Le premier traité global contre la cybercriminalité : de la confrontation géopolitique au compromis professionnel

En août 2024, le Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles (ci-après dénommé le « Comité spécial »), créé par la résolution 74/247 de l'Assemblée générale des Nations Unies du 27 décembre 2019, a approuvé et soumis à l'adoption de l'Assemblée générale le projet de la Convention des Nations Unies contre la cybercriminalité ; renforcement de la coopération internationale de la lutte contre certaines infractions commises au moyen de systèmes d'information et de communication et pour la communication des preuves sous forme électronique d'infractions graves (ci-après dénommée « la Convention », « la Convention de l'ONU »).[1] Le traité a été rédigé pendant quatre ans, avec les sessions du Comité spécial et les consultations intersession organisées au siège des Nations unies à New York et à Vienne.[2]

Aspects de la Convention relatifs à la politique étrangère

L'essence et l'apparence de la criminalité et des forces du maintien de l'ordre sont aujourd'hui hautement technologiques et n'ont déjà plus grand-chose à voir avec la confrontation entre les personnages des histoires de « poche » de Čapek datant du XXe siècle qui est relativement récent. Il n'est pas nécessaire de citer à nouveau les statistiques omniprésentes sur la croissance exponentielle de la cybercriminalité dans notre pays et à l'étranger, il suffit d'affirmer que ce traité international global est plus qu'opportun, il est attendu depuis longtemps et marque un tournant pour la communauté mondiale.

Quoi qu'il en soit, le processus de négociations pour élaborer la Convention, ayant été initié par notre pays, a été marqué tout au long de son déroulement par

le contexte géopolitique extrêmement défavorable dû à la montée des tensions au niveau international, et il a été à plusieurs reprises sur le point d'échouer. Il a repris sans surprise, tout comme dans une mauvaise parodie, la confrontation civilisationnelles entre « l'Occident collectif » néolibéral et ses satellites, d'une part, et, de l'autre part, une grande partie de la majorité mondiale, en particulier le monde islamique. Le vote sur le projet de Convention à l'initiative de l'Iran a mis cette confrontation en évidence de manière éclatante.

Les premières étapes de la rédaction du traité se sont déroulées sur le fond des déclarations antirusses des agents diplomatiques adverses qui ont fait preuve d'un manque d'engagement en faveur d'une coopération mutuellement respectueuse, sinon au moins purement pragmatique, ce qui a provoqué une riposte immédiate. Au stade de la finalisation du document ils se sont mis au chantage « diplomatique » et aux mises à court du temps artificielles. Cette manière agressive de propulser leur agenda politique a considérablement empêché le dialogue professionnel interétatique entre les experts dans les domaines de l'application des lois, de la justice et de la transformation numérique, ayant exacerbé le manque de confiance mutuelle et ayant créé une atmosphère destructrice dans laquelle l'acceptation ou le rejet de certaines propositions sur le texte de la Convention par les délégués praticiens dépendait parfois non pas tant de leur essence mais plus de l'État-auteur.

Les contributions des parties prenantes multiples engagées – les ONG et les sociétés informatiques occidentales, ainsi que les irrégularités en matière de visas incompatibles avec le statut du pays hôte du siège de l'ONU – ont également joué un rôle déstabilisateur. Ce genre de discussions sont par leur nature parfaitement stériles en ce qui concerne la recherche de la vérité, du fait qu'elles se déroulent sous influence des facteurs se trouvant complètement hors sujet. Mais si elles arrivent à accoucher d'une vérité, celle-ci meurt tout de suite en bas âge, tandis

que la discussion elle-même se transforme en un conflit qui exclut toute possibilité de la coopération constructive.

Les délégations ont été contraintes de gaspiller leurs ressources à rechercher réciproquement toutes sortes de portes dérobées malveillantes[3], de bombes logiques et d' « œufs de Pâques » dans le texte du projet de Convention, en bref, à identifier les vulnérabilités et les signes de mauvaise foi de la part des contreparties qui auraient pu introduire ces vulnérabilités au cours de la rédaction du document.

L'élaboration et la promotion des approches russes au sein du Comité spécial et leur codification sous la forme des normes spécifiques dans la Convention ont été facilitées par un travail conjoint coordonné au sein du Groupe de travail interinstitutions et pendant les sessions du Comité spécial, par de nombreuses négociations avec les partenaires partageant les mêmes idées et les délégations démontrant les approches constructives, organisées par le ministère russe des Affaires étrangères, par un travail de sensibilisation, et par la présentation de la monographie (disponible dans la base de données SHERLOC de l'ONUDC et sur le site web du Comité spécial) et du rapport en marge de la session. [4]

Le Parquet de la Fédération de Russie, tout comme le Ministère des Affaires étrangères de la Fédération de Russie, joue un rôle de premier plan dans la détermination des règles du jeu globales dans le domaine juridique virtuel international ; les fonctions de ces organismes dans la coordination des activités des agences chargées de l'application des lois dans la lutte contre la criminalité, d'une part, et dans la coordination de la mise en œuvre d'une politique étrangère unifiée de l'État dans ce domaine et la coordination des activités des autorités exécutives fédérales dans la mise en œuvre de la politique nationale dans le domaine de la sécurité de l'information internationale, d'autre part, sont complémentaires.

Par l'ordre n°352 du Procureur Général de la Fédération de Russie du 6 juillet 2020, un Groupe de travail interinstitutions pour lutter contre la criminalité dans le domaine de l'information a été créé sous les auspices du Parquet Général de la Fédération de Russie afin d'assurer la participation aux travaux du Comité spécial, d'élaborer la position russe consolidée sur le projet de Convention et de travailler sur les questions visant à améliorer l'efficacité des organismes chargés de l'application des lois en matière de lutte contre la cybercriminalité. Le Groupe, dirigé par le Procureur Général adjoint de la Fédération de Russie, comprend les représentants du Parquet Général de la Fédération de Russie, du Ministère des Affaires étrangères de la Fédération de Russie, du Bureau du Conseil de sécurité de la Fédération de Russie, du Comité d'enquête de la Fédération de Russie, du Ministère de l'Intérieur de la Fédération de Russie, du Service fédéral de sécurité de la Fédération de Russie, du Service de renseignement extérieur de la Fédération de Russie, du Ministère du Développement numérique de la Fédération de Russie et du Ministère de la Justice de la Fédération de Russie.

Compte tenu de l'accomplissement du mandat du Groupe de travail interinstitutions concernant l'élaboration de la Convention, son travail ultérieur visera, entre autres, à assurer la mise en œuvre des procédures nationales pour son entrée en vigueur en Russie (formulation des déclarations et des réserves, mise à jour de la législation en vigueur de la Fédération de Russie en vue de la ratification), ainsi que l'élaboration d'un protocole additionnel à la Convention (il est présumé qu'il ne comprendra que la partie substantive – les éléments supplémentaires des actes susceptibles d'être criminalisés).

Or, un projet de loi fédérale élaboré par le Parquet Général de la Fédération de Russie fait actuellement l'objet d'une approbation interinstitutions visant à réglementer la procédure de sauvegarde des données électroniques sur demande des autorités étrangères ou russes et, dans le même temps, à empêcher

les fournisseurs russes du service d'accès à l'Internet de répondre aux demandes étrangères de sauvegarde ou de fourniture des données reçues directement de l'étranger.

Il est difficile de dire si l'entrée en vigueur et le fonctionnement de la Convention de l'ONU ont un effet négatif sur les nouvelles adhésions à la Convention du Conseil de l'Europe sur la cybercriminalité de 2001 (Convention de Budapest).

