O., « Enforcement of the Right to Digital Privacy », *Virtual freedoms, terrorism and the law*, G. De Minico et O. Pollicino (dir.), New York, Routledge, 2021, pp. 23 - 44.

POULY C., « La lutte contre le terrorisme et la protection de la vie privée : Surveillance de masse, une cruelle nécessité ? », *La lutte contre le terrorisme*, S. Jacopin et A. Tardieu (dir.), Paris, A. PEDONE, 2017, pp. 227 - 243.

SERRA CRISTOBAL R., « Processing Personal Data on EU Cross-Border Movements to Fight Terrorism », *Virtual freedoms, terrorism and the law*, G. De Minico et O. Pollicino (dir.), New York, Routledge, 2021, pp. 45 - 62.

TERUEL LOZANO G.M., « Freedom of Expression behind the Incitement to Terrorism in a Globalised World by the Internet », *Virtual freedoms, terrorism and the law*, G. De Minico et O. Pollicino (dir.), New York, Routledge, 2021, p. 135 – 156.

B. Articles de revues

BARCZENTEWICZ M., « Schrems III : Gauging the Validity of the GDPR Adequacy Decision for the United States », *ICLE*, 25 septembre 2023, p. 2.

BIANCHI S., MANCUSO M., PATERNOSTER C., KALPAKIS G., TSIKRIKA T., VROCHIDIS S., KOSHUHAROVA D. et JAEGER B., « Artificial Intelligence to Counter Cyber-Terrorism », *Proceedings of the International Conference on Cybersecurity and Cybercrime*, Vol. X, 2023, pp. 12 – 21.

DUBUISSON F., « La définition du ″terrorisme″ : débats, enjeux et fonctions dans le discours juridique », *Confluences Méditerranée*, 2017/3 (n°102).

KEMPF O., "Le cyberterrorisme : un discours plus qu'une réalité », *Hérodote*, 2014/1-2 (n°152-153), pp. 82 - 97.

LUDLOW P., « What is a Hacktivist? », *Opinionator - The New York Times*, disponible sur https://archive.nytimes.com/opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist/?searchResultPosition=1, 13 janvier 2013.

PASTRANA SANCHEZ A., « A critical concept of terrorism for criminal prosecution », *INECS*, 2022, n°17, article 6.

TURKALJ K., « Les enjeux de la réglementation sur la conservation des données de communications électroniques à la lumière de la jurisprudence de la Cour de justice de l'Union européenne », *Zbornik radova Pravnog fakulteta u Splitu*, god. 57, 1/2020, pp. 53 – 84.

C. Sources de droit international et européen

Union européenne

Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), *J.O.U.E.*, L 178, 17 juillet 2000.

Décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme, *J.O.U.E.*, L 164, 22 juin 2002.

Décision 2005/671/JAI du Conseil du 20 septembre 2005 relative à l'échange d'informations et à la coopération concernant les infractions terroristes, *J.O.U.E.*, L 253/22, 29 septembre 2005.

Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.U.E.*, L 105/54, 13 avril 2006.

Directive 2013/40/EU du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, *J.O.U.E.*, L 218/8, 14 août 2013.

Directive (EU) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil, *J.O.U.E.*, L 88/6, 31 mars 2017.

Décision (UE) 2018/889 du Conseil du 4 juin 2018 relative à la conclusion, au nom de l'Union européenne, de la convention du Conseil de l'Europe pour la prévention du terrorisme, *J.O.U.E.*, L 159/1, 22 juin 2018.

Décision (UE) 2018/890 du Conseil du 4 juin 2018 relative à la conclusion, au nom de l'Union européenne, du protocole additionnel à la convention du Conseil de l'Europe pour la prévention du terrorisme, *J.O.U.E.*, L 159/15, 22 juin 2018.

Règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne, *J.O.U.E.*, L 172/79, 17 mai 2021.

Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), *J.O.U.E.*, L 277/1, 27 octobre 2022.

Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale, *J.O.U.E.*, L 191/118, 28 juillet 2023.

Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales, *J.O.U.E.*, L 191/181, 28 juillet 2023.

Règlement (UE) 2024/… du Parlement européen et du Conseil du … établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), cor01, 16 avril 2024.

Conseil de l'Europe

Convention sur la cybercriminalité, *STE* n°185, Budapest, 23 novembre 2001, en vigueur le 1er juillet 2004.

Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, *STE* n° 189, Strasbourg, 28 janvier 2003, en vigueur le 1er mars 2006.

Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques, *STE* n°224, Strasbourg, 12 mai 2022.

Convention du Conseil de l'Europe pour la prévention du terrorisme, *STCE* n° 196, Varsovie, 16 mai 2005, en vigueur 1er juin 2007.

Protocole additionnel à la Convention du Conseil de l'Europe pour la prévention du terrorisme, *STCE* n°217, Riga, 22 octobre 2015, en vigueur le 1er juillet 2017.

D. Jurisprudence

Cour de justice de l'Union européenne

C.J.U.E., arrêt *Sabam v. Netlog*, 16 février 2012, C-360/10, ECLI:EU:C:2012:85.

C.J.U.E., arrêt *Digital Rights Ireland*, 8 avril 2014, C-293/12 et C-594/12, ECLI:EU:C:2014:238.

C.J.U.E., *Maximillian Schrems v. Data Protection Commissioner*, 6 octobre 2015, C-362/14, ECLI:EU:C:2015:650.

C.J.U.E., arrêt *Tele2Sverige AB c. Post-och telestyrelsen* et *Secretary of State for the Home Department c. Tom Watson et a.,* 21 décembre 2016, C-203/15 et C-698/15, ECLI:EU:C:2016:970, § 111.

C.J.U.E., *Avis 1/15*, 26 juillet 2017, §§ 149 – 150.

C.J.U.E., *Data Protection Commissioner* v. *Facebook Ireland, Maximillian Schrems*, 16 juillet 2020, C-311/18, ECLI:EU:C:2020:559.

Cour européenne des Droits de l'Homme

Cour eur. D.H., arrêt *Leroy c. France*, 2 octobre 2008, n°36109/03.

Cour eur. D. H., arrêt *Szabo and Vissy c. Hongrie*, 12 janvier 2016, n°37138/14.

Cour eur. D.H., arrêt *Big Brother Watch et a. c. Royaume-Uni,* 13 septembre 2018, n°58170/13, 62322/14 et 24969/15.

Cour eur. D.H., arrêt *Rouillan c. France*, 23 juin 2022, n°28000/19.

E. Autres sources officielles

UNODC Report, *The use of the Internet for terrorist purposes*, United Nations Office, New York, 2012, p. 3 et 4.

Cour eur. D. H., *Guide sur la jurisprudence de la Cour européenne des droits de l'Homme – Terrorisme*, disponible sur https://ks.echr.coe.int/web/echr-ks/terrorism, mis à jour le 31 août 2023.

Cour eur. D.H., *Guide sur l'article 15 de la Convention européenne des droits de l'homme – Dérogation en cas d'état d'urgence*, disponible sur https://ks.echr.coe.int/web/echr-ks/article-15, mis à jour le 31 août 2023.

Conseil de l'Europe, *Convention sur la cybercriminalité : protocole sur la xénophobie et le racisme et deuxième protocole sur le renforcement de la coopération et de la divulgation de preuves électroniques*, rapports explicatifs et notes d'orientation, disponible sur www.coe.int/cybercrime, décembre 2023.

Commission européenne, *E-evidence – cross-border access to electronic evidence : Improving cross-border access to electronic evidence*, disponible sur https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en#documents, consulté le 12 mai 2024.