INTRODUCTION

Le 9 août 2024, l'Assemblée générale des Nations Unies a adopté la Convention sur la cybercriminalité, un texte considéré par ses proponents comme une étape majeure dans la mise en place d'un cadre juridique universel pour répondre aux cybermenaces modernes. Ces dernières incluent non seulement le piratage de données sensibles, mais aussi des actes tels que les attaques par ransomware, la fraude en ligne ou les intrusions dans des infrastructures critiques, qui ont des répercussions internationales.[1]

L'adoption de cette Convention a suscité de vives critiques, notamment de la part des défenseurs des droits numériques[2] et des détracteurs de la Convention de Budapest, officiellement connue sous le nom de « Convention sur la cybercriminalité »,[3] qui estiment que la nouvelle Convention s'en éloigne trop peu tant, tant dans son approche générale que dans son contenu. Les menaces aux droits humains liées à cette Convention méritent ainsi de faire l'objet d'une attention particulière : s'agit-il de menaces découlant des textes d'incrimination, qui pourraient élargir de manière excessive les infractions en matière de cybercriminalité, ou des dispositifs procéduraux, tels que l'harmonisation des procédures pénales et les mécanismes de coopération internationale ?

Les critiques ont d'abord exprimé des préoccupations quant aux nouveaux pouvoirs de surveillance électronique transfrontalière accordés par la Convention. En effet, ces dispositions instaurent une coopération internationale en matière de surveillance et d'enquête relative à tout « *crime grave* », une notion que chaque État peut en grande partie définir selon ses propres critères, ce qui soulève des inquiétudes quant au risque d'abus et aux atteintes aux libertés fondamentales, telles que la protection de la vie privée et la liberté d'expression. Un point particulièrement préoccupant concerne les régimes autoritaires qui pourraient utiliser ces mécanismes de coopération internationale pour renforcer leur contrôle interne. Les risques d'abus sont exacerbés par l'absence

---

[1] Pour de plus amples informations sur la genèse de la nouvelle Convention, voir G. PRIYANDITA; B. HOGEVEEN, "The UN cybercrime Convention: a victory for state sovereignty", (2024) *The Strategist*, disponible sur: https://www.aspistrategist.org.au/the-un-cybercrime-Convention-a-victory-for-state-sovereignty/ . Il est également rappelé que la Convention attend toujours d'être adoptée par l'Assemblée générale des Nations Unies.

[2] À cet égard, il a été noté de manière critique que, bien que l'objectif déclaré de la Convention soit la prévention et la répression de la cybercriminalité (cf. article 1), son champ d'application inclut également la collecte et l'utilisation de preuves électroniques dans le cadre d'enquêtes et de procédures pénales, et ce, non seulement pour les infractions liées à la cybercriminalité, mais également pour « toute infraction pénale » (article 23, paragraphe 2, alinéa c)). Voir B. SAUL, Human Rights Assessment of the Draft United Nations Cybercrime Convention Statement by the United Nations Special Rapporteur on the promotion and protection of human rights while countering terrorism, disponible sur: https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/2024-07-25-stm-SR-CT-Cybercrime-Convention.pdf. Voir également S. DUROY, L. KHASANOVA, Cyberespionage and Human Rights: A Disappointing Balance, in A. SEGURA SERRANO (ed.), *Global Cybersecurity and International Law,* London, 2024, ch. 7.

[3] Sur cette Convention, voir J. CLOUGH. "A world of difference: The Budapest Convention on Cybercrime and the challenges of Harmonisation." *Monash University Law Review,* 40.3 (2014), p. 698-736; J. CLOUGH, "The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World", *Crim Law Forum*, 23, (2012), p. 363–391.

de normes harmonisées et contraignantes pour définir ce qui constitue un « crime grave », laissant chaque État libre de fixer ses propres critères.

Malgré ces préoccupations légitimes, auxquelles s'ajoutent celles relatives aux normes en matière de juridiction (Art. 22),[4] la Convention constitue néanmoins un cadre juridique visant à renforcer la coopération internationale contre les cybercrimes transnationaux, tels que les attaques par phishing, les ransomwares et les attaques par déni de service (DDoS), qui menacent à la fois les individus, les entreprises et les États. En définissant des normes communes pour la qualification des infractions et les procédures judiciaires, ce texte vise donc à améliorer l'harmonisation entre les juridictions nationales et à garantir des réponses plus efficaces aux menaces numériques.

Ensuite, bien que la Convention établisse des principes pour la protection des droits humains, nombre de critiques estiment que ces garanties demeurent insuffisantes.[5] L'article 6, paragraphe 2, stipule en effet que : « *rien dans cette Convention ne doit être interprété comme permettant la suppression des droits de l'homme ou des libertés fondamentales* », mais cette disposition, bien qu'importante, reste largement théorique en l'absence de mécanismes de contrôle rigoureux pour en assurer l'application effective. Par exemple, l'absence d'un organe de supervision dédié, tel qu'un comité d'experts indépendants, affaiblit les garanties des droits humains incluses dans le texte.

L'objectif du présent article est d'examiner si, en l'absence de telles garanties, certains États pourraient contourner leurs obligations en matière de droits humains sous couvert de lutte contre la cybercriminalité.

I. LES GARANTIES DES DROITS HUMAINS INSCRITES DANS LA CONVENTION ET LEURS FAIBLESSES

[4] À cet égard, il convient de se pencher sur les observations de E. SCHER-ZAGIER, 'The New UN Cybercrime Treaty Is a Bigger Deal Than Even Its Critics Realize' (2024) *Lawfare,* disponible sur: https://www.lawfaremedia.org/article/the-new-un-cybercrime-treaty-is-a-bigger-deal-than-even-its-critics-realize. Il souligne qu'une des dispositions du traité autoriserait les États à exercer leur juridiction sur des actes extraterritoriaux causant du préjudice à leurs ressortissants, une notion connue sous le nom de juridiction personnelle passive. Il met également en lumière que, selon cette interprétation de la juridiction personnelle passive dans le cadre du traité sur la cybercriminalité, la Russie pourrait, par exemple, demander l'assistance de la Turquie pour surveiller et extrader un journaliste américain en vacances à Istanbul. Ce journaliste aurait mis au jour une base de données mal configurée et aurait rapporté l'exposition des données personnelles de citoyens russes, un acte qui pourrait être considéré comme un accès illégal selon l'article 7. En outre, il est pertinent de consulter le même auteur dans son essai intitulé 'Jurisdictional Creep: The UN Cybercrime Convention and the Expansion of Passive Personality Jurisdiction', *Yale Journal of Law & Technology*, 27 (2024), en ligne.

[5] C. PLUMB, 'Understanding the UN's new international treaty to fight cybercrime', (2024) *UN CPR*, disponible sur: https://unu.edu/cpr/blog-post/understanding-uns-new-international-treaty-fight-cybercrime

Cette section s'attache à analyser les garanties des droits humains intégrées dans la Convention sur la cybercriminalité, en mettant en évidence le fragile équilibre qui existe entre la sécurité numérique et la protection des droits fondamentaux.[6] Nous nous pencherons plus spécifiquement sur les articles 6 et 24 à 30, qui jouent un rôle crucial non seulement dans la sauvegarde des libertés individuelles, mais également dans l'octroi aux États des instruments nécessaires pour combattre la criminalité en ligne. Une attention particulière portera sur les risques potentiels d'abus et les dérives autoritaires, particulièrement dans les régimes politiques où des pratiques de surveillance illégale peuvent se développer.