D'une part, dans la Convention de l'ONU, qui a été adoptée près d'un quart de siècle plus tard, les principales normes de la Convention de Budapest ont été reproduites ou améliorées, bien que non entièrement mises à jour. D'autre part, la « Convention-mère » de 2001 reste compétitive car elle a été considérablement modernisée en 2022 avec l'adoption de son deuxième Protocole additionnel relatif au renforcement de la coopération et de la divulgation des preuves électroniques, qui contient les mécanismes extraterritoriaux simplifiés recherchés, qui sont plus proches des instruments de l'Union européenne fondés sur la reconnaissance mutuelle des mandats et qui n'ont pas été inclus dans la Convention de l'ONU et n'ont a priori pas pu l'être, à savoir : la divulgation directe par les registraires des noms de domaine et les fournisseurs des services TIC situés sur le territoire d'un pays partie au Protocole des informations en leur possession ou sous leur contrôle concernant les titulaires des noms de domaine et les abonnés (utilisateurs), respectivement, à la suite de demandes et de mandats émanant des autorités chargées de l'application des lois et des autorités judiciaires d'un autre pays partie (bien qu'à de nombreux égards, en vertu des réserves, des régimes de la notification et de la consultation de l'État du fournisseur des services, cette disposition peut être limitée à la coopération interétatique) ; l'exécution des mandats de l'autre partie pour la fourniture accélérée des données relatives aux abonnés et au trafic ; la divulgation accélérée des données informatiques stockées à travers des points de contact 24/7 sans

demande d'entraide judiciaire ; la fourniture de l'entraide judiciaire dans des situations d'urgence. Un État ne peut pas participer au Protocole avec ce régime simplifié sans participer à la « Convention-mère ».

L'application du nouveau traité global devrait également prendre en compte les risques de son éventuelle instrumentalisation déloyale à des fins politiques ou militaires, tels que ceux émanant des capacités renforcées de manière intensive et des plans de l'Ukraine et de ses alliés visant à collecter massivement des preuves électroniques, y compris les renseignements trouvés dans les sources ouvertes, contre la Fédération de Russie. Un certain nombre de projets interétatiques ont déjà été mis en place, avec un financement substantiel alloué à cet effet. [5] Ces preuves électroniques peuvent être obtenues en vertu de la Convention de manière indirecte, par le biais de divers types de mandataires et sous le couvert des procédures engagées par des tiers pour les infractions pénales de droit commun.

Afin de prévenir de tels scénarios et d'autres menaces pour la sécurité nationale, les règles relatives à la coopération interinstitutions pour la réception des demandes des autorités compétentes des États étrangers concernant les crimes et autres délits commis avec l'utilisation (l'application) des technologies de l'information et de la communication, les attaques informatiques et les incidents informatiques, ont été élaborées et font actuellement l'objet d'une procédure d'approbation.

Le contenu principal de la Convention peut être divisé en parties substantielle (criminalisation des actes) et procédurale, ainsi qu'en parties intra-étatique et inter-étatique. Cette publication se concentre principalement sur les parties procédurale et interétatique, en dressant la liste de leurs avantages et inconvénients respectifs, ainsi que sur l'enregistrement par l'auteur des résultats de certains travaux préparatoires visant à éclairer les intentions des rédacteurs en tant que moyen d'interprétation du traité.

L’étendue de la Convention

La Russie a constamment insisté sur la nécessité de l’étendue globale de la Convention, conformément au mandat du Comité Spécial établi dans ses aspects substantiels et procéduraux, ainsi que sur les seuils bas en ce qui concerne les opportunités pour la coopération en matière de lutte contre la criminalité, tandis que le camp opposé préconisait le champ d’application le plus étroit possible ainsi que les seuils hauts pour activer la mise en pratique des obligations. Les mêmes appelaient à « ne pas saturer la radiodiffusion » par les requêtes de moindre importance, à éviter la surcharge contre-productive des ressources nationales limitées par ce genre de requêtes, et surtout par les requêtes ne respectant pas l'exigence de double incrimination, par celles qui concernent des infractions administratives, des dossiers trop peu importants pour respecter l’exigence *de minimis*, ce qui, par ailleurs, ne prendrait pas en compte le cumul des infractions pénales de moindre gravité et compromettrait la prévention de la varie criminalité.

Au final, la possibilité d'accéder à ce type de requêtes a été incluse dans la Convention en tant qu'une exception à la règle de refus. Elles peuvent être considérées à la discrétion de l’État partie requis, à l’instar de la Convention des Nations Unies contre la criminalité transnationale organisée de 2000 (Convention de Palerme) et de certaines autres conventions. Si l’exigence de double incrimination n'est pas respectée, l’État partie requis peut également refuser la préservation des données.

Les obligations des Parties à la Convention relative à la coopération internationale en matière d'échange des preuves sous forme électronique (à la différence du régime national) et au sein du réseau 24/7 sont limitées, outre les infractions qui y sont établies, uniquement par les infractions graves, telles que définies dans la Convention, alors que conformément à la Convention de

Budapest, par exemple, une telle limitation ne peut être imposée par les États-parties qu'à l'interception de contenu des communications et l'information sur le trafic.

Toutefois, l'étendue de la coopération internationale est réduite principalement par le moyen de l'établissement de ses formes principales par la Convention exclusivement en matière des infractions reconnues comme telles conformément à celle-ci (établies dans le chapitre sur l'incrimination), il s'agit notamment de la coopération en matière de l'extradition, du transfert temporaire d'une personne détenue, du transfert d'une procédure pénale, des enquêtes conjointes, de toutes mesures de saisie et de confiscation à l'encontre des avoirs et même des procédures de l'assistance en matière d'application de la loi (art. 47).

Certaines dispositions de la Convention (y compris l'article 38 sur le transfert des détenus) sont conçues en tant que discrétionnaires et non pas impératives (l'État-partie requis peut, mais n'est pas obligé de fournir une entraide ou une assistance – pouvoir vs être obligé), ce qui, bien que de telles dispositions sont utilisées dans la pratique conventionnelle, prive dans une large mesure ces règles de leur valeur ajoutée, puisque une tel possibilité ne nécessite pas un traité international entre des États, toujours destiné à fixer des engagements réciproques, et les États sont eux-mêmes libres de fournir une assistance appropriée à leur seul discrétion, y compris sur la base des principes de la réciprocité ou de la courtoisie internationale. Pour cette raison, les énoncés « s'efforcent » et « prennent des mesures (efficaces) » ont été utilisées en tant que solution de compromis dans certaines dispositions clefs de la Convention qui n'avaient pas fait l'objet d'un consensus.

Ainsi, les règles d'une importance fondamentale de la coopération internationale en matière d'interception en temps réel de l'information sur le trafic et le contenu des communications, par analogie avec la Convention de

Budapest (bien qu'elle pose une obligation explicite d'entreprendre une telle coopération et non seulement de s'efforcer de coopérer, comme le prévoit la Convention des Nations Unies), représentent les normes de renvoi à cause des références à d'autres traités et (ou) au droit interne des États-parties, et elle ne s'appliquent que conjointement avec de tels instruments. Certaines délégations n'ont pas accepté le caractère impératif de ces règles en raison de l'absence ou de l'insuffisance des moyens pour ce type de coopération dans les pays respectifs. En règle générale, les États-Unis ne peuvent pas s'accorder une entraide judiciaire en matière d'interception du contenu des communications.[6]

La Convention utilise, comme certaines autres conventions des Nations Unies, une triade des phases de la procédure pénale « enquête, poursuite ou procédure judiciaire[7]» aux fins de son application au niveau national, ainsi qu'au niveau interétatique.

À la différence de la procédure pénale russe, l'enquête (pénale) désigne dans le vocabulaire universel du droit international non seulement les procédures de l'instruction préparatoire ou de l'enquête préliminaire proprement dites, mais également les vérifications préalables à l'enquête et les activités opérationnelles et d'enquête, ainsi que les enquêtes financières menées par les cellules du renseignement financier.[8]

La littérature internationale reconnaît l'enquête réactive et l'enquête proactive (généralement associée au recours à la livraison surveillée, à l'infiltration opérationnelle, etc.) et parfois également l'enquête déstabilisante, qui correspondent en principe au concepts russes de l'enquête proprement dite et des poursuites pénales, de la détection et de la répression des infractions, respectivement.[9]

Dans les instruments supranationaux de l'Union européenne relatifs aux injonctions permettant l'échange transfrontière des preuves, y compris les preuves électroniques[10], au sein de l'UE, l'énoncé « avoir des motifs raisonnables

de croire que l'infraction a été commise, est en train d'être commise ou est susceptible d'être commise » est utilisé.

