La définition fonctionnelle de la notion de cybercriminalité

par Romain Ciswicki
Doctorant en droit public à l'Université de Grenoble-Alpes
ATER à l'Université de Lorraine à Nancy

Le terme de *« cyber »* renvoie aux nouvelles technologies du numérique, et en particulier l'Internet. La *« criminalité »* est une traduction littérale de l'anglais *criminality*, qui concerne le droit pénal – ou *criminal law* – plutôt que la notion française de criminalité ou de criminologie. Ainsi, il serait plus juste de parler de *« cyberdélinquance »* ou de *« cyberinfraction »*, même si le terme couvre bien l'ensemble des comportements prohibés, et non spécifiquement à la catégorie des crimes en droit français. Il est dès lors possible de considérer que la cybercriminalité concerne l'ensemble des actes en lien avec les nouvelles technologies, en particulier de l'information et de la communication dont Internet, et prohibés par le droit pénal. C'est d'ailleurs la définition générale retenue par le gouvernement français en des termes quasiment identiques. Selon cette définition, la cybercriminalité concerne *« toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet »*[1].

Il apparait que la lutte contre la cybercriminalité doit être transnationale pour répondre à ce phénomène globalisé, qui remet en cause la notion physique de frontière comme cadre géographique de la répression. Il faut dès lors, pour que la lutte contre la cybercriminalité soit efficace, respecter un certain parallélisme des formes, et que les États s'accordent sur une définition commune de la cybercriminalité. Or, cette nécessité se heurte aux conceptions nationales, qui se traduisent par un droit pénal largement hétérogène dans ce domaine. Comme pour la lutte contre le terrorisme ou pour les questions relatives à la protection de l'environnement, la cybercriminalité met au défi la notion de territorialité et plus

1. *Protéger les internautes*, Rapport du groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014, p. 12.

largement le volontarisme étatique, éléments régulateurs du droit international, non seulement du fait de l'aspect globalisé des réseaux informatiques, mais aussi des conséquences susceptibles d'être engendrées.

Au niveau international, il est donc nécessaire que le droit se saisisse de ce phénomène, dans le but de sécuriser le cyberespace et de réguler son utilisation, de même que les informations qui y sont contenues, ou qui y transitent. À cet égard, il semble indispensable de proposer une définition de la cybercriminalité au niveau international, préalable indispensable pour que les juges puissent identifier les comportements entrant dans son champ matériel. Il convient cependant de constater qu'une telle approche conceptuelle apparait inefficace pour lutter au niveau supranational contre ce phénomène (**I**). Face à cette inefficacité, une approche fonctionnelle semble nécessaire (**II**).

I. L'inefficacité d'une appréhension conceptuelle de la cybercriminalité

L'approche conceptuelle consiste ici à s'intéresser à la notion même de cybercriminalité dans le but de pouvoir y rattacher l'ensemble de ses manifestations. Cette appréhension induit la nécessité d'une définition générale de la notion. Dans le contexte de la cybercriminalité, cette appréhension semble inefficace du fait la polymorphie de la notion (**A**). De ce fait, les États adoptent des solutions différentes pour un même acte pouvant être considéré comme cybercriminel (**B**).

A. Une inefficacité liée à la polymorphie de la notion

La cybercriminalité peut prendre des formes très différentes, puisque l'infraction peut être directement liée aux technologies de l'information et de la communication ou indirectement liée à ces technologies. Ainsi, les réseaux informatiques peuvent constituer la cible de l'infraction, en particulier lorsqu'il s'agit d'une atteinte au système informatique lui-même ou aux données informatiques qui y sont contenues. De même, les réseaux informatiques peuvent aussi constituer le moyen de commettre ou de faciliter une infraction dite classique, ils ne sont dès lors qu'un vecteur à cette infraction. La cybercriminalité peut également résulter d'une combinaison des deux. Cette polymorphie fait d'elle un phénomène difficilement conceptualisable, ce qui rend périlleuse toute tentative de définition générale. Dès lors, l'ensemble des actes susceptibles d'entrer dans le champ matériel de la cybercriminalité n'est pas identifiable de manière précise. Une définition trop large aurait le défaut de l'imprécision, alors qu'une définition étroite se heurterait à l'hétérogénéité des actes visés.