A) Article 6 : enjeux et défis pour concilier droits fondamentaux et lutte contre la cybercriminalité

L'article 6, paragraphe 2, constitue un pilier central de la Convention, réaffirmant que les droits et libertés fondamentaux ne doivent en aucun cas être sacrifiés sous prétexte de la lutte contre la cybercriminalité. Cette disposition, précédée par une autre qui stipule que : « *Les États parties veillent à ce que la mise en œuvre de leurs obligations en vertu de la présente Convention soit conforme à leurs obligations en vertu du droit international des droits de l'homme* », souligne que les États ont non seulement l'obligation de respecter ces droits, comme s'il ne s'agissait que d'obligations négatives, mais aussi de les promouvoir activement, en assumant des obligations positives. Autrement dit, il ne suffit pas de s'abstenir de porter atteinte aux droits de l'homme ; les États doivent également prendre des mesures concrètes pour les garantir. Cependant, bien que ces dispositions soient cruciales sur le plan théorique, l'absence de mécanismes robustes et clairs pour surveiller la conformité des États à ces principes suscite des préoccupations quant à l'efficacité de leur application. En effet, une simple déclaration de principes ne peut assurer la protection des droits et libertés fondamentaux sans des actions concrètes et des systèmes de contrôle rigoureux, visant à garantir que ces droits soient véritablement respectés dans la pratique.

La question de la mise en œuvre des principes généraux de la Convention touche directement à la volonté politique des États et à leur capacité d'intégrer ces dispositions dans leur cadre législatif national.[7] Bien que la Convention des Nations Unies sur la cybercriminalité ait été saluée comme une avancée significative dans la coopération internationale pour lutter contre la criminalité en ligne, elle repose essentiellement sur la bonne foi des États dans le respect et l'application de leurs

[6] J. PIELEMEIER, 'Rethinking the United Nations Cybercrime Treaty', (2024) *Just Security,* disponible sur: https://www.justsecurity.org/100333/rethinking-united-nations-cybercrime-treaty/

[7] UN NEWS, 'Global Cybercrime Treaty: A delicate balance between security and human rights', 2024, disponible sur: https://news.un.org/en/interview/2024/02/1146772

engagements. Cette approche laisse donc la place à des disparités potentielles dans l'interprétation et l'application des normes relatives aux droits humains. Certains États pourraient, par exemple, être tentés de restreindre les droits et libertés fondamentaux sous le prétexte de combattre la cybercriminalité, ce qui n'est pas interdit de manière absolue par l'article 6 susmentionné, invoquant des motifs de sécurité nationale ou de stabilité sociale. Une telle latitude pourrait conduire à des abus, compromettant ainsi l'équilibre entre la sécurité et la protection des droits fondamentaux, qui reste l'un des défis principaux de l'application de cette Convention.

Concrètement, la mise en œuvre des engagements relatifs aux droits humains dans le cadre de la nouvelle Convention sur la cybercriminalité pourrait être entravée par plusieurs défis majeurs.[8]

En premier lieu, le manque de sensibilisation et l'absence d'engagement concret des États à instituer des comités de suivi ou des mécanismes d'évaluation pour vérifier leur conformité aux obligations internationales représentent un obstacle notable.[9] Ces dispositifs sont pourtant essentiels pour garantir que les engagements pris à l'échelle mondiale soient traduits en actions concrètes au niveau national. Sans une structure robuste de suivi, l'efficacité de la Convention serait considérablement affaiblie, laissant place à des interprétations erronées, voire abusives, de ses dispositions. Cela risquerait de perturber l'équilibre délicat entre la lutte contre la cybercriminalité et la protection des droits et libertés fondamentaux.

En outre, l'absence d'un organe de contrôle indépendant pour superviser l'application de la Convention aggrave ces préoccupations. Un tel organe serait essentiel pour surveiller les mesures adoptées par les États et garantir leur conformité aux droits fondamentaux. Sans une telle supervision extérieure, le risque est grand que certains gouvernements exploitent la lutte contre la cybercriminalité pour justifier des politiques répressives, aboutissant à des violations des droits humains. La marge de manœuvre laissée aux États dans l'interprétation et l'application des dispositions de la Convention reflète une lacune structurelle qui pourrait favoriser des abus au détriment des libertés individuelles. Il apparaît donc crucial de renforcer les mécanismes de suivi et d'intégrer une supervision indépendante pour assurer une application cohérente et respectueuse des droits humains.

Un exemple frappant de ce risque réside dans la manière dont certains gouvernements, notamment au sein de régimes autoritaires, peuvent exploiter la lutte contre la cybercriminalité pour justifier des mesures répressives. Ces mesures incluent souvent la surveillance de masse, la censure de l'information, la répression des dissidents et, dans certains cas, l'arrestation de journalistes ou d'activistes sous des accusations de cybercriminalité ou d'infractions informatiques définies de

[8] T. MICKELLEA, "A United Nations Convention on cybercrime." *Cap. UL Rev*. 48 (2020), p.189.

[9] A. GUINCHARD, "Towards a supportive legal environment for global cybersecurity: the case for a public interest defense in international legal instruments on cybercrime." *Global Cybersecurity and International Law.* Routledge, 2024, p. 193-214.

manière vague. Cette tendance inquiétante a déjà été observée dans plusieurs pays, où des lois sur la cybercriminalité sont détournées pour restreindre la liberté d'expression et réprimer l'opposition politique. En l'absence de garanties robustes en matière de droits humains et d'une supervision indépendante, la Convention pourrait, involontairement, faciliter ces dérives autoritaires.

Si l'idée d'un comité de suivi dédié à la protection des droits fondamentaux semble pertinente dans ce contexte, il convient de s'interroger sur sa faisabilité dans le cadre d'une Convention dont l'objectif principal est l'harmonisation des droits nationaux pour lutter contre la cybercriminalité. D'autres Conventions pénales ou de coopération internationale, telles que la Convention de Palerme sur la criminalité transnationale organisée ou la Convention de Budapest sur la cybercriminalité, n'intègrent pas de comités de suivi spécifiquement chargés de la protection des droits humains. Cependant, ces instruments prévoient des mécanismes de coopération technique ou des réunions périodiques entre les parties pour évaluer la mise en œuvre générale.

Le manque de clarté et prévisibilité dans les procédures d'enquête relatives à la cybercriminalité, notamment en matière de collecte de données personnelles et de surveillance en ligne, représente une source croissante de préoccupation. L'absence de clarté concernant la manière dont ces enquêtes sont conduites, ainsi que les pouvoirs étendus octroyés aux autorités, pourrait favoriser une surveillance disproportionnée, menaçant ainsi la vie privée des citoyens. Cette surveillance, lorsqu'elle n'est pas encadrée par des garanties légales strictes, devient un véritable danger pour les libertés individuelles et la protection des données personnelles. Toutefois, la Convention demeure ambigüe quant aux exigences spécifiques en matière de transparence et de supervision judiciaire qui devraient accompagner ces enquêtes, laissant ainsi des zones d'ombre préoccupantes.

Par ailleurs, un autre obstacle à la mise en œuvre efficace des engagements en matière de protection des droits humains de la Convention réside dans la diversité des cadres juridiques nationaux. En accordant aux États une marge de manœuvre pour adapter ses dispositions à leurs législations nationales, la Convention risque de créer des écarts significatifs dans la protection des droits humains. Dans les pays où l'État de droit est fragile, les engagements pris au titre de la Convention pourraient se limiter à de simples déclarations d'intention, sans réelle traduction pratique, ouvrant ainsi la voie à des violations potentielles des droits fondamentaux. Les disparités législatives entre les différents pays, combinées à des priorités politiques divergentes, compliquent l'établissement de normes universelles robustes pour protéger les libertés individuelles tout en luttant efficacement contre la cybercriminalité.