Dans une large mesure on a parvenu à surmonter, en la contournant soigneusement, la réticence des opposants à étendre les mécanismes de coopération prévues par la Convention (l'entraide judiciaire et l'assistance en matière d'application de la loi, à l'exception des mesures préventives, de l'échange limité des informations et de l'assistance technique), en particulier les mesures coercitives intrusives, dont l'application nécessite une décision d'un tribunal, sur les phases de la détection, de la prévention et de la répression des infractions, que ce soit dans le contexte de l'application de ce traité global au niveau national ou international.

Ainsi, outre le tandem « prévenir et combattre » utilisé tout au long du texte de la Convention et l'article 47 (Coopération entre les services de détection et de répression) de la Convention, ce résultat a été obtenu principalement grâce à l'introduction de la définition du terme « enquête pénale » correspondant à nos intérêts dans les Notes interprétatives relatives aux articles spécifiques de la Convention, qui font en effet partie intégrante de la Convention, y compris grâce à l'article 19 de la Convention sur la participation et la tentative (des infractions tentées). Dans le même contexte, les fonctionnalités du réseau 24/7 (art. 41) ont une importance particulière.

Conformément au paragraphe 4 des Notes interprétatives (relatif aux articles 23 et 35 de la Convention), l'expression « enquêtes pénales » désignent les situations où les circonstances factuelles donnent des motifs raisonnables de croire qu'une infraction pénale (y compris une infraction établie conformément à l'article 19 de la Convention) a été commise ou est en train d'être commise, y compris dans les cas où une enquête vise à arrêter l'infraction concernée ou à prévenir sa commission.

Par conséquent, le terme « enquête » dans son interprétation juridique internationale universelle, utilisé dans les volets nationaux et internationaux de la Convention tout au long de son texte, peut englober des actes d'investigation comme les activités opérationnelles et d'enquête, ayant le caractère anticipatif et secret, dans la compréhension admise dans le droit russe – aux stades de la détection, de la prévention et de la répression des infractions pénales[11].

Il est indispensable de constater qu'à cet égard, on a réussi à dépasser la Convention de Budapest, qui dans son interprétation littérale n'est aucunement applicable aux stades de la prévention des infractions.

Plusieurs délégations optaient fermement pour la nécessité d'un seuil élevé de l'activation des normes pertinentes de la Convention – uniquement dans le cas d'une infraction déjà commise, revendiquant ultérieurement le caractère facultatif des Notes interprétatives[12].

Outre ce genre de déclarations, qui seraient probablement faites à l'égard de la Convention par certains États-parties, la Fédération de Russie fera face à une autre difficulté liée à l'application des dispositions de la Convention sur la coopération internationale en matière de l'obtention des preuves sous forme électronique, notamment l'article 44 (perquisition et accès similaire aux données électroniques stockées, leur saisie et divulgation), l'article 45 (collecte en temps réel des informations sur le trafic) et l'article 46 (interception des information sur le contenu du trafic), non pas en rapport aux enquêtes[13] ou actes judiciaires, mais afin de demander et d'entamer les activités opérationnelles et d'enquête [14] dans le cadre des dossiers placés sous contrôle opérationnel en l'absence des résultats de la vérification au préalable ou de la mise en cours d'une procédure criminelle. Le problème consiste en ce que la Convention exige pour ces actions le respect de la procédure d'entraide (judiciaire) dans le domaine de la justice pénale, qui, conformément au droit russe (articles 453-457 du Code de Procédure Pénale de la Fédération de Russie), ne s'applique qu'aux procédures pénales (l'enquête

préliminaire ou du moins la vérification du signalement d'une infraction, ainsi que procédure judiciaire) et qui est destiné à obtenir des preuves recevables, tandis que les activités opérationnelles et d'enquête sont en général menées sous le régime de l'assistance internationale en matière d'application de la loi (de police à police), visant à obtenir des informations pertinentes de point de vue opérationnel. Dans tous les cas respectifs, la Convention de Budapest utilise le terme « entraide », plus large et plus avantageux (les articles 31, 33 et 34), qui peut englober l'entraide judiciaire, ainsi que l'assistance en matière d'application de la loi.

La formule retenue a permis dans une certaine mesure de remédier à la disparition à la passivité de la majorité de la norme classique relative aux techniques d'enquête spéciales secrètes, qui est inscrite dans la Convention de Palerme et dans d'autres instruments universels, ce qui a été absolument absurde du point de vue de l'arsenal traditionnel des moyens et des méthodes de la lutte contre la cybercriminalité.

Essentiellement, en raison du manque de la connaissance profonde de la question de la part de certaines délégations, l'institution classique de l'entraide judiciaire consulaire en matière pénale, complétée par des dispositions relatives à l'utilisation des systèmes de vidéoconférence ou de conférence téléphonique contenues dans le projet russe de Convention de 2021 (art. 54), a été exclue de la convention[15]. À propos, il ne reste pas grand-chose de ce projet initial dans la Convention[16]. La Convention ne mentionne absolument pas le problème actuel des immunités électroniques, y compris les immunités juridiques internationales, dans la procédure pénale[17].

La Convention n'offre pas aux États-parties, bien qu'il soit urgent de le faire, à envisager, afin de garantir de manière effective la recevabilité et la loyauté des preuves recueillies conformément à la Convention, de mettre en place des plateaux sécurisées et des chaînes de communication entre eux pour

l'authentification et la certification des demandes d'entraide judiciaire et des preuves transmises exclusivement sous forme électronique et numérique (sans papier) et, le cas échéant, la reconnaissance mutuelle des signatures, sceaux ou timbres électroniques utilisés pour ces demandes et preuves, lorsque cela est pertinent, en connectant ces plateaux et chaînes à des points de contact joignables 24/7. Le paragraphe 14 de l'article 40 (entraide judiciaire) de la Convention contient une règle vague qui ressemble à peine à une telle disposition.

La résistance des opposants au champ d'application élargi avait une autre explication évidente. La participation à la Convention de Budapest, qui pourtant prétend être universelle plutôt que régionale, et à ses protocoles, est en fait liée pour les pays qui ne sont pas membres du Conseil de l'Europe à l'appartenance au club fermé des « démocraties développées », dont la porte ne s'ouvre qu'à l'invitation du Comité des ministres du Conseil de l'Europe, alors que celle de la Convention des Nations Unies est grande ouverte à tout État. Les « démocraties développées » ne sont pas disposées à coopérer avec ceux qui sont classés comme « États voyous », qui violent les droits de l'homme et se comportent mal dans l'espace d'information, au même niveau et selon les mêmes règles qu'ils suivent dans les relations entre eux, au sein de la société « respectable ». Le produit final des efforts conjoints démontre que cette répugnance a été largement surmontée d'une manière ou d'une autre.

Les droits de l'homme

Le camp pro-occidental a cherché à insérer dans la Convention les dispositions qui empêcheraient son application non seulement dans le contexte national, mais aussi en vue de la coopération internationale, en invoquant les menaces généralisées pour les droits de l'homme. Ils ont souligné le caractère sans précédent du traité international en cours d'élaboration en ce qui concerne

le degré d'intrusion de ses dispositions dans les droits et libertés fondamentaux de l'homme, en particulier ceux qui sont relatifs au secret des communications, à la vie privée en général et au secret personnel, avec un accent sur la nécessité d'établir les garanties correspondantes de leur respect.

Il est bien connu que ceux qui veulent coopérer trouvent des moyens, ceux qui ne le veulent pas, trouvent des excuses. Dans le cas de la Convention, il n'est pas nécessaire d'identifier les motifs admissibles pour le refus d'entraide ou d'assistance demandées, puisque leur éventail est présenté, en particulier, dans le paragraphe 21 de l'article 40, et deux d'entre eux (l'atteinte éventuelle à l'ordre public et la contradiction avec les exigences du système juridique de l'État requis), en raison de la pratique existante en matière de la praxis juridique, peuvent être considérées comme exhaustives, couvrant un certain nombre d'autres. Par conséquent, outre les possibilités d'abus politique de ces motifs, indiquées ci-après, à d'autres conditions égales et du point de vue purement pratique du travail des organismes compétents centraux et autres dans les pays en matière d'application de la loi et de justice, sur les questions de l'entraide judiciaire et de l'assistance en matière d'application de la loi, la lutte contre « les portes dérobées » en matière de droits de l'homme dans la Convention serait à juste titre perçue comme une bataille contre les moulins à vent.