La notion a pourtant fait l'objet de plusieurs tentatives de définition au niveau international, sans qu'aucune ne soit réellement contraignante. Ainsi,

l'Organisation de coopération et de développement économiques (OCDE) fut la première organisation internationale à s'être intéressée à la fraude liée à l'informatique, proposant notamment un état des lieux des législations existantes, et faisant état de propositions de réformes. Il en résulte la définition suivante : *« l'abus informatique est tout comportement illégal, contraire à l'éthique ou non autorisé, qui concerne un traitement automatique et/ou une transmission de données »*[2]. Les caractéristiques retenues pour cette criminalité concernent *« l'entrée, l'altération, l'effacement et /ou la suppression de données et de programmes dans l'intention de commettre un transfert illégal de dons, de commettre un faux ou d'entraver le fonctionnement du système informatique et/ou de télécommunication ; la violation du droit exclusif du détenteur d'un programme informatique protégé dans l'intention de l'exploiter commercialement et de le mettre sur le marché ; l'accès dans un système informatique et/ou de télécommunications ou l'interception d'un tel système fait sciemment et sans l'autorisation du responsable du système, en violant les règles de sécurité ou dans une intention malhonnête ou nuisible »*[3]. Elle constitue une définition consensuelle ne permettant pas une harmonisation des législations nationales, puisqu'elle renvoie à une démarche dictée par une vision interne. De plus, la référence à des éléments relevant de l'éthique semble peu satisfaisante sur le plan juridique, du fait de la diversité des traditions juridiques et sociétales. L'approche pénale semble demeurer la principale solution envisageable[4].

Au niveau onusien, la cybercriminalité correspond à *« Toute infraction susceptible d'être commise à l'aide d'un système ou d'un réseau informatique, dans un système ou un réseau informatique ou contre un système ou un réseau informatique »*[5]. Ici encore, cette définition demeure peu satisfaisante, en ce qu'elle ne permet pas d'appréhender de manière conceptuelle la notion de cybercriminalité, bien qu'elle fasse référence au système informatique ou au réseau informatique. Elle ne renvoie pas à des comportements précis, et les États ne peuvent s'y référer pour adopter des législations uniformes. D'ailleurs, l'Organisation reconnaît expressément les difficultés liées à la définition de la cybercriminalité, en insistant sur le caractère *« artificiel »* du terme et en rappelant la diversité de ses formes ainsi que de ses conséquences[6]. Elle permet cependant de dégager *« un certain consensus de base sur les comportements cybercriminels à réprimer »*, qui porte sur les contenus numériques, tels ceux à caractère obscène, ou encore les paris en ligne et le

2. *La fraude liée à l'informatique : analyse des politiques juridiques*, rapport de l'OCDE, Paris, 1986, p. 7.
3. *Ibid*.
4. H. Altermann & A. Bloch, « La fraude informatique », *Gaz. Pal.*, 3 septembre 1988, (246-247), p. 2-6.
5. *La prévention du crime et le traitement des délinquants,* Dixième Congrès des Nations-Unies, Vienne, 10-17 avril 2000.
6. *Étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États membres, la communauté internationale et le secteur privé pour y faire face*, rapport de l'ONUDC, 2013, UNODC/CCPCJ/EG.4/2013/2.

recours à des cybermarchés illicites, par exemple pour le trafic de drogue et la traite des êtres humains. De même, les atteintes à la confidentialité, à l'intégrité et à l'accessibilité des systèmes informatiques font également l'objet d'un certain consensus au niveau des législations nationales, même si *« l'analyse détaillée des dispositions des textes législatifs analysés révèle des approches divergentes »*[7].