B) Articles 24 à 30 : limites et risques pour les droits fondamentaux face à la lutte contre la Cybercriminalité

Un aspect particulièrement critique de la nouvelle Convention sur la cybercriminalité se trouve dans l'article 24, qui stipule dans son premier paragraphe que chaque État partie doit s'assurer que : « *l'établissement, la mise en œuvre et l'application des pouvoirs et procédures prévus dans ce chapitre (Chapitre IV) soient soumis aux conditions et aux garanties établies par son droit national*». Cette formulation, que l'on peut qualifier de regrettable, apparaît sous des formes légèrement différentes dans d'autres dispositions du même chapitre, notamment aux articles 28 et 30. Cette disposition délègue la responsabilité de la protection des droits humains aux législations nationales de chaque État, ce qui suscite des inquiétudes quant à la cohérence et l'efficacité des garanties offertes à l'échelle internationale. Dans les contextes où les législations nationales sont déjà insuffisantes pour assurer une protection adéquate des droits humains, cette situation pourrait entraîner des conséquences graves, voire désastreuses. Certains États pourraient ainsi exploiter les mesures de lutte contre la cybercriminalité pour légitimer des restrictions sur la liberté d'expression ou pour cibler des opposants politiques, compromettant des droits fondamentaux. Cette dynamique pose non seulement des questions sur la protection des individus, mais accentue également le risque d'une dérive autoritaire sous prétexte de sécurité nationale.

De plus, cette dépendance à la législation nationale met en lumière des questions cruciales concernant la cohérence et l'universalité des protections offertes. En effet, si chaque État est libre d'appliquer ses propres normes, il devient d'autant plus difficile d'assurer une protection uniforme des droits humains à l'échelle internationale. La protection des droits fondamentaux doit demeurer une priorité centrale, même face à l'augmentation de la criminalité numérique. Il est également essentiel de reconnaître que certains États, en s'appuyant sur leurs propres définitions de la « cybercriminalité », pourraient mettre en place des lois qui, au lieu de protéger les citoyens, viseraient à renforcer le contrôle étatique.[10] Par exemple, certaines législations sur la « cybercriminalité » peuvent inclure des dispositions qui permettent aux autorités de surveiller ou d'interférer dans la vie privée des citoyens sous prétexte de lutte contre les actes criminels en ligne.

Prenons l'exemple de certains pays qui, au nom de la sécurité nationale ou de la lutte contre la radicalisation, peuvent adopter des lois très larges permettant la surveillance des communications

[10] En Russie, par exemple, la loi dite "Yarovaya" adoptée en 2016 oblige les fournisseurs de services numériques à conserver les données des utilisateurs et à les mettre à disposition des services de sécurité. Bien que présentée comme une mesure antiterroriste, cette loi a suscité des critiques internationales, car elle donne aux autorités un accès large et peu encadré aux informations privées des citoyens, ce qui pourrait être utilisé pour réprimer la dissidence. Amplius, voir Media Law, 'Data Retention under the 2016 "Yarovaya Law"', (2016) Russia: Disrupting the European Status Quo?', disponible sur: https://www.medialaws.eu/data-retention-under-the-2016-yarovaya-law-in-russia-disrupting-the-european-status-quo/

privées ou l'accès aux données personnelles des citoyens, sans réel contrôle judiciaire. Cela peut ainsi donner lieu à des abus, où les droits à la vie privée, à la liberté d'expression et même à un recours judiciaire effectif seraient compromis. En 2018, par exemple, la France a adopté une loi sur la cybercriminalité renforçant les pouvoirs de surveillance des autorités.[11] Si cette loi vise à protéger les citoyens contre les attaques informatiques, elle a également été critiquée pour les risques qu'elle fait peser sur la vie privée, notamment en raison de la possibilité d'une surveillance accrue sur Internet sans garanties suffisantes pour les libertés individuelles.[12] Ce type de situation montre comment une législation mal encadrée, même avec de bonnes intentions, peut évoluer vers un renforcement du contrôle étatique.

Les implications de cette lacune sont particulièrement préoccupantes dans les régimes autoritaires, où la justification au nom de la sécurité nationale est fréquemment invoquée pour mettre en œuvre des mesures répressives. À cet égard, il est important de souligner que des pays tels que la Chine, la Russie et l'Iran ont adopté des législations en matière de cybercriminalité qui, sous couvert de sécurité numérique, ont été utilisées pour réprimer la dissidence et restreindre les libertés fondamentales.[13] Ces régimes, en se prévalant de la nécessité de protéger leurs citoyens contre des menaces cybernétiques, justifient souvent des actions qui visent à museler les voix critiques, à surveiller les activités en ligne des citoyens et à contrôler l'accès à l'information.

Il convient également de souligner que les articles 28 à 30 de la Convention, qui traitent de la recherche et de la saisie de données électroniques ainsi que de la collecte en temps réel de données de trafic, sont non seulement peu clairs, mais accordent une grande discrétion aux États. L'article 28 impose à chaque État partie d'adopter des mesures législatives permettant à ses autorités compétentes d'accéder à des systèmes d'information et de communication ainsi qu'à des données électroniques stockées. Toutefois, cette disposition ne précise pas suffisamment les conditions dans lesquelles cet accès doit être exercé, ce qui crée un flou juridique.

De même, l'article 30 stipule que chaque État partie doit adopter les mesures nécessaires pour permettre à ses autorités de collecter ou d'enregistrer des données, y compris des données de contenu, en temps réel, via des moyens techniques. Cela inclut également la possibilité de contraindre un fournisseur de services à coopérer avec les autorités pour la collecte de données spécifiques. Cette latitude, combinée à l'absence de clarté, soulève des préoccupations quant à la

[11] Pour des approfondissements sur la législation française en matière de cybercriminalité, voir D. CHILSTEIN, 'Législation sur la cybercriminalité en France', (2010) *Revue internationale de droit comparé*, p. 553-606.

[12] M. MACIEL-HIBBARD, ' Protection des données personnelles et cyber (in) sécurité', (2018) *Politique étrangère*, p. 55-66.

[13] S. ARSENE, 'La Chine et le contrôle d'Internet. Une cybersouveraineté ambivalente', (2019) *Annuaire Français de Relations Internationales*, p. 20.

protection en particulier de la vie privée et à la potentielle instrumentalisation de ces mesures à des fins répressives.

De même encore, l'article 59, en matière d'implémentation de la Convention, prévoit, aux paragraphes 1 et 2, que : "*Chaque État partie doit prendre les mesures nécessaires, y compris législatives et administratives, conformément aux principes fondamentaux de son droit interne, pour garantir l'application de ses obligations au titre de cette Convention.*" Par ailleurs, "*chaque État partie peut adopter des mesures plus strictes ou sévères que celles prévues par cette Convention pour prévenir et combattre les infractions établies conformément à celle-ci."*

Ainsi, la grande discrétion laissée aux États dans l'application de ces articles et d'autres dispositions similaires pourrait favoriser des abus, notamment par des enquêtes menées sans les garanties juridiques nécessaires. Les mesures d'investigation, qui devraient être soumises à des contrôles rigoureux pour protéger la vie privée des individus, risquent ainsi de devenir des instruments de répression. Par conséquent, la question de la protection des droits humains dans le cadre de la Convention mérite d'être posée avec une acuité renouvelée.

C) Les risques pour les droits humains associés aux pouvoirs d'enquête reconnus par la Convention

Un aspect particulièrement alarmant de la nouvelle Convention réside dans sa capacité à permettre aux États d'établir des procédures d'enquête qui pourraient être utilisées pour surveiller illégalement leurs citoyens. Par exemple, la possibilité de collecter des données en temps réel, sans une supervision adéquate, soulève des préoccupations majeures quant aux violations potentielles des droits humains,[14] notamment celles touchant à la vie privée. En effet, la collecte indiscriminée de données représente un risque inhérent pour la protection de la vie privée, car elle donne aux gouvernements les moyens de surveiller leurs citoyens sans aucun contrôle judiciaire ou cadre de responsabilité. Cette situation est d'autant plus préoccupante dans les régimes autoritaires, où la dissidence et l'opposition sont systématiquement réprimées. Dans de tels contextes, les outils de surveillance, au lieu de servir la sécurité publique, peuvent être détournés pour étouffer les voix critiques et restreindre les libertés fondamentales, mettant ainsi en péril la démocratie et l'état de droit.