Il s'agit des scénarios quotidiens des relations bilatérales entre l'État requérant et l'État requis qui sont parties à la Convention, pour s'accorder ou se refuser l'entraide judiciaire sur la base des motifs que la Convention énonce. Et rien n'empêche, par exemple, la Conférence des parties à la Convention de Palerme, qui ne contient pas de dispositifs de sûreté de large proportion, ou tout autre mécanisme d'examen des conventions d'aborder les violations des droits de l'homme dans le cadre de leur application.

Les dispositions de l'article 6, paragraphe 2 (Le respect des droits de l'homme) de la Convention (même si elles sont grammaticalement imparfaites,

tout comme le titre de la Convention, à cause de la réticence à révéler un compromis) sont devenues l'un des éléments les moins consensuels du processus des négociations. Néanmoins, celles-là ont résisté lors du vote. L'article 24 de la Convention énonce les conditions et les garanties générales pour assurer les droits de l'homme, y compris le principe de proportionnalité, tandis que l'article 36, parmi les règles de protection des données personnelles, contient de facto un motif supplémentaire pour le refus de coopérer citant la législation nationale dans ce domaine. En outre, la formule classique pour les droits de l'homme concernant le refus d'extradition pour les raisons de la discrimination, est extrapolée aux motifs du refus d'entraide judiciaire, ce qui ne figure pas dans les conventions sectorielles en vigueur.

À première vue, la question se pose naturellement: qui d'entre nous, remplissant ses obligations volontaires en vertu des traités internationaux sur les droits de l'homme et ayant prescrit les valeurs similaires et leurs garanties dans la Loi Fondamentale de son pays, les partageant et les professant, peut s'opposer à ces formulations correctes de la Convention? Leur rejet par de nombreux pays s'explique principalement par la « fluidification » des dispositions de la Convention contre la criminalité par un langage propre à la problématique des droits de l'homme, inhabituel pour ses objectifs et n’ayant pas d’équivalent dans le passé, ce qui crée un précédent indésirable. De plus, il s’agit du danger de l’instrumentalisation politique des dispositions au détriment de la coopération bilatérale entre les parties à la Convention.

Un tel danger pourrait émaner de tout tiers ou d'un groupe des tiers souhaitant assumer, directement ou indirectement par le biais de la Conférence des Parties, le rôle d'évaluateur du respect des exigences de la Convention à cet égard et inculper l'État demandant l'entraide et, surtout, l'État la fournissant pour les violations réelles ou perçues de la Convention, contrôler la liste des personnes

pénalisées, imposer des sanctions à leur encontre, ce qui freinera la coopération bilatérale dans le cadre de la Convention.

Les théories de conspiration orwelliennes ont également été exploitées dans le cadre de l'agenda des droits de l'homme. La rédaction et l'adoption de la Convention à tous les stades ont été accompagnées – il est bien probable que sa future application sera aussi – du battage incompétent et de la désinformation délibérée l'entourant en tant qu'outil présumé des agences de sécurité nationale, c'est-à-dire, de la « surveillance de masse », en particulier aux mains des régimes non démocratiques.

Par ailleurs, la Convention elle-même n'a rien à voir avec les activités de renseignement et de contre-espionnage aux fins de la sécurité nationale, mais se situe exclusivement dans le domaine de la justice pénale, vise à obtenir des preuves admissibles soumises à un contrôle judiciaire (alors que la communauté du renseignement se soucie peu de leur admissibilité) et peut également servir à des activités opérationnelles de « renseignement » (*national security intelligence, counterintelligence*) dans le domaine de l'application de la loi *(law enforcement intelligence, criminal intelligence)*.

C'est précisément pour dissiper toute inquiétude à ce sujet que le mot « spécifique » est inclus dans le texte, par analogie avec la Convention de Budapest, étant, de l'avis de beaucoup, redondant à cause de son évidence, pour faire référence à des enquêtes criminelles, des poursuites ou des procédures judiciaires individuelles et définies, ainsi qu'aux données et communications générées par celles-ci – par opposition à une collecte et à un stockage des données généraux, proactifs et massifs. À l'époque, en particulier à la lumière des révélations d'Edward Snowden, le Comité de la Convention de Budapest a dû repousser les attaques similaires de la part de l'Union européenne en raison de l'élaboration d'un prototype du Deuxième protocole additionnel à la Convention et dans le contexte de son article 32(b).[18]

Il n'y avait aucune perspective d'accord sur la question connexe d'établir les obligations pour les fournisseurs de services TIC de retenir (par opposition à préserver) des données, notamment en raison de la position selon laquelle la Convention ne devrait pas faire le secteur privé assumer de telles obligations, ce qui lui imposerait des coûts financiers énormes et, pour bon nombre de ses représentants, inabordables. La situation était similaire lors de l'adoption de la Convention de Budapest.[19]

Les « portes dérobées » extraterritoriales

La Fédération de Russie s'est catégoriquement opposée à l'expansion des éléments extraterritoriaux dans le texte du traité, et tout d'abord à l'introduction de tout analogue du paragraphe « b » de l'article 32 de la Convention de Budapest. En même temps, étant donné que la couche centrale du cyberespace forme un niveau logique (virtuel) qui n'a pas de frontières matérielles ni géographiques, les garanties de la protection de la souveraineté territoriale stipulées dans l'article 5 de la Convention se transforment facilement en garanties éphémères, sujettes à la libre interprétation d'une partie engagée, dont le point de vue, selon une expression bien connue, dépend du « lieu de la localisation » dans l'espace physique ou sur le territoire d'un pays concret.

Comme nous l'avons déjà mentionné, le Comité spécial a manqué une occasion unique de réglementer la prévention des cyber-opérations secrètes transfrontalières unilatérales menées par les États participants dans le but de contourner la coordination bilatérale. Ces opérations créent un risque de « tirer sur les amis » en ce qui concerne les activités secrètes réciproques et vont à l'encontre du droit international en termes de souveraineté des États et de protection des droits de l'homme.[20]

Les cyberpuissances développées de « l'Occident collectif », qui souhaitent maintenir leurs opérations proactives, unilatérales et extraterritoriales du

piratage informatique gouvernemental dans une zone grise juridique, se sont heurtées à une résistance farouche lorsqu'elles ont tenté d'établir les règles universelles minimales pour leur conduite. Encore une fois, sous le prétexte plausible qu'il n'est pas souhaitable que les activités secrètes autres que celles prévues par la Convention (surveillance électronique sous forme d'acquisition secrète (interception) des données relatives au trafic et au contenu) interfèrent avec les droits de l'homme, tandis que l'ampleur de cette interférence est particulièrement élevée.[21]

A son tour, un projet de loi fédérale « de blocage » a été élaboré, qui est actuellement en cours de rédaction dans la Douma d'État, la chambre basse de l'Assemblée Fédérale de la Fédération de Russie.[22] Il vise à contrer l'adoption par les organismes étrangers et internationaux des mesures unilatérales pour la collecte indépendante illégale des preuves, y compris électroniques, et autres informations dans la Fédération de Russie, notamment par le biais de contacts transfrontaliers à distance avec des personnes physiques et morales situées sur le territoire de la Fédération de Russie, et à faire face aux mesures pour attirer de cette manière des citoyens russes à l'étranger afin de les arrêter.

En consentant, sous une forme ou une autre, à l'hébergement des serveurs, des réseaux et des autres équipements d'un fournisseur étranger, l'État donne essentiellement son consentement explicite ou implicite à l'utilisation et autres types de traitement, y compris aux fins de l’application extraterritoriale de la loi, des données qui y sont stockées ou transmises par le fournisseur en possession ou sous contrôle duquel elles se trouvent, à moins que l'État d'accueil n'établisse de règles strictes pour la localisation de ces données ni spécifie d'autres conditions pour leur traitement, par exemple, selon le critère de la nationalité des personnes concernées par les données personnelles traitées. Et vice-versa, l'État dont le fournisseur offre ses services à l'étranger, y place son infrastructure technique et, en outre, obtient une localisation juridique (et une représentation

accréditée) par le pays hôte, accepte en règle générale l'interaction de son fournisseur avec les autorités de ces pays, y compris dans le domaine de l'application de la loi et quelle que soit la nationalité des personnes concernées par les données personnelles traitées.