B. Une inefficacité conduisant à des solutions différentes

Il convient tout d'abord de rappeler que, du fait de sa dimension pénale, et en l'absence de toute prise en compte internationale, la notion renvoie à des actes prohibés par les législations nationales. La détermination de cette législation appartient aux États, qui disposent du monopole de la qualification pénale, et qui décident dès lors souverainement des actes considérés comme illicites. Cette affirmation se retrouve dans la sémantique du principe de légalité, qui renvoie à la loi nationale et au principe légaliste de la souveraineté de la loi comme expression de la volonté générale d'une Nation[8]. Le principe de légalité de protéger les individus contre l'arbitraire a également et indirectement pour effet de confier le monopole de la détermination des infractions cybercriminelles aux États, creusant ainsi les divergences étatiques et réduisant les chances d'un consensus autour de la notion de cybercriminalité. Cela peut se révéler problématique, dans la mesure où les moyens développés par les cybercriminels pour commettre leurs actes illicites semblent induire une nécessaire adaptation de la matière juridique[9]. La célérité de l'évolution technologique s'oppose à la pesanteur du travail législatif, qui repose sur la volonté aléatoire d'une société à appréhender un comportement illicite comme tel.

En l'absence de définition générale et contraignante de la cybercriminalité au niveau international, les États adoptent ainsi une vision de la cybercriminalité qui leur est propre. Un acte cybercriminel peut donc très bien être considéré comme tel dans un État alors qu'il ne l'est pas dans un autre, conduisant à des solutions hétérogènes à l'égard de certains comportements identiques. Un exemple concerne les atteintes à la propriété intellectuelle. Face à la pratique massive du téléchargement illégal via Internet, le législateur français a posé un cadre légal spécifique à ce type d'atteinte par deux lois de 2009[10], de même qu'il

7. *Ibid*.
8. B. de Lamy, « Dérives et évolution du principe de la légalité en droit pénal français : contribution à l'étude des sources du droit pénal français », *Les Cahiers de droit*, 50 (3-4), 2009, p. 587.
9. J. Pradel, « Les infractions relatives à l'informatique », *Revue internationale de droit comparé*, 1990, 42-2, p. 815-816.
10. Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet (loi dite « HADOPI I ») ; loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet (loi dite « HADOPI II »).

a créé la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI), autorité administrative indépendante de lutte contre les atteintes aux droits d'œuvres protégées[11]. Ainsi, l'article L. 336-3 du Code de la propriété intellectuelle oblige le titulaire de l'abonnement internet à veiller à la sécurisation de son accès contre toute utilisation portant atteinte au droit d'auteur ou à un droit voisin. De plus, la loi de 2016 relative à la liberté de la création, à l'architecture et au patrimoine[12] modifiant l'article L. 336-2 du Code de la propriété intellectuelle prévoit la possibilité pour un titulaire de droits sur les œuvres et objets protégés de demander au Tribunal de grande instance, statuant en la forme des référés, ou au Centre national du cinéma et de l'image animée, d'ordonner toutes mesures propres à prévenir ou à faire cesser une atteinte à un droit d'auteur ou à un droit voisin.