[14] A. PYTLAK, 'In search of human rights in multilateral cybersecurity dialogues', *Routledge handbook of international cybersecurity*, Routledge, 2020, pp. 65-78.

De plus, cette problématique est exacerbée par le caractère incertain de certains termes utilisés dans la nouvelle Convention, qui, combiné à la latitude laissée aux États d'apporter des réserves, soulève de sérieuses inquiétudes. En effet, comme mentionné précédemment, l'article 23, paragraphe 3, alinéa a), prévoit que « *Chaque État partie peut se réserver le droit d'appliquer les mesures visées à l'article 29 de la présente Convention concernant la collecte en temps réel de données de trafic uniquement aux infractions ou catégories d'infractions spécifiées dans la réservation, à condition que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus restreint que celui des infractions auquel s'appliquent les mesures visées à l'article 30 de la présente Convention* ». Cette formulation pourrait, par conséquent, entraîner des interprétations larges et variées qui portent atteinte aux droits et libertés fondamentaux. Prenons le cas d'un État qui définit dans sa réservation des catégories d'infractions telles qu'« *atteinte à la stabilité de l'État* » ou « *activités subversives* ». Ces notions, très larges et sujettes à interprétation, pourraient être utilisées pour surveiller en temps réel les communications de groupes d'opposition politique, de journalistes indépendants ou même de citoyens exprimant des critiques sur les réseaux sociaux. Par exemple, un journaliste dénonçant des actes de corruption ou un citoyen participant à des manifestations pacifiques pourrait être ciblé sous prétexte qu'il constitue une menace pour la « *stabilité de l'État* ». Cela montre comment cette disposition, si elle est utilisée de manière abusive, pourrait aboutir à des violations des droits fondamentaux tels que la vie privée, la liberté d'expression et la liberté de réunion.

Par ailleurs, l'article 18, qui traite de la responsabilité des personnes morales, stipule que « *Chaque État partie doit adopter les mesures nécessaires, conformément à ses principes juridiques, pour établir la responsabilité des personnes morales pour leur participation aux infractions établies conformément à cette Convention* ». Bien que cette disposition vise clairement à renforcer la lutte contre la cybercriminalité en tenant les entreprises et organisations responsables de leurs actes, elle soulève néanmoins des préoccupations importantes quant à ses potentielles répercussions sur les droits individuels. En effet, la manière dont cette responsabilité est définie et appliquée peut avoir des conséquences indirectes mais significatives sur les libertés fondamentales. Par exemple, dans un contexte où les entreprises, en particulier les plateformes numériques, sont tenues responsables des infractions commises par leurs utilisateurs, celles-ci pourraient être incitées à adopter des pratiques restrictives pour éviter d'éventuelles sanctions. Ces pratiques incluraient la surveillance généralisée des activités en ligne, la suppression préventive de contenus jugés litigieux ou encore la divulgation massive de données personnelles. Ces mesures, bien que prises dans un but de conformité, risquent de porter atteinte à la vie privée des utilisateurs et de limiter leur liberté d'expression.

Ce risque est d'autant plus préoccupant dans des juridictions où les garanties procédurales sont faibles ou inexistantes. En l'absence de mécanismes de contrôle judiciaire solides, l'établissement

de cette responsabilité pourrait être utilisé comme un prétexte pour forcer les entreprises à coopérer avec les autorités de manière arbitraire. Cela pourrait conduire à des abus, tels que des enquêtes injustifiées ou des représailles politiques à l'encontre des individus exprimant des opinions critiques ou engagés dans des activités jugées subversives.

Un exemple concret illustre bien ces dangers : supposons qu'un média indépendant utilise une plateforme numérique pour publier des articles critiques envers un gouvernement. Si cette plateforme était tenue responsable de ces contenus, elle pourrait être contrainte de suspendre les comptes des journalistes ou, pire encore, de transmettre leurs données personnelles aux autorités. Une telle situation limiterait non seulement la liberté de la presse, mais mettrait également en péril la sécurité des journalistes concernés, créant ainsi un climat de peur et d'autocensure. Ainsi, bien que l'article 18 représente une avancée dans la lutte contre la cybercriminalité, il est essentiel que les États encadrent strictement son application. Des garanties claires doivent être mises en place pour prévenir tout abus et protéger les droits fondamentaux des individus, afin d'éviter que cette disposition, au lieu de renforcer la sécurité, ne devienne un outil de restriction des libertés.

La définition de la "cybercriminalité" varie considérablement d'un pays à l'autre et n'est pas universellement acceptée, ce qui rend cette notion sujette à des interprétations larges. Certaines Conventions internationales, comme la Convention de Budapest sur la criminalité informatique du Conseil de l'Europe, tentent de définir la cybercriminalité de manière plus précise en incluant des infractions telles que l'accès illégal à un système informatique, l'atteinte à la confidentialité des données, et la fraude en ligne. Cependant, cette définition reste insuffisante pour exclure les abus possibles. En effet, l'ambigüité inhérente à la notion de "cybercriminalité" permet à certains gouvernements de l'étendre à des actes qui ne relèvent pas strictement de la criminalité, comme la diffusion de critiques politiques ou sociales en ligne. Par conséquent, ce flou conceptuel ouvre la voie à des interprétations variées, permettant à des régimes autoritaires de classer certaines expressions ou actions en ligne comme des actes criminels, menaçant ainsi la liberté d'expression.

Par exemple, un État pourrait décider que des commentaires, des articles ou des publications en ligne, jugés défavorables à son régime ou à ses institutions, constituent des actes de cybercriminalité. Dans ce cadre, il pourrait se référer à la Convention de Budapest ou à d'autres instruments juridiques similaires pour justifier des mesures répressives contre des individus ou des groupes exprimant des opinions dissidentes. Une telle interprétation pourrait avoir des conséquences dramatiques, en particulier en ce qui concerne la liberté d'expression et la sécurité des journalistes, qui sont souvent en première ligne de la défense des droits humains et de l'accès à une information indépendante.

Les risques ne se limitent pas à la définition expansive des infractions liées à la cybercriminalité. En effet, les dispositions relatives aux incriminations contenues dans ces instruments peuvent facilement être interprétées de manière à inclure des activités qui, dans un autre contexte, ne relèveraient pas du domaine criminel. Par exemple, des expressions de désaccord politique ou des critiques publiques de l'État peuvent être assimilées à des "*infractions numériques*" telles que l'incitation à la haine ou à la violence, ou encore la diffusion de contenus jugés "préjudiciables". Cette définition trop floue permettrait aux autorités de considérer toute forme de critique en ligne comme un acte criminel, renforçant ainsi le contrôle sur les opinions politiques et sociales.

Mais au-delà de cette ambigüité dans les incriminations, les dispositions relatives à la procédure pénale de la Convention représentent un autre terrain de préoccupation. Par exemple, la possibilité d'effectuer une surveillance accrue en temps réel des communications électroniques, ainsi que l'accès sans restriction aux données personnelles des utilisateurs, pourrait être utilisée pour cibler des journalistes ou des militants politiques. Si ces mesures sont appliquées sans garanties juridiques suffisantes, elles risquent de mener à des violations des droits fondamentaux, notamment à travers l'espionnage, l'interception illégale des communications privées ou des détentions arbitraires. L'absence de contrôle judiciaire dans ces processus permettrait une répression ciblée, sans que les victimes aient un recours effectif.