Ainsi, objectivement et en réalité, il existe un conflit positif de compétence entre plusieurs États en ce qui concerne les données à l'endroit où se trouvent: le fournisseur des TIC; le stockage ou la transmission de données et / ou le(s) dispositif(s) de stockage et de transmission de données; et l'abonné (l'utilisateur). L'État de nationalité de l'abonné (de l'utilisateur) peut également être ajouté sous certaines conditions.

L'article 27 de la Convention a un potentiel extraterritorial important, bien qu'il soit situé, contrairement à l'article 32 de la Convention de Budapest, dans la partie interne plutôt qu'internationale du traité. Il convient de tenir compte du fait que les articles « internes » exigent que l'État partie établisse des pouvoirs pour ses organismes, que la Convention ne considère que comme pouvoirs minimaux, laissant à l'État partie l'entière liberté d'en étendre la portée (art. 59).

Conformément à l'article 27 de la Convention, qui est similaire à l'article 18 de la Convention de Budapest, chaque État partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre ses autorités compétentes de donner des ordres: a) à une personne se trouvant sur son territoire de fournir les données électroniques spécifiques en sa possession ou sous son contrôle, stockées dans un système d'information et de communication ou sur un support électronique de données; et b) à un fournisseur de services offrant ses services sur le territoire d'un État partie de présenter les données des abonnés concernant ces services qui sont en possession ou sous contrôle de ce fournisseur de services.

Ainsi, les dispositions de l'article 27 « a » de la Convention n'excluent pas leur éventuelle application pour l'accès transfrontalier unilatéral par les autorités d'un État à les données stockées sur le territoire d'un autre État, sans recours à

l'entraide judiciaire internationale ou à l'assistance en matière d'application de la loi, en contactant, si nécessaire avec l'utilisation des mesures coercitives, la personne en possession des données, dont la nature, la propriété et la licéité d'être en possession de cette personne sont illimitées. Ici il pourrait s'agir de toute personne physique ou morale qui ait l'accès extraterritorial illégal aux serveurs et d'autres dispositifs situés dans un autre État, ainsi qu'aux données qui y sont stockées, qui puissent entrer en sa possession à la suite d'une infraction couverte par la Convention et être ainsi légalisées par cette norme de la Convention aux fins de la justice pénale; il pourrait s'agir d'un détenteur de secret transfuge, etc. Enfin, malgré l'existence d'une règle extraterritoriale spécifique sur le fournisseur de services dans le paragraphe « b », du même article, les documents interprétatifs de l'article 18 identique à la Convention de Budapest soulignent à juste titre que le paragraphe « b » s'étend également sur les fournisseurs de services.[23] En outre, contrairement à la nature strictement limitée des données dans le paragraphe « b », leurs catégories dans le paragraphe « a » dans les articles des deux Conventions ne sont limitées en rien. Les fournisseurs de services, en particulier les fournisseurs étrangers, peuvent disposer de toutes les données provenant de serveurs étrangers et d'autres dispositifs.[24]

Le paragraphe « b » de l'article 27 de la Convention des Nations Unies établit un critère de compétence ciblé : ses dispositions prévoient la possibilité pour un État sur le territoire duquel le fournisseur prête ses services dans le domaine des TIC de réclamer directement les informations sur les abonnés qui font partie de ces services et que le fournisseur possède ou contrôle. Ainsi, vu la variabilité de l'emplacement des données dans le cloud, il n'y a que le lieu de la prestation du service et le fait que le fournisseur possède ou contrôle les données concernées qui comptent, et non l'emplacement (y compris à l'étranger) du fournisseur et des données (serveurs) comme telles.

La note d'orientation du Comité de la Convention de Budapest définit la notion de la prestation des services sur le territoire d'un État et du lien réel et substantiel du fournisseur des services avec cet État. « Les Parties peuvent considérer que le fournisseur des services « fournit ses services sur le territoire d'une Partie » si : le fournisseur des services octroie aux personnes sur le territoire d'une Partie la possibilité de s'abonner à ses services (et ne bloque pas, par exemple, l'accès à ces services) et *(condition cumulative)* le fournisseur des services a établi un lien réel et substantiel avec cette Partie. Les facteurs qui s'y rapportent comprennent le degré auquel le fournisseur de services oriente ses activités vers ces abonnés (par exemple, en faisant de la publicité locale ou de la publicité dans la langue du territoire de la Partie), utilise les informations sur les abonnés (ou les données du trafic y reliées) au cours de son activité, interagit avec ses abonnés dans la Partie ou autrement peut être considéré établi sur le territoire d'une Partie. Le seul fait que le fournisseur de services utilise un nom de domaine ou une adresse électronique qui sont liés à un pays concret ne crée pas de présomption que son domicile est situé dans ce pays. C'est pourquoi l'exigence que les informations à fournir sur les abonnés doivent concerner les services du fournisseur prêtés sur le territoire d'une Partie peut être considérée comme remplie même si ces services sont prêtés par l'intermédiaire d'un nom de domaine de premier niveau qui se rapporte à une autre compétence ».

La note remarque également que « les régimes juridiques reconnaissent de plus en plus qu'aussi bien dans le domaine de la justice pénale que dans celui de la protection de la vie privée et des données l'emplacement des données n'est pas un facteur définitif pour établir une compétence ».

La Convention n'a pas inclus la norme (à propos, personne n'a fait trop d'efforts pour le faire) similaire au paragraphe « b » de l'article 32 de la Convention de Budapest, bien douteux pour la Russie – celle concernant le droit à l'accès transfrontalier unilatéral aux données numériques stockées dans un autre

État partie à cette convention et hors du domaine public sur l'accord de la personne légitimement habilitée à les divulguer à une partie étrangère et sans avis obligatoire de cet autre État. En cas d'exemple de l'application de la norme, on cite souvent l'inspection du dispositif du suspect (coopérant) avec sa boîte e-mail dans un domaine étranger ouverte (avec les données stockées sur un serveur étranger) avec l'Accord de cette personne.

En même temps, bien d'autres scénarios que rien ne limite sont possibles, où que cette personne se trouve et quand. Dans son interprétation officielle donnée par la note d'orientation du Comité de la Convention de Budapest, la norme est pratiquement inapplicable à la requête des données des utilisateurs auprès des fournisseurs des services dans le domaine des TIC à l'étranger car il serait peu probable que les fournisseurs, n'étant habituellement que détenteurs de ces données, sans les contrôler ni les posséder (et n'ayant donc pas de pouvoirs légitimes de les divulguer), puissent donner leur accord légitime et volontaire pour la divulgation des données des utilisateurs[25]. (Il faut dire que cette explication contredit ladite note d'orientation du Comité pour l'article 18 de la Convention de Budapest (sous-paragraphe «a» du paragraphe 1 de l'article 18) qui indique que les fournisseurs de services font partie de ces personnes habilitées[26].)

La comparaison des dispositions de la Convention des Nations Unies avec celles de la Convention de Budapest dans les parties analysées permet de conclure que dans le cas où la personne donnant son consentement aux termes du paragraphe « b » de l'article 32 de la Convention de Budapest ne se trouve pas à l'étranger[27], mais sur le territoire de l'État dont l'organisme obtient l'accès aux données stockées à l'étranger (le scénario principal du paragraphe « b » de l'article 32), les dispositions du paragraphe « b » de l'article 32 de la Convention de Budapest coïncideront en grande partie avec les dispositions des sous-paragraphes « a » et « b » de l'article 18 de cette dernière et de l'article de la

Convention des Nations Unies. Les articles 16–17 de la Convention de Budapest et 25–26 de la Convention des Nations Unies sont également liés en ce qui concerne la possibilité du stockage extraterritorial et l'accès aux données car ils ne limitent pas le nombre des destinataires des réclamations présentées par les organismes compétents et ne citent pas d'autres indices territoriaux pour leur application.