Ce dispositif de lutte a donné l'occasion au Tribunal de grande instance de Paris de rendre trois décisions majeures sur la base de l'article L. 336-2 du Code de la propriété intellectuelle. Il a été ordonné en 2013 la fermeture de seize sites relevant du site de streaming *Allostreaming* qui proposaient une *« représentation des œuvres sans avoir obtenu l'autorisation des auteurs et une reproduction des mêmes œuvres »*[13]. De même, il a ordonné le blocage des sites de téléchargement illégal *The Pirate Bay* et de ses miroirs en 2014[14], et *T411* en 2015[15]. Au cours de cette dernière affaire, la société *Free*, partie à l'instance, avait souligné la facilité pour les internautes de contourner ces mesures de blocage, ce à quoi les juges avaient répondu que *« les mesures sollicitées visent le plus grand nombre des utilisateurs, lesquels n'ont pas nécessairement le temps et les compétences pour rechercher les moyens de contournement que les spécialistes trouvent et conservent en mémoire »*, confirmant dès lors la relative inefficacité de ces mesures. Ces sites étant hébergés à l'étranger, et les mesures française ne concernant que les internautes français, il est assez aisé de trouver par une simple recherche des solutions pour contourner le blocage des sites *The Pirate Bay* et *T411* accompagnées de tutoriels permettant au plus grand nombre de les mettre en œuvre[16]. Par conséquent, si les dispositions du droit français sont particulièrement protectrices de la propriété intellectuelle, ces trois affaires mettent en lumière la nécessité de mettre en œuvre une lutte internationale contre cette pratique.

11. De manière plus précise, la triple mission d'HADOPI consiste en la promotion du développement de l'offre légale et l'observation de l'utilisation licite et illicite des œuvres sur Internet, la protection des œuvres à l'égard des atteintes aux droits qui leur sont attachés dans le cadre de la réponse graduée, et en la régulation de l'usage des mesures techniques de protection.
12. Loi n° 2 016-925 du 7 juillet 2016 relative à la liberté de la création, à l'architecture et au patrimoine.
13. TGI Paris, 28 novembre 2013, n° 11/60 013.
14. TGI Paris, 4 décembre 2014, n° 14/03 246.
15. TGI Paris, 2 avril 2015, n° 14/08 177.
16. Une solution consiste au changement du *Domain Name System (D.N.S.)*.

Face à ce constat, et dans le but d'éviter l'émergence de *« paradis digitaux »*, par analogie aux *« paradis fiscaux »*[17] et de lutter contre l'émergence de réseaux cybercriminels, il est absolument nécessaire d'harmoniser les différentes législations nationales au sujet de la cybercriminalité. Il faut dès lors qu'une infraction qualifiée comme telle dans un État soit également érigée en infraction dans d'autres États pour lutter efficacement contre la cybercriminalité, et que la sanction encourue soit identique, ou en tout cas suffisamment dissuasive.

II. La nécessité d'une appréhension fonctionnelle de la cybercriminalité

Contrairement à l'appréhension conceptuelle, l'approche fonctionnelle consiste à déterminer les manifestations de la cybercriminalité, permettant ainsi de clarifier son contenu. Si cette appréhension est réalisée par le Conseil de l'Europe (**A**), elle demeure cependant insuffisante pour lutter efficacement contre la cybercriminalité (**B**).

A. Une appréhension fonctionnelle réalisée par le Conseil de l'Europe

La Convention du Conseil de l'Europe sur la cybercriminalité signée à Budapest le 23 novembre 2001[18] constitue le seul instrument contraignant au niveau international. Elle vise à harmoniser les législations nationales sur la cybercriminalité. L'intérêt est de proposer une définition fonctionnelle de la notion de cybercriminalité, c'est-à-dire d'élaborer une liste d'infractions qui devront être reprises dans les droits nationaux. Elle évite ainsi toute tentative de conceptualisation, qui ne permet pas d'identifier avec certitude l'ensemble des actes susceptibles de faire l'objet d'une qualification pénale. Elle va au contraire s'intéresser plutôt aux manifestations de la cybercriminalité. Ainsi, la Convention de Budapest précise que relèvent de la cybercriminalité certaines infractions générales telles que l'accès illégal et l'interception illégale, l'atteinte à l'intégrité des données et du système, l'abus de dispositif, ainsi que la falsification informatique et la fraude informatique[19]. De même, la Convention identifie des infractions spécifiques