Cela soulève des préoccupations majeures concernant non seulement la protection de la vie privée, mais aussi la liberté d'expression et l'indépendance des journalistes. La possibilité d'être surveillé, censuré ou puni en raison d'une simple critique du gouvernement met en danger l'intégrité des médias et, plus largement, l'accès à une information libre et pluraliste. En conséquence, il devient crucial de veiller à ce que les Conventions internationales ne soient pas détournées pour limiter les libertés fondamentales, mais plutôt utilisées de manière à assurer une réelle protection contre les abus liés à la cybercriminalité, tout en préservant les droits individuels.

Les journalistes, en tant que gardiens de la vérité, sont souvent les premiers à faire l'objet de mesures répressives dans des environnements où la liberté d'expression est menacée. Par conséquent, si la Convention est utilisée pour restreindre ces libertés, elle pourrait non seulement nuire à la capacité des médias à opérer librement, en limitant leur autonomie éditoriale, mais aussi compromettre le droit du public à être informé de manière objective et indépendante. En effet, des lois mal interprétées ou appliquées de manière excessive pourraient conduire à une surveillance intrusive des journalistes, à la censure de contenus critiques, voire à des représailles contre ceux qui exercent leur droit à la liberté d'expression. Cela aurait pour effet de créer un climat de peur et d'autocensure parmi les journalistes et les organes de presse, réduisant ainsi la diversité des opinions disponibles. En limitant l'accès à des informations diverses et impartiales, une telle

répression porterait atteinte au droit du public à être informé de manière transparente, objective et libre de toute influence gouvernementale ou partisane. Ainsi, il devient impératif de clarifier la définition de la cybercriminalité et d'établir des garde-fous solides pour protéger les droits fondamentaux des individus, en particulier dans le domaine de l'expression et de l'information.

Il est également crucial que les États, en mettant en œuvre les dispositions de la Convention, veillent à établir des protocoles clairs concernant la gestion et la protection des données personnelles. En effet, dans le cadre de la cybercriminalité, les mesures de surveillance, la collecte de données de trafic et l'accès aux communications électroniques peuvent entraîner une collecte massive de données personnelles, souvent sensibles. Cela soulève des préoccupations majeures en matière de vie privée, en particulier si les données collectées ne sont pas correctement protégées ou utilisées à des fins autres que celles pour lesquelles elles ont été initialement recueillies.

Les États doivent donc garantir que la gestion de ces données respecte les principes de proportionnalité et de nécessité. Par exemple, il est essentiel de limiter la collecte de données à ce qui est strictement nécessaire pour lutter contre la cybercriminalité, en évitant toute forme de surveillance de masse injustifiée. De plus, des protocoles clairs doivent être mis en place pour assurer la sécurité de ces données, prévenir les fuites et garantir que celles-ci ne soient pas utilisées à des fins répressives ou politiques.

Il est également important que des mécanismes de contrôle et de transparence soient prévus afin que les citoyens aient la possibilité de connaître les données collectées à leur sujet et, le cas échéant, d'exercer leurs droits de rectification ou de suppression. Une gestion responsable des données personnelles est essentielle pour maintenir la confiance du public dans les institutions et garantir que la lutte contre la cybercriminalité ne se fasse pas au détriment des libertés individuelles. Dans ce contexte, il est impératif que les règlementations sur la protection des données soient intégrées au cadre de la Convention, afin de garantir que la collecte et le traitement des informations soient effectués dans le respect des droits fondamentaux des individus. Cela implique la nécessité de mettre en place des directives précises qui régissent les conditions d'accès aux données personnelles par les États dans le cadre d'enquêtes criminelles.

De telles directives devraient définir les limites de l'accès aux informations sensibles, en précisant les circonstances dans lesquelles les données peuvent être collectées, ainsi que les procédures à suivre pour assurer la transparence et la responsabilité. Par ailleurs, il est essentiel que ces mesures préservent le droit à la vie privée des citoyens, garantissant ainsi que les efforts déployés pour lutter contre la cybercriminalité ne se traduisent pas par une surveillance excessive ou par des violations des droits individuels.

II. LES AVANCÉES ET ENJEUX POUR LES DROITS HUMAINS ASSOCIÉS À LA MISE EN ŒUVRE DE LA CONVENTION.

Bien qu'elle marque des avancées notables dans la lutte contre la cybercriminalité, la mise en œuvre de la nouvelle Convention sur la cybercriminalité soulève néanmoins des enjeux significatifs en matière de protection des droits humains. En effet, cette Convention, en vue de renforcer les mécanismes de coopération internationale et d'améliorer la répression des infractions en ligne, doit également faire face à des questions complexes liées aux principes fondamentaux de transparence et de respect des libertés individuelles.

D'un côté, la Convention représente un progrès essentiel dans la lutte contre la cybercriminalité, un phénomène en constante évolution qui transcende les frontières nationales et qui nécessite une réponse coordonnée et rapide des autorités compétentes. L'objectif de cette Convention est donc de renforcer la coopération internationale en matière d'enquête et de poursuite des cybercriminels, en facilitant l'échange d'informations et l'accès aux données électroniques nécessaires. Ces avancées permettent, par exemple, une réponse plus rapide aux infractions, comme le piratage ou la fraude en ligne, et une plus grande efficacité dans la traque des responsables de ces crimes.

Cependant, d'un autre côté, l'application de cette Convention soulève des préoccupations majeures en ce qui concerne la protection des droits humains, notamment en matière de transparence des procédures d'enquête. En effet, la mise en œuvre de ces mécanismes de coopération rapide et d'accès aux données peut parfois se faire au détriment de la transparence et du contrôle démocratique. Les procédures d'accès aux informations électroniques, bien que nécessaires pour enquêter efficacement sur les cybercriminalités, peuvent potentiellement être utilisées de manière excessive ou inappropriée, ce qui pose des risques pour la protection de la vie privée et pour la surveillance des actions des autorités.

De plus, la Convention pourrait entraîner des atteintes aux libertés fondamentales, comme le droit à la vie privée ou à un procès équitable, si les mesures mises en place ne respectent pas des normes strictes de protection des données personnelles et des droits des individus. Par exemple, l'accès à des informations privées à travers des demandes transnationales pourrait être effectué sans les garanties nécessaires en matière de respect des droits des personnes concernées, en particulier lorsqu'il s'agit de données sensibles ou de personnes n'étant pas directement impliquées dans l'enquête.

Dans ce contexte, la société civile, les défenseurs des droits humains et les acteurs internationaux ont un rôle crucial à jouer pour garantir que l'application de cette Convention se fasse dans le respect total des principes de transparence et des droits fondamentaux. Ces acteurs peuvent, par exemple, plaider pour une supervision indépendante des procédures d'enquête et des mécanismes d'accès aux données, afin d'éviter tout abus. Ils peuvent aussi appeler à l'adoption de mécanismes de contrôle rigoureux pour assurer que les mesures adoptées ne portent pas atteinte à la liberté d'expression, à la vie privée et à d'autres droits protégés par les Conventions internationales.

Ainsi, cette section explore non seulement les risques potentiels associés à la mise en œuvre de la Convention, notamment ceux liés à la transparence et à la protection des droits humains, mais met aussi en lumière les réponses apportées par la société civile face à ces défis. Ces réponses visent à sensibiliser l'opinion publique et à promouvoir des réformes qui garantissent un équilibre entre la lutte contre la cybercriminalité et le respect des libertés fondamentales, afin d'assurer une mise en œuvre de la Convention qui soit à la fois efficace et respectueuse des droits humains.

A) Les avancées réalisées par la Convention dans le domaine de la cybercriminalité

Les avancées réalisées par la Convention dans le domaine de la cybercriminalité se manifestent principalement à travers le renforcement de la coopération internationale, la facilitation de l'accès aux données à des fins d'enquête, et la création de mécanismes judiciaires plus efficaces pour lutter contre la criminalité transnationale sur Internet. Ces progrès ont permis de répondre aux défis uniques posés par les cybercriminels qui, souvent, opèrent au-delà des frontières nationales, exploitant les failles des systèmes juridiques et des infrastructures en place.