Ainsi, les différences essentielles entre l'article 27 de la Convention des Nations Unies et le paragraphe « b » de l'article 32 de la Convention de Budapest témoignent dans leur ensemble d'un potentiel extraterritorial plus large de l'article 27 de la Convention des Nations Unies par rapport à l'article 32 de la Convention de Budapest dans les cas dudit scénario et se résument comme suit :

dans la première, les données concrètes comme telles sont fournies par la personne, dans la seconde, l'accès aux données concrètes ou leur obtention se font par les forces de l'ordre elles-mêmes ou par l'intermédiaire de quelqu'un à l'aide du système informatique situé sur le territoire de leur État. Le résultat final en question, c'est-à-dire l'obtention des données comme telles depuis l'étranger, est le même, bien qu'en cas d'accès direct les forces de l'ordre peuvent obtenir un volume de données dépassant les limites du consentement de la personne, mais cette portion de données non autorisée peut être reconnue comme preuve inadmissible ;

dans la première, les actions des forces de l'ordre sont coercitives et la personne est tenue de s'y soumettre, dans la seconde, les actions des forces de l'ordre visant à un accès indépendant ou indirect ne peuvent être effectuées que sur le consentement légitime et bénévole de la personne ;

dans la première, l'exigence que la personne dispose des données requises sur une base légitime n'est pas présentée, dans la seconde, la personne doit disposer des pouvoirs légitimes pour divulguer les données aux forces de l'ordre par ledit système informatique.

À la lumière desdites dispositions des deux paragraphes de l'article de la Convention des Nations Unies, la mise en place de la norme spéciale « extraterritoriale » introduite depuis 2022 dans les accords intergouvernementaux bilatéraux passés sur la coopération dans le domaine de la sécurité informatique internationale peut se révéler comme problématique en ce qui concerne sa réalisation pratique. Par exemple, conformément à l'Accord entre le Gouvernement de la Fédération de Russie et le Gouvernement de la République d'Azerbaïdjan sur la coopération visant à assurer la sécurité informatique internationale du 24.06.2022 (article 2), « l'accord transfrontalier aux informations numériques stockées dans le réseau informatique d'un des États des Parties est inadmissible sans interaction officielle avec les organismes compétents appropriées des États des Parties ; cette interaction peut être réalisée notamment dans le cadre des négociations internationales bilatérales et multilatérales, y compris sur l'entraide judiciaire en matière pénale, aussi bien que dans le cadre de la coopération internationale des forces de l'ordre »[28].

Comme nous le voyons, l'interdiction conventionnelle concerne l'accès transfrontalier aux informations numériques comme telle sans faire exception des cas d'un tel accès par les forces de l'ordre directement ou par l'intermédiaire de toute personne ou d'un fournisseur de services TIC. En outre, cette interdiction n'a pas de restrictions quant à la nature des informations qui peuvent en réalité appartenir également au domaine public (sources ouvertes). C'est pourquoi ladite formule standard exige un perfectionnement.

Compte tenu de l'utilisation des messageries étrangères, du courrier électronique, des échanges crypto[29] et d'autres services Internet par la population, l'évidence devrait être admise que les actions des forces de l'ordre reflétées dans ces normes de la Convention des Nations Unies, y compris à l'égard d'un détenteur illégitime des données, aussi bien que l'exemple suscité du recours au paragraphe « b », tant diabolisé, de l'article 32 de la Convention de

Budapest, sont une pratique professionnelle quotidienne et routinière, c'est pourquoi limiter l'emplacement du système TIC et du porteur des données, cités à l'article 27, à l'intérieur du territoire de l'État dont les organismes réalisent leurs pouvoirs de donner des ordres appropriés, ne serait pas conforme aux réalités « sur le terrain »[30]. Par contre, l'étendue dans l'espace de l'application des normes concernant la fouille et la saisie des données (article 28) est strictement limitée au territoire de l'État des organismes qui en donnent l'ordre et où le système d'information et de communication qui stocke les données ou sa partie ou le porteur des données sont situées, tandis que celle des normes concernant l'interception des données sur le trafic ou le contenu (articles 29–30) est limitée au territoire de l'État où les moyens techniques en question sont utilisés ou les messages en questions sont transmis à l'aide d'un système d'information et de communication.

Selon les articles 42, 44 et 45 de la Convention, c' est l'État dont le territoire abrite le système d'information et de communication au moyen duquel les données électroniques sont stockées, qui est le destinataire d'une demande de préservation ou de la prestation des données électroniques; et au cas de l'interception des données de trafic c'est l'État sur le territoire duquel les messages sont transmis au moyen du système d'information et de communication (cependant l'article 46 ne concrétise pas l'État-destinataire dont le territoire est touché au cas de l'interception des données). Ces textes eux-mêmes peuvent être considérés dans l'environnement actuel comme fallacieux, conduisant délibérément à l'adresse erronée « n'importe où » : l'enquêteur qui fait la demande d'entraide judiciaire ne sait pas et ne peut pas savoir exactement et spécifier dans sa demande où, dans quel système d'information, dans quel pays et à quel moment le fournisseur stocke et traite les données qui intéressent l'enquêteur ou transmet les messages.

L'utilisation de l'informatique en nuage et la navigation anonyme posent le problème de la localisation des données : la perte d'informations sur leur localisation, y compris l'absence de telles informations chez le fournisseur lui-même ; les situations où les données formant un tout unique (ressource d'information) dans un état fragmenté et/ou dynamique (en migration) sont dispersées dans les juridictions différentes ou comportent de multiples copies miroirs. Le problème de l'écoulement incontrôlé du trafic national en dehors de l'infrastructure nationale d'information se pose également, notamment en raison de l'exploitation du systèmes de communication par satellite non géostationnaires (en orbite basse) et de l'accès à l'Internet à large bande de type « Starlink ».

Pour ces raisons, dans la pratique juridique actuelle, les destinataires des demandes de la conservation et de l'extraction des données sont en règle générale les États de « nationalité » des fournisseurs des services TIC et autres dépositaires. La juridiction procédurale de l'État pour les systèmes d'information, les réseaux et les données, fondée sur la localisation du fournisseur ou de ses activités professionnelles, est définie de manière illustrative par rapport à l'État de destination des demandes dans la Loi type d'entraide judiciaire en matière pénale de l'ONUDC : il s'agit de l'État dans lequel le fournisseur qui détient ou contrôle les données est situé, établi ou, du fait de son activité de stockage, de transmission ou de traitement des données, opère d'une autre manière à partir de cet État.[31]

Sur l'insistance de la délégation russe au Comité spécial, la Convention a inclus les dénouements appropriés reflétant l'état réel des choses. Par exemple, dans l'article 41 (Réseau 24/7) parmi les compétence du centre de contact on trouve celle à donner les informations concernant l'emplacement du fournisseur de services, s'il est connu de l'État partie requis, pour aider l'État partie requérant à formuler sa demande. L'article 42 (Coopération internationale aux fins de la

préservation accélérée de données électroniques stockées) stipule que l'État partie requérant peut recourir au réseau 24/7 prévu à l'article 41 de la présente Convention pour demander des informations concernant la localisation des données électroniques stockées au moyen d'un système d'information et de communication et, s'il y a lieu, des informations concernant la localisation du fournisseur des services. Les dispositions de ces deux articles contribuent également à l'application des articles 43-46 de la Convention.[32] En outre, les demandes doivent inclure, à titre d'information alternative : toute information disponible permettant d'identifier le dépositaire des données électroniques stockées ou la localisation du système d'information et de communication (demandes de conservation des données) ; toute donnée disponible permettant d'identifier le propriétaire ou l'utilisateur des données ou la localisation du système d'information et de communication (demandes d'interception des données de trafic).

La Convention de Budapest, quant à elle, ne retient que le territoire où se trouvent les données pertinentes (communications interceptées, systèmes informatiques) comme critère pour déterminer l'État destinataire requis dans le cadre de la coopération internationale, ce qui ne correspond pas aux réalités modernes de l'informatique en nuage et constitue un critère insuffisant et dépassé. Dans le Deuxième Protocole additionnel de 2022 à la Convention de Budapest le critère cité est remplacé de manière justifiée par la localisation de la présence physique du prestataire de services dans l'État concerné.[33]

L'exception concerne l'interception de conversations et d'autres interceptions en temps réel de communications et d'autres données, qui peuvent être requis non seulement à l'État du prestataire de services, mais aussi, dans de nombreux cas, voire dans la majorité d'entre eux, aux États de localisation:

l'abonné (utilisateur) et/ou l'appareil terminal détenu ou utilisé par l'abonné (utilisateur);

l'équipement terminal ou de transit ou les réseaux du fournisseur par lesquels les données sont transmises.