17. S. Ghernaouti & A. Dufour, *Internet*, Paris, PUF, coll. « Que sais-je ? », 2017, p. 110.
18. Convention du Conseil de l'Europe sur la cybercriminalité, Budapest, 23 novembre 2001, STCE n° 185.
19. Art. 2 à 8 de la Convention de Budapest. L'article 2 concerne l'accès intentionnel et sans droit à tout ou partie d'un système informatique ; l'article 3 incrimine l'interception intentionnelle et sans droit de données informatiques ; l'article 4 définit cette infraction comme le fait intentionnel et sans droit d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques ; l'article 5 concerne l'entrave grave, inten-

dont l'objet est déterminé avec les infractions se rapportant à la pornographie enfantine et les infractions liées aux atteintes à la propriété intellectuelle[20]. Il convient aussi d'ajouter les propos de nature raciste et xénophobe au titre du protocole additionnel à la Convention de Budapest[21].

Cette énumération exhaustive constitue la définition fonctionnelle de la notion de cybercriminalité. Elle possède un double avantage : tout d'abord, elle permet d'identifier et de définir avec certitude les différents actes et comportements relevant de la cybercriminalité, pour qu'ils soient repris dans les législations internes des États, puisque les actes sont clairement définis par la Convention. Au-delà de la qualification de ces infractions, la Convention précise également que doivent être érigées en infraction pénale la complicité et la tentative[22]. Les sanctions doivent être effectives, proportionnées et dissuasives[23], ce qui pose un cadre relatif dans la détermination de la peine par les États. Ensuite, elle fait de la Convention un véritable instrument vivant, puisqu'une définition générale de la cybercriminalité pourrait devenir obsolète du fait de l'évolution technologique. Par cette approche, de nouvelles infractions peuvent être ajoutées par le biais de protocoles additionnels. Le protocole relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques a ainsi permis d'ajouter de telles infractions au dispositif conventionnel.

Il convient également de préciser que la Convention est ouverte à la signature aux États non-membres du Conseil de l'Europe, ce qui donne à cet instrument une véritable portée mondiale, absolument nécessaire en vue de lutter efficacement contre la cybercriminalité. Le Conseil de l'Europe apparait dès lors comme une organisation visant la sensibilisation, la persuasion, la valorisation, ou encore l'émulation des bonnes pratiques[24]. N'étant pas l'acteur principal de la lutte contre la cybercriminalité, puisque les États procèdent à la qualification pénale, l'Organisation assure néanmoins un cadre de négociation favorisant la convergence des volontés, tout en garantissant une approche potentiellement universelle avec l'ouverture aux États non-européens. En outre, ce cadre de négociation

---

tionnelle et sans droit, au fonctionnement d'un système informatique ; l'article 6 vise à interdire la production, la vente, l'obtention ou la possession d'un dispositif ou d'un mot de passe pour la commission des infractions précédemment évoquées ; les articles 7 et 8 concernent les techniques de tromperie comme la falsification de documents officiels par des moyens informatiques, ou d'escroquerie comme par exemple la fraude à la carte bancaire ou lors de paiements en ligne.

20. Art. 9 et 10 de la Convention de Budapest.

21. 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, Strasbourg, 28 janvier 2003, *STCE* n° 189.

22. Art. 11 de la Convention.

23. Art. 13 de la Convention.

24. J.-P. Willaime, « Le Conseil de l'Europe face à la diversité culturelle et religieuse », *Les Champs de Mars*, 2015/1, n° 26, p. 153.

permet d'aboutir à un instrument juridique contraignant, évitant les risques d'une fragmentation du droit par la conclusion d'accords bilatéraux[25].

B. Une appréhension fonctionnelle insuffisante

Face à ces avantages, des difficultés subsistent dans la lutte contre la cybercriminalité par le Conseil de l'Europe. La technique conventionnelle reste privilégiée, ce qui fait de lui une organisation internationale dont les actes demeurent soumis au consentement des États membres exprimé par la signature et la ratification, et au sein de laquelle les injonctions impératives et contraignantes se heurtent à sa dimension géographique, et à la diversité culturelle de ses États membres[26].