L'un des objectifs principaux de la Convention des Nations Unies sur la cybercriminalité réside dans la création d'un cadre international plus fluide et plus rapide pour la coopération entre les États afin de lutter efficacement contre les cybercrimes. Avant l'adoption de cette Convention, les mécanismes de coopération internationale étaient souvent fragmentés, chaque État ayant ses propres procédures, ce qui compliquait les enquêtes et les poursuites transfrontalières. La Convention a donc mis en place un cadre juridique commun et coordonné pour surmonter ces obstacles et renforcer l'efficacité de la lutte contre les crimes numériques.
La Convention a spécifiquement établi, dans l'article 35, un ensemble de principes généraux relatifs à la coopération internationale, destinés à faciliter les enquêtes et les poursuites judiciaires

concernant les infractions pénales liées à la cybercriminalité. Cet article stipule que les États parties doivent coopérer entre eux, conformément aux dispositions de la Convention, ainsi qu'aux autres instruments internationaux applicables en matière de coopération pénale. L'objectif est d'assurer une assistance mutuelle dans la collecte, l'obtention, la préservation et la communication de preuves électroniques, notamment pour les crimes cybernétiques, mais aussi pour d'autres infractions graves ayant une dimension internationale. Cette coopération s'étend au gel, à la saisie, à la confiscation et à la restitution des produits du crime, ce qui permet de rendre les poursuites plus efficaces et de limiter l'impunité des cybercriminels.

L'article 35 met également l'accent sur la simplification des procédures d'assistance judiciaire. Les autorités compétentes des États parties peuvent ainsi demander et recevoir de l'aide pour mener des enquêtes sur des infractions spécifiques telles que le piratage, la fraude en ligne, la cyberintimidation, ou encore les crimes liés aux données personnelles. Le texte précise également que la double incrimination ne constitue pas un obstacle, c'est-à-dire que même si l'infraction n'est pas définie de la même manière dans les législations des deux États parties, la coopération sera tout de même possible si l'acte est considéré comme une infraction pénale dans les deux pays concernés.

L'article 36 de la Convention traite de la protection des données personnelles, un sujet central dans les enquêtes cybercriminelles, où les données échangées peuvent être sensibles et doivent être protégées conformément aux normes nationales et internationales. Cet article impose aux États parties de garantir que les transferts de données personnelles soient conformes à leurs lois internes et aux obligations internationales relatives à la protection de la vie privée.

Ainsi, bien que la Convention encourage l'échange de données entre les pays pour lutter contre la cybercriminalité, elle impose des garanties spécifiques pour la sécurité des informations. En cas de transfert de données personnelles, les États doivent s'assurer qu'elles sont protégées de manière adéquate, notamment en garantissant la confidentialité et en prévenant les abus. L'article 36 prévoit également la possibilité pour les États de conclure des accords bilatéraux ou multilatéraux pour faciliter ce transfert de données, tout en respectant les principes de protection des données.

L'article 37 de la Convention aborde l'enjeu de l'extradition, une procédure cruciale pour garantir que les cybercriminels puissent être traduits en justice, peu importe où ils se trouvent. La Convention facilite l'extradition des personnes accusées de cybercriminalité entre les États parties, en stipulant que, lorsque la personne concernée est présente sur le territoire d'un autre État, l'extradition peut être accordée pour les infractions pénales énumérées dans la Convention, pourvu qu'elles soient punissables dans les deux pays concernés. L'article 37 permet également aux États de traiter certaines infractions cybercriminelles qui pourraient ne pas être explicitement couvertes

par les législations nationales sous la forme d'une coopération extrajudiciaire, garantissant ainsi une meilleure fluidité dans les demandes d'extradition. L'article 37 prévoit aussi la possibilité de renforcer cette coopération via des traités d'extradition bilatéraux ou multilatéraux, et autorise l'utilisation de la Convention comme base légale pour l'extradition, même en l'absence de traités formels entre certains États parties. Cela contribue à réduire les délais et les obstacles administratifs, permettant une réaction rapide face à la montée des crimes numériques transnationaux.
L'article 40 de la Convention est particulièrement important dans le contexte de l'enquête sur les cybercrimes, car il traite de la collecte et de la préservation des preuves électroniques. Il garantit que les autorités compétentes puissent avoir accès aux preuves numériques nécessaires pour mener des enquêtes et des poursuites judiciaires, facilitant ainsi la traque des criminels sur Internet. En outre, l'article 41 de la Convention prévoit des mécanismes pour assurer la coopération des fournisseurs de services, qui sont souvent cruciaux dans les enquêtes sur les cybercrimes, notamment pour la conservation des données et la collaboration dans le cadre des demandes internationales.

La Convention a mis en place un cadre juridique spécifique permettant aux États de demander à d'autres États parties de préserver rapidement des données électroniques avant qu'elles ne soient supprimées ou modifiées. Par exemple, selon l'Article 42, un État partie peut demander à un autre de préserver des données électroniques stockées sur son territoire, afin de pouvoir y accéder dans le cadre d'une enquête judiciaire. Ce processus de préservation permet d'éviter que des preuves cruciales ne soient détruites avant qu'une demande officielle d'entraide judiciaire ne soit faite. En effet, l'État requérant peut initier cette procédure de préservation grâce au réseau 24/7, un mécanisme prévu à l'Article 41, qui permet une réponse immédiate, même en dehors des heures ouvrables, garantissant ainsi que les données essentielles soient protégées sans délai.
Un aspect fondamental de ce mécanisme est que la double incrimination (principe selon lequel une demande d'entraide judiciaire ne peut être accordée que si l'infraction est également punissable dans les deux États concernés) n'est pas exigée pour la préservation des données. Cela facilite considérablement les échanges internationaux en matière de cybercriminalité, en permettant à un pays de prendre des mesures de protection des données sans avoir à prouver que l'infraction en question est également illégale dans le pays requis. La seule exigence est que la demande de préservation soit correctement formulée, conformément aux critères énoncés dans la Convention, et qu'elle contienne des informations sur l'infraction, les données concernées, et l'autorité qui formule la demande.

Une fois la préservation des données effectuée, l'État requérant dispose d'une période de 60 jours minimum pour soumettre une demande formelle d'accès aux données, ce qui lui permet de prendre les mesures nécessaires pour l'accès, la saisie, ou la divulgation des données concernées (Article 42). Si nécessaire, cette période peut être prolongée, garantissant ainsi une flexibilité qui répond à la rapidité nécessaire dans les enquêtes liées à la cybercriminalité.

En plus de la préservation des données, la Convention prévoit également des procédures pour la divulgation accélérée de données de trafic (Article 43). Si, lors de la préservation des données de trafic, il est découvert qu'un fournisseur de services dans un autre État partie a joué un rôle dans la transmission de la communication, ce dernier doit divulguer rapidement les données permettant d'identifier le fournisseur de services et le chemin emprunté par la communication. Cela permet d'accélérer les enquêtes et de localiser plus rapidement les responsables des infractions, notamment dans des affaires de piratage ou de fraude en ligne.

L'Article 44 de la Convention permet également une coopération renforcée pour l'accès aux données électroniques stockées. Lorsqu'un État partie souhaite accéder à des données stockées sur le territoire d'un autre État partie, il peut formuler une demande d'entraide judiciaire, qui doit être traitée en fonction des instruments internationaux applicables. La demande doit être traitée de manière urgente si les données sont particulièrement susceptibles d'être perdues ou modifiées, ce qui est souvent le cas dans les enquêtes liées à la cybercriminalité. Les États parties sont ainsi encouragés à répondre rapidement aux demandes d'accès aux données électroniques, surtout lorsque ces données sont essentielles pour une enquête en cours.