Langue de la Convention

Afin d'assurer la cohérence des textes, faisant également foi, de la Convention dans les six langues officielles de l'ONU, un Groupe de concordance du Comité spécial a été établi. Ce Groupe englobe six sous-groupes linguistiques représentatifs (chaque sous-groupe étant à son tour composé de représentants de différents pays où la langue en question est une langue d'État ou officielle), qui se sont consultés régulièrement en étroite coordination avec les traducteurs des sections de traduction de l'Office de l'ONU à Vienne.

Dans un premier temps, les experts du Groupe ont décidé de ne pas considérer les textes de la Convention de Palerme et d'autres conventions de l'ONU comme inviolables et de ne pas élaborer de glossaires spéciaux sur le modèle du glossaire de la Convention de Palerme, mais plutôt de corriger dans la nouvelle Convention un grand nombre d'inexactitudes et d'incohérences entre les versions linguistiques identifiées au cours de près d'un quart de siècle d'application de la Convention de Palerme et de la Convention de l'ONU contre la corruption de 2003 (Convention de Mérida). Au sein du groupe, le texte russe a été soigneusement comparé avec l'anglais (qui était le « premier parmi les égaux », puisque la Convention a été principalement rédigée dans cette langue) et l'espagnol (ensuite dans les agences de l'ONU avec les autres langues), avec la participation active des membres de la délégation russe - représentants des forces de l'ordre, du Ministère du développement numérique, des communications et des médias et des diplomates. Ce format interinstitutionnel a permis, en collaboration avec les traducteurs viennois, de produire un texte russe de haute qualité linguistique et juridique, tout en éliminant les lacunes constatées

en anglais et en espagnol et en veillant à ce que les différents termes juridiques soient identiques les uns aux autres dans leur sens actuel.

Les rédacteurs, à l'instar de la Convention de Budapest, sont initialement convenus de n'utiliser que des termes neutres sur le plan technologique dans le traité afin de s'assurer que la Convention soit indéfiniment applicable, indépendamment de l'émergence de nouvelles technologies ; elle ne définit même pas la preuve électronique et utilise à la place le terme « la preuve sous forme électronique », qui peut être interprété comme étant à la fois plus large et plus étroit que la preuve électronique, étant donné que la preuve électronique peut parfois inclure certaines informations sur papier également.[34]

L'identification, la prévention, la répression et la détection des infractions sont des étapes distinctes de la lutte contre la criminalité. Elles incluent parfois l'action préventive, et la prévention et la répression font partie du champ d'application de « l'anticipation ». Le défi consistait à s'assurer que toutes ces étapes soient incluses dans les parties nationales et internationales de la Convention. Contrairement au mandat du Comité spécial, la Convention a choisi d'utiliser le terme « lutter » au lieu de « contrer ». Le choix de l'équivalent anglais du terme étroitement spécialisé « la répression » a posé quelques difficultés, car les termes *« disruption »* et *« frustration »*, qui sont les plus proches de ce terme et qui désignent l'interruption de toute action entamée et inachevée, sont utilisés dans les législations étrangères, mais pas dans les conventions, dans ce sens étroitement spécialisé.

En même temps, *le terme « suppression » utilisé* dans ces textes est traduit de manière variable à la fois comme répression et comme lutte en général, et a un sens plus large de neutralisation, de blocage d'une activité plutôt que de répression stricte, tout comme le terme *« deterrence » (*« l'obstruction », « l'inadmissibilité ») a un champ d'application plus large. Les anglophones ont tendance à considérer la répression comme une composante du terme de la

prévention sans le distinguer comme un élément indépendant de l'anticipation. L'idée initiale, largement approuvée, d'exprimer un concept en deux (« la prévention » pour désigner à la fois «предупреждение и пресечение» (« la prévention et la répression »), bien qu'utilisée (par exemple « l'intégrité » signifiant «честность и неподкупность» (« l'honnêteté et l'intégrité »), ne semblait pas souhaitable, compte tenu également du chapitre VI (Mesures préventives) de la Convention, où il ne s'agit que de l'action préventive. Par conséquent, on a choisi la meilleure option consistant à inclure le stade de la répression d'une infraction dans le concept d'enquête, ou plutôt dans l'un de ses objectifs (stopper ou empêcher la commission de l'infraction) dans les notes interprétatives sur la Convention.

Il convient de tenir compte du fait qu'en raison des différences entre les systèmes juridiques des pays du monde (par exemple, la convergence de l'enquête préliminaire (précontentieuse) et les activités opérationnelles et d'enquête, la variabilité du contenu du concept de « l'affaire pénale ») et l'universalité de la langue des documents internationaux, les noms des actes de procédure (d'enquête, judiciaires) dans le droit étranger et international ne coïncident souvent pas avec ceux utilisés dans le droit russe, et les activités opérationnelles et d'enquête nationales (secrètes) sont dans la plupart des cas désignées comme des mesures d'enquête *(investigative measure)*, de renseignement *(criminal (law enforcement) intelligence operation)* ou sont inclues dans le concept juridique international obstructif « *special investigative technique » (« techniques d'enquête spéciales »),* de sorte que les désignations terminologiques en elles-mêmes soient arbitraires et ne doivent pas être déterminantes dans le choix d'un type particulier d'entraide judiciaire ou d'assistance en matière d'application de la loi.

Aux fins des traités internationaux, les autorités judiciaires, les autorités de justice pénale dans l'ordre juridique russe désignent traditionnellement les

structures d'enquête préliminaire (l'enquête et l'instruction préliminaire), les organes du Parquet et les tribunaux[35]; par conséquent, « les documents judiciaires » désignent les documents émis par eux ou émanant d'eux.

Les éléments suivants sont également à noter comme autres caractéristiques de la traduction.

La double traduction du terme « infraction » en « правонарушение » et « преступление » selon le contexte : la première est principalement utilisée dans la combinaison « infraction pénale » (dans de nombreuses juridictions, elle est divisée en fonction de sa gravité en « crimes » et « délits ») lorsque la Convention établit (criminalise) les actes en cause, tandis que la seconde est utilisée dans d'autres contextes, où sa signification en tant que crime déjà établi ou couvert par la Convention est évidente. Il en va de même pour le terme « saisie » : le contexte définit s'il s'agit d'un terme procédural spécial restreint « выемка » ou « арест » qui se réfère à des mesures d'enquête ou judiciaires distinctes, notamment celles nécessitant une décision judiciaire, ou d'un terme plus large « изъятие », qui englobe à la fois « выемка » et une inspection et toute autre action d'enquête et activités opérationnelles et d'enquête qui peuvent inclure la saisie d'objets de quelque manière que ce soit.

Le terme « *grooming »,* pour désigner « la sollicitation ou la manipulation psychologique aux fins de commettre une infraction sexuelle à l'encontre d'un enfant » figurant à l'article 15 de la Convention, n'a pas d'équivalent en russe pour désigner le phénomène en question, qui pourrait être considéré comme un emprunt étranger courant pouvant être utilisé dans des actes juridiques de ce niveau. L'étymologie du mot est d'une manière ou d'une autre liée à la galanterie, à la cajolerie. Le terme translitteré « grooming » en russe est utilisé principalement dans ses autres significations dans les domaines de la zoologie et des procédures de soins aux animaux de compagnie. Par conséquent, le terme anglais en un seul mot reçoit une définition en russe qui reflète l'essence du

phénomène - la création de relations de confiance (dans le but de commettre une infraction sexuelle à l'encontre d'un enfant).

Conclusion

Tout traité international, en particulier multilatéral, est plus ou moins le fruit d'un compromis. Dans le cas de la Convention, il s'agissait d'un équilibre délicat et d'un compromis au carré, qui a priori n'était pas en mesure de générer quelque chose de très percutant. Mais contre toute attente, il a été possible d'élaborer un texte recherché de grande qualité, qui intègre une combinaison de meilleurs éléments des conventions de Palerme et de Budapest. L'allégorie de l'enfant est appropriée pour tout traité international (et pas seulement pour un traité bilatéral, qui est plus naturel dans ce sens), et pour la Convention en particulier. Ce premier-né tant attendu a été élevé dans un environnement toxique qui n'avait pas grand-chose à voir avec l'esprit des Nations Unies, et il est né dans l'agonie, contre les desseins et les demandes des parents délibérément incompatibles. Quoi qu'il en soit, la Convention est notre propre enfant, dont le développement sain et la réussite sont entre nos mains.