Ainsi, cette définition fonctionnelle ne vaut que pour les États qui ont souverainement décidé de participer à la lutte contre la cybercriminalité, en signant et ratifiant la Convention. Or, pour lutter efficacement contre la cybercriminalité, il est absolument nécessaire que la totalité des États, ou du moins une vaste majorité, dispose d'une législation similaire en la matière. La Convention de Budapest compte soixante et une ratifications[27]. Ce total est important dans la recherche d'un instrument à dimension internationale, et ce face à l'importante diversité des législations de ces États. Il reste cependant éloigné d'une véritable appréhension globale. En ce qui concerne les États membres du Conseil de l'Europe, seuls la Russie, l'Irlande, Saint Marin et la Suède n'ont pas ratifié la Convention. En ce qui concerne les États non-membres, on compte seulement dix-huit ratifications. Le problème est plus important concernant le protocole additionnel, puisqu'il ne compte que trente et une ratifications des États membres ou non membres du Conseil. Dix-neuf États membres du Conseil de l'Europe n'ont pas ratifié la Convention, tandis que seulement trois signatures d'États non-membres ont fait l'objet d'une ratification. La relative faiblesse de la participation est problématique, puisque la Convention ne constitue qu'un socle minimal d'infractions qui doit être complété au fur et à mesure par des protocoles additionnels. Par conséquent, le risque de fragmentation de la lutte est réel, notamment lorsqu'il s'agira d'étoffer le dispositif de nouvelles infractions.

De même, le risque est de voir apparaître une véritable dilution au fur et à mesure des protocoles additionnels qui concerneraient des infractions liées à certaines traditions juridiques. On peut ainsi craindre une appréhension *a minima* de la cybercriminalité, avec des infractions consensuelles. Par exemple, aucune infraction relative à l'injure ou à la diffamation commise par le biais d'un système informatique, en particulier sur les réseaux sociaux, puisque le Protocole

25. F. Benoit-Rohmer & H. Klebes, *Le droit du Conseil de l'Europe, vers un espace juridique paneuropéen*, Éditions du Conseil de l'Europe, 2005, p. 98.
26. J.-L. Burban, *Le Conseil de l'Europe*, P.U.F., « Que sais-je ?», 3e édition, n° 885, 1996, p. 18.
27. coe.int., consulté le 18 décembre 2018.

ne concerne que les propos racistes et xénophobes. Loin d'être négligeable dans son contenu, il illustre pourtant les difficultés de cette recherche d'harmonisation des législations nationales du fait d'un niveau de protection différent de la liberté d'expression. La Cour européenne des droits de l'homme permet une uniformisation relative de ce standard de protection, mais uniquement au niveau européen. En outre, il est notamment possible de relever l'absence d'infractions liées à l'incitation au terrorisme. Une approche similaire a été adoptée par le Conseil de l'Europe avec la Convention du 16 mai 2005 pour la prévention du terrorisme[28], qui impose aux États de prendre certaines mesures au niveau national. Elle prévoit des dispositions relatives à la coopération internationale, sans que les États ne puissent mettre en œuvre les moyens d'enquête liés au cyberespace stipulés par la Convention de Budapest, et en particulier des prérogatives en termes de collecte en temps réel de données informatiques[29].

De plus, le degré de précision du dispositif conventionnel doit permettre aux États de définir et de sanctionner ces infractions de manière uniforme, sans qu'il n'y ait de doute sur le sens de ces infractions. Cette absence de marge d'appréciation pour le législateur national, et *a fortiori* pour le juge national ne laisse aucune place à l'interprétation pour la prise en compte de nouveaux actes cybercriminels. La Convention prévoit un certain nombre d'infractions sans pour autant poser des éléments identificateurs, avec une définition générale en particulier. Une telle définition aurait eu l'avantage de guider les États lorsqu'ils mettent en conformité leur droit national avec la Convention, tout en leur permettant de conserver une certaine marge d'appréciation quant à d'autres formes de cybercriminalité hors nomenclature. De ce fait, la cybercriminalité aurait abouti à une prise en compte plus large, alors qu'elle doit être regardée dans le strict cadre des définitions de la Convention et du Protocole additionnel. Elle ne répond donc à aucune autre forme de logique que la volonté des États, dans la mesure où ceux-ci décident qu'un acte est cybercriminel mais ne le constatent pas. La logique est inversée, puisqu'au lieu de se saisir d'un phénomène par un travail de conceptualisation, ses contours sont artificiellement tracés. Ainsi, certains actes susceptibles d'être considérés comme relevant naturellement et sans équivoque à la cybercriminalité pourrait être ignorés du fait d'une volonté des États de ne pas l'incriminer. Enfin, sur le plan organique, l'interprétation et la mise en œuvre de la Convention sont confiées au Comité de la Convention sur la cybercriminalité (T-CY)[30] constitué

28. Convention du Conseil de l'Europe pour la prévention du terrorisme, Varsovie, 16 mai 2005, *STCE* n° 196.

29. Art. 20 de la Convention qui concerne la collecte en temps réel de données relatives au trafic : cette disposition concerne à la fois l'habilitation des autorités étatiques compétentes, mais aussi l'obligation pour les fournisseurs de services à procéder à cette collecte, et à prêter son concours et son assistance pour une telle collecte.

30. Art. 46 alinéa 1 de la Convention de Budapest : *« Les Parties se concertent périodiquement, au besoin, afin de faciliter : a. l'usage et la mise en œuvre effectifs de la présente Convention, y compris l'identification de tout problème en la matière, ainsi que les effets de*

des États Parties. Il convient de se demander si l'instrument pourra de ce fait faire l'objet d'une interprétation dynamique et évolutive comme la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe par le juge de Strasbourg, qui a par exemple tiré de la protection du droit au respect de la vie privée et familiale une jurisprudence liée à la protection des données personnelles[31]. Une telle interprétation pourrait se révéler judicieuse pour appréhender une notion de cybercriminalité en constante mutation du fait des avancées technologiques.

En conclusion, l'approche fonctionnelle du Conseil de l'Europe apparait comme nécessaire pour lutter efficacement contre la cybercriminalité, sans qu'elle ne soit toutefois pleinement satisfaisante. Elle doit s'accompagner à la fois d'une plus large adhésion des États, mais aussi de nouvelles infractions pour compléter et étoffer la notion de cybercriminalité. Cette appréhension fait office de modèle, repris par exemple par l'Union européenne, qui dispose d'une force normative bien plus importante. Cependant, la Convention de Budapest demeure le seul instrument juridique contraignant à vocation globale. Il semble nécessaire de s'appuyer sur les projets GLACY et GLACY+ (Action Globale sur la Cybercriminalité en français), ce dernier étant mené conjointement par Conseil de l'Europe et l'Union européenne, et visant à promouvoir la Convention dans le monde et à assister les États dans sa mise en œuvre, en particulier par des formations et des partages d'expériences. Ce projet semble porter ses fruits, puisque l'on constate une vague de ratification depuis 2017 avec douze nouveaux États, dont la Grèce, Monaco et Andorre pour les États membres du Conseil de l'Europe, ainsi que l'Argentine, le Cap-Vert, le Chili, le Costa Rica, le Maroc, le Paraguay, les Philippines, le Sénégal, et les Tonga.

---

toute déclaration ou réserve faite conformément à la présente Convention ; b. l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique ; c. l'examen de l'éventualité de compléter ou d'amender la Convention ».

31. CEDH (Gde Ch.), 4 décembre 2008, *S. et Marper C. Royaume-Uni*, req. n° 30 562/04 et 30 566/04, § 67 : *« le simple fait de mémoriser les données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 ».*