Les enquêtes conjointes, prévues à l'Article 48, offrent également une possibilité de coopération directe entre les services de détection et de répression des États parties. Cela permet de coordonner les efforts entre plusieurs pays pour enquêter sur des cybercrimes transnationaux, en échangeant des informations et en partageant des ressources. Les enquêtes conjointes sont particulièrement utiles pour traiter des affaires impliquant plusieurs juridictions et lorsque la nature des crimes dépasse les frontières nationales.

Le cadre juridique instauré par la Convention facilite la coopération internationale et accélère le processus d'accès aux données numériques, ce qui est crucial pour contrer efficacement la cybercriminalité. En fournissant des outils pour la préservation et la divulgation rapide des données, la Convention permet aux États de répondre plus rapidement aux incidents de cybersécurité et de rendre les enquêtes plus efficaces. De plus, la création de mécanismes tels que le réseau 24/7 et la coopération via des demandes de préservation et d'accès renforce la réactivité des autorités face à des infractions numériques de plus en plus sophistiquées et complexes.

Ainsi, la Convention a marqué une étape importante dans la réponse juridique aux défis posés par la criminalité en ligne, en améliorant l'accès aux données stockées et en facilitant la collaboration entre les pays, tout en garantissant le respect des droits de l'homme et de la législation locale.

La Convention sur la cybercriminalité a favorisé la mise en place de mécanismes essentiels pour renforcer la coopération internationale dans la lutte contre la criminalité informatique, notamment par la création de centres nationaux de contact (NCC). Ces centres sont devenus des entités cruciales pour la facilitation de l'échange rapide d'informations entre les autorités des États parties, dans le cadre d'enquêtes transnationales liées à des infractions informatiques et à des réseaux criminels internationaux.

En vertu de la Convention, chaque État partie est tenu de désigner un point de contact opérationnel 24 heures sur 24 et 7 jours sur 7, capable de fournir une assistance immédiate dans le cadre d'enquêtes pénales, de poursuites ou de procédures judiciaires relatives à des infractions visées par le texte, mais également en ce qui concerne la collecte, la préservation et l'obtention de preuves électroniques. Ces points de contact sont essentiels pour garantir une coopération efficace et rapide, notamment dans des situations où des cyberattaques ou des activités criminelles transnationales nécessitent une action urgente.

Le rôle des NCC s'étend à la facilitation de plusieurs types de mesures, notamment la préservation des données électroniques en vertu des articles 42 et 43 de la Convention, la fourniture de conseils techniques, ainsi que la localisation des suspects ou encore l'apport d'informations juridiques nécessaires pour mener à bien les enquêtes. Ces mécanismes sont particulièrement importants dans les cas où des preuves électroniques sont susceptibles d'être détruites ou modifiées rapidement, comme c'est souvent le cas dans les affaires de piratage informatique ou de fraude en ligne.

L'un des principes fondamentaux de cette coopération est la capacité d'agir selon des procédures accélérées, permettant une réponse immédiate aux demandes de coopération. L'Article 35 de la Convention souligne que, même si le point de contact désigné ne relève pas directement des autorités compétentes en matière d'entraide judiciaire, il doit assurer une coordination avec ces autorités pour garantir une mise en œuvre rapide et efficace des mesures nécessaires à l'enquête.

Un autre aspect crucial de ces centres réside dans leur formation et leur équipement, afin de garantir un personnel compétent, capable de traiter les demandes de manière efficace. Cette capacité à assurer une réponse immédiate est indispensable pour répondre aux défis posés par la cybercriminalité moderne, qui est souvent de nature transnationale et nécessite une intervention rapide pour limiter les effets dommageables d'une attaque.

La Convention permet également aux États parties de renforcer leurs réseaux existants de points de contact, y compris les réseaux internationaux spécialisés, tels que ceux de l'Organisation Internationale de Police Criminelle (INTERPOL), pour faciliter l'échange d'informations entre les autorités policières et judiciaires. Ces partenariats renforcent davantage la coopération entre les États et permettent une réponse coordonnée face aux menaces cybercriminelles mondiales.

En somme, les centres nationaux de contact jouent un rôle fondamental dans la réponse internationale aux défis posés par la cybercriminalité. Ils facilitent non seulement l'échange rapide et sécurisé d'informations entre les États, mais agissent également comme des points de coordination essentiels dans les enquêtes transnationales. Ces mécanismes permettent d'assurer une coopération fluide et réactive face aux attaques informatiques, qui sont souvent menées par des réseaux criminels opérant à l'échelle mondiale. Grâce à la mise en place de ces centres, la Convention sur la cybercriminalité a permis de renforcer les capacités des États à répondre de manière efficace aux menaces liées à la cybercriminalité, contribuant ainsi à la sécurisation de l'espace numérique international.

B) Les Enjeux de la Transparence pour les Droits Humains et le rôle de la société civile

La transparence est un principe essentiel dans le cadre des enquêtes sur la cybercriminalité, car elle garantit non seulement le respect des droits humains, mais aussi la légitimité des actions menées par les États. Dans ce contexte, il ne s'agit pas simplement d'une exigence abstraite, mais d'une condition préalable pour assurer une véritable responsabilité des États dans l'utilisation des pouvoirs d'enquête qui leur sont attribués par la Convention. Cela implique la mise en place de mécanismes de contrôle efficaces, non seulement au niveau des procédures judiciaires, mais aussi dans la gestion des critères et des justifications qui sous-tendent les actions de surveillance et d'accès aux données personnelles.

L'enjeu de la transparence ne se limite pas à la procédure judiciaire elle-même, mais s'étend également aux modalités de coopération internationale, en particulier dans le cadre de l'assistance judiciaire mutuelle. [15] Les États doivent être tenus de rendre publics les critères et les justifications de leurs demandes de coopération, en précisant les circonstances dans lesquelles ces demandes sont formulées et en veillant à ce que les processus d'échange d'informations respectent les principes de proportionnalité et de nécessité. [16] Sans une telle transparence, il existe un risque considérable que la

[15] J. PENNEY, "Cybersecurity, Human Rights, and Empiricism: The Case of Digital Surveillance." *The Oxford Handbook of Cyber Security* (2021): 409.

[16] Voir également Article 40 de la Convention.

Convention soit perçue non pas comme un outil de protection des droits humains, mais comme un levier de contrôle excessif, mettant en péril la confiance du public dans les institutions chargées de la mise en œuvre de ces mesures.

Dans cette dynamique, la société civile joue un rôle crucial. Il est impératif que les organisations non gouvernementales (ONG) et les acteurs de la défense des droits humains soient non seulement informés des actions entreprises par les États, mais aussi impliqués activement dans le suivi et la vérification de leur conformité avec les normes internationales. Leur capacité à intervenir, à signaler les dérives et à défendre les droits des individus est essentielle pour garantir que les efforts déployés pour lutter contre la cybercriminalité ne se traduisent pas par une surveillance excessive ou par des violations des droits fondamentaux. L'accès à des informations pertinentes, en particulier sur les critères d'accès aux données personnelles, doit être garanti pour assurer la responsabilité des États et la transparence des procédures.

En définitive, la transparence, lorsqu'elle est correctement appliquée et suivie de manière indépendante par la société civile, devient un instrument fondamental non seulement pour la protection des droits humains, mais aussi pour garantir que la lutte contre la cybercriminalité se fasse dans le respect des principes démocratiques. Ce processus contribue à prévenir toute forme d'abus ou de dérive, en établissant des garde-fous clairs qui permettent d'assurer que la collecte et le traitement des données n'outrepassent pas les droits fondamentaux des individus. Il s'agit ainsi de renforcer la légitimité de la Convention et de préserver l'équilibre entre la sécurité publique et la protection des libertés individuelles.

La société civile joue un rôle essentiel dans la surveillance de la mise en œuvre de la nouvelle Convention sur la cybercriminalité et dans la protection des droits humains. [17] Les organisations non gouvernementales (ONG) et les défenseurs des droits humains doivent être pleinement associés à l'élaboration et à la mise en œuvre des lois qui découlent de la Convention. Leur participation peut apporter des perspectives essentielles sur la manière dont ces lois peuvent être appliquées de manière à respecter les droits humains tout en luttant efficacement contre la cybercriminalité. De plus, leur engagement est crucial pour garantir que les préoccupations relatives aux droits humains ne soient pas ignorées lors des discussions politiques.

L'implication de la société civile est également déterminante pour favoriser un débat public éclairé autour de la Convention. Il est essentiel que les voix critiques soient entendues afin de s'assurer que les mesures adoptées dans le cadre de la Convention ne portent pas atteinte aux libertés fondamentales. Par ailleurs, le renforcement des capacités de la société civile à surveiller les actions

[17] Voir dans le contexte spécifique de la protection des victimes l'article 34, paragraphe 4 de la Convention.

gouvernementales et à promouvoir la transparence est indispensable pour maintenir l'intégrité des droits humains face à l'augmentation de la surveillance numérique.
Des initiatives telles que des forums de discussion, des ateliers et des campagnes de sensibilisation devraient être organisées pour informer le public sur les enjeux soulevés par la Convention et leurs implications pour les droits humains. Ces efforts contribueront à créer un environnement dans lequel les citoyens peuvent exprimer leurs préoccupations, participer activement au processus décisionnel et influencer les politiques publiques. En favorisant un dialogue ouvert et inclusif, nous pouvons nous assurer que la lutte contre la cybercriminalité ne se fasse pas au détriment des droits fondamentaux.

REMARQUES CONCLUSIVES

En conclusion, bien que la Convention des Nations Unies sur la cybercriminalité apporte d'importantes avancées dans la lutte contre les infractions numériques, elle soulève des enjeux considérables pour la protection des droits humains. L'objectif de cette Convention est de renforcer la coopération internationale pour contrer les crimes en ligne, mais il existe un risque substantiel que certains États exploitent les mécanismes prévus dans ce cadre pour contourner leurs obligations en matière de droits humains sous prétexte de lutter contre la cybercriminalité. Ce danger est d'autant plus manifeste malgré la présence de l'article 60 de la Convention, qui impose une cohérence entre les engagements relatifs à la cybercriminalité et les autres obligations internationales en matière de droits humains.

L'article 60 vise à garantir que la mise en œuvre de la Convention ne soit pas en contradiction avec les traités internationaux existants, y compris ceux relatifs aux droits fondamentaux. Cependant, cette disposition ne suffit pas à éliminer complètement les risques d'interprétations abusives. Certains États pourraient, en effet, l'utiliser comme prétexte pour adopter des mesures répressives et justifiées par la lutte contre la cybercriminalité, tout en négligeant les principes essentiels des droits humains qui doivent présider à toute législation.

En outre, les préoccupations liées à l'application de l'article 24, qui traite de l'accès aux données électroniques et de la coopération internationale en matière de cybercriminalité, renforcent cette problématique. La gestion de ces informations sensibles, couplée à un manque de transparence dans les procédures d'enquête, met en lumière la nécessité impérative de protéger les droits fondamentaux des individus. Si l'accès facilité aux données et la coopération internationale sont cruciaux pour la répression de la cybercriminalité, ils ne doivent pas se faire au détriment de la vie privée, de la liberté d'expression et du droit à un recours effectif.

Les récentes avancées introduites par la Convention, telles que la mise en place des centres nationaux de contact (NCC) joignables 24 heures sur 24, 7 jours sur 7, offrent des mécanismes importants pour faciliter la coopération transnationale en matière de lutte contre la cybercriminalité. Ces centres, qui permettent une communication rapide et directe entre les États parties, contribuent à une réponse plus immédiate et coordonnée face aux cyberattaques et autres formes de criminalité en ligne. Toutefois, ces mesures de coopération doivent être équilibrées par un contrôle adéquat, afin d'éviter qu'elles ne soient utilisées pour exercer une surveillance excessive ou intrusive sur les populations.

En ce sens, les États doivent veiller à ce que la mise en œuvre de cette Convention respecte pleinement les standards de protection des droits humains. Cela inclut la nécessité de garantir que les lois nationales, en particulier celles liées à la cybercriminalité, ne deviennent pas des instruments de répression au détriment des droits fondamentaux. Par conséquent, il est crucial que la Convention ne soit pas perçue comme un moyen de restreindre les libertés individuelles sous prétexte de sécurité numérique. À cet égard, il est impératif d'intégrer les droits numériques, qui représentent une extension des droits humains traditionnels, dans toutes les discussions sur la cybersécurité. L'accès à Internet, la liberté d'expression en ligne et la protection de la vie privée doivent être reconnus comme des droits fondamentaux incontournables et non comme des privilèges.

Ainsi, bien que la Convention puisse servir de fondement pour une coopération internationale efficace, elle ne doit en aucun cas justifier des mesures qui empiètent sur les libertés individuelles. L'engagement des États à respecter les droits humains, tout en luttant contre la cybercriminalité, est essentiel pour garantir que cette Convention ne soit pas détournée de son objectif initial, à savoir la préservation de la sécurité et de la justice dans le cyberespace, tout en assurant la protection des droits des citoyens.

La mise en œuvre de la Convention requiert également la promotion de mécanismes de contrôle solides, similaires à ceux des Conventions internationales en matière de criminalité, pour s'assurer que la lutte contre la cybercriminalité ne devienne pas un prétexte pour des violations des droits humains. Ces mécanismes devraient inclure des organes de surveillance indépendants, chargés d'évaluer les lois en vigueur, d'enquêter sur les éventuelles violations des droits et de formuler des recommandations visant à améliorer les pratiques législatives. Ces comités devraient intégrer des représentants de la société civile, des experts en droits humains et des techniciens spécialisés dans les défis numériques, afin de garantir une approche globale et équilibrée.

Parallèlement, des programmes de formation à destination des forces de l'ordre et des législateurs sont nécessaires pour les sensibiliser aux enjeux des droits humains dans le contexte de la

cybercriminalité. Ces formations devraient aborder des thèmes essentiels, tels que la protection de la vie privée, la liberté d'expression et les droits des journalistes, afin de prévenir toute dérive dans l'application des lois et des mesures de cybersécurité.

Dans cette perspective, l'implication active de la société civile et des acteurs internationaux, tels que les organisations non gouvernementales (ONG) et les institutions multilatérales, demeure cruciale pour surveiller et signaler les abus liés à l'application des lois sur la cybercriminalité. Il est impératif que ces acteurs aient la possibilité de dialoguer avec les États pour soumettre leurs préoccupations et proposer des solutions qui permettent d'équilibrer la sécurité et les libertés fondamentales.

Enfin, la coopération entre gouvernements, ONG et entreprises technologiques sera déterminante pour établir un environnement numérique respectueux des droits humains. Les entreprises, en particulier celles impliquées dans la surveillance numérique, doivent adopter des pratiques éthiques et veiller à ce que leurs technologies ne soient pas utilisées de manière abusive. La collaboration entre les différentes parties prenantes permettra de trouver un consensus pour garantir un avenir numérique où la sécurité et les droits humains coexistent harmonieusement. La lutte contre la cybercriminalité et la protection des droits humains ne doivent pas être vues comme des objectifs antagonistes, mais comme des composantes complémentaires d'un ordre mondial fondé sur le respect et la dignité de l'individu.

En définitive, la nouvelle Convention des Nations Unies sur la cybercriminalité doit être utilisée comme une base pour construire un cadre de coopération internationale efficace, tout en assurant que les droits de l'homme demeurent au cœur de cette lutte, afin de garantir un monde numérique sûr, juste et respectueux des libertés individuelles. Cela nécessite une vigilance collective et un engagement constant de toutes les parties prenantes.