Nous devrons tous poursuivre et améliorer notre travail professionnel, difficile et laborieux pour lutter contre la cybercriminalité dans l'architecture multipolaire de l'ordre mondial contemporain, y compris le bloc des États « inamicaux »[36], maintenant que nous disposons d'un nouvel outil universel, dont l'efficacité dépendra principalement de nous-mêmes, et qu'un nouveau jour férié sera déclaré en l'honneur de l'adoption de la Convention - la Journée internationale de la lutte contre la cybercriminalité. Les succès spécifiques que nous allons célébrer ce jour-là dépendent également de nous.

Publication originale :

Литвишко П. Первый глобальный договор против киберпреступности: от геополитической конфронтации к профессиональному компромиссу // Международная жизнь. – 2024. – № 11. – С. 4–27.

URL: https://interaffairs.ru/virtualread/ia_rus/112024/files/assets/downloads/publication.pdf

Auteur : Petr Litvichko, Candidat ès sciences juridiques, Directeur Général adjoint de la Direction Générale de la coopération juridique internationale – Directeur de la Direction d'entraide judiciaire et d'application des lois, Parquet Général de la Fédération de Russie, Assistant principal du Procureur Général de la Fédération de Russie

---

1 À l'heure actuelle, la capitale du Viêt Nam est provisoirement envisagée comme lieu possible d'ouverture de la Convention à la signature, c'est pourquoi elle pourrait, selon la tradition, être appelée la Convention de Hanoï.

2 L'auteur était membre de la délégation de la Fédération de Russie au Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles (2021-2024), membre du groupe pour l'harmonisation des versions linguistiques du Comité spécial représentant la Fédération de Russie.

Le contenu de cette publication reflète les évaluations juridiques de l'auteur et ne représente pas l'opinion officielle.

3 Le terme argotique « porte dérobée », courant dans l'environnement international de la sécurité de l'information et au-delà, n'est pas toujours utilisé correctement en relation avec la pratique contractuelle consistant à introduire des dispositions indésirables dans un document en cours d'élaboration (des « portes dérobées en matière de droits de l'homme », etc.), car il ne tient pas compte de l'étymologie et de la signification dans le lexique cybernétique du terme « porte dérobée » (*backdoor*), dont il est dérivé. Il implique donc, avant tout, la nature secrète ou au moins implicite de la mise en œuvre et du fonctionnement de certaines fonctionnalités cachées ou non déclarées (voir les termes et définitions de la norme GOST R 51275-2006). Compte tenu de la nature évidente des dispositions contractuelles et de leur effet escompté (comme dans le cas des « portes dérobées en matière de droits de l'homme »), il est incorrect de les considérer comme des moyens de portes dérobées.

4 National legal frameworks and approaches to challenges in gathering electronic evidence across borders in light of the new global Convention provisions: Russian Federation's perspective: Side event at the Concluding session of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes; United Nations HQ, New York, Jan. 30, 2024.

Les documents ci-après proviennent du site web officiel du Comité spécial.
URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (date de référence: 14.10.2024)

5 CyberUA: Strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine // Site web du Conseil de l'Europe. URL: https://www.coe.int/en/web/kyiv/cyberua (date de référence: 14.10.2024); Eurojust and the war in Ukraine; Core International Crimes Evidence Database (CICED) // Site web d'Eurojust. URL: https://www.eurojust.europa.eu/eurojust-and-the-war-in-ukraine (date de référence: 14.10.2024) ; *Hill S.* International Efforts to Collect Evidence Related to Russia's Aggression Against Ukraine // Saint Louis University Law Journal. 2024. Vol. 68. No. 2. P. 243–255 ; *Quilling Ch.* The Future of Digital Evidence Authentication at the International Criminal Court // Journal of Public & International Affairs. 2022. P. 7 ; *Назарко А.А.* Електронні докази в українському кримінальному судочинстві: Дослідження правових реалій та теоретичних перспектив // Науковий вісник Ужгородського Національного Університету. Серія Право. 2023. Вип. 80. Ч. 2. С. 183–188 [Nazarko A.A. Preuves électroniques dans la justice pénale ukrainienne : étude des réalités juridiques et perspectives théoriques // Bulletin scientifique de l'Université nationale d'Oujhorod. Série Droit. 2023. Numéro 80. Ch. 2. Pp. 183-188] ; *Литвишко П.А.* Уголовно-процессуальные аспекты решения Международного Суда ООН по делу «Украина против Российской Федерации» от 31 января 2024 года // Вестник Университета прокуратуры Российской Федерации. 2024. № 4(102). С. 108–123 [Litvichko P.A. Aspects procéduraux pénaux de la décision de la Cour internationale de Justice dans l'affaire « Ukraine contre Fédération de Russie » du 31 janvier 2024 // Bulletin de l'Université du Parquet de la Fédération de Russie. 2024. N° 4(102). Pages 108-123].

6 Practical Guide for Requesting Electronic Evidence across Borders. Vienna: United Nations, 2021. P. 39.

7 Selon les sources officielles d'interprétation de certaines conventions universelles, le terme « procédure judiciaire » (*judicial proceedings*) utilisé dans ces conventions peut inclure dans certains pays la procédure avant jugement, tandis que le terme « procédure » (*a proceeding*) « vise toutes les procédures publiques officielles, qui peuvent inclure la phase précédant le procès ». Le terme « proceedings », selon le contexte, peut désigner la procédure en général (procédure pénale, qui commence au moment du signalement d'une infraction, aux termes du Code de Procédure Pénale de la Fédération de Russie et d'autres systèmes juridiques continentaux), plutôt que la notion plus étroite de « jugement », ainsi qu'un acte procédural distinct.

Consultez : Legislative guides for the implementation of the United Nations Convention against Transnational Organized Crime and the Protocols thereto. New York: United Nations, 2004. P. 217, 220. Paras. 453, 465; Legislative guide for the implementation of the United Nations Convention against Corruption. New York: United Nations, 2012. P. 168. Para. 597; Technical guide to the United Nations Convention against Corruption. New York: United Nations, 2009. P. 163; Legislative Guide to the Universal Legal Regime against Terrorism. New York: United Nations, 2008. P. 39–40; Travaux préparatoires des négociations en vue de l'élaboration de la Convention des Nations Unies contre la criminalité transnationale organisée et des protocoles s'y rapportant (New York : Nations Unies, 2006. P. 222); UNODC Revised Manual on the Model Treaty on Mutual Assistance in Criminal Matters. P. 67–68, 70. Paras. 5–7, 12; Mutual Legal Assistance Manual. Belgrade: Council of Europe Office in Belgrade, 2013. P. 75.

8 Pour plus d'informations, consultez: Кольцов Д.В. Негласные оперативно-розыскные мероприятия как форма реализации специальных методов расследования в российском законодательстве // Труды Академии управления МВД России. 2022. № 4(64). С. 147–158.

[Koltsov D.V. Activités opérationnelles et d'enquête secrètes comme forme de la mise en œuvre de techniques d'enquête spéciales dans la legislation russe // Ouvrages de l'Académie de gestion du Ministère de l'Intérieur de la Russie. 2022. N 4(64). Pages 147-158.].

[9] Référentiel d'aide à la lutte contre la traite des personnes. New York : Nations Unies, 2008. Outil 5.2–5.5. Pages 177–185 ; Литвишко П.А. Международное сотрудничество в области борьбы с преступностью: избранные вопросы // Сборник материалов по международному сотрудничеству Следственного комитета Российской Федерации. М., 2015. С. 213–233 [Litvichko P.A. Coopération internationale dans la lutte contre la criminalité : questions choisies // Collection de documents sur la coopération internationale du Comité d'enquête de la Fédération de Russie. M., 2015. Pages 213-233.].

[10] Règlement (UE) 2023/1543 du Parlement Européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution des peines privatives de liberté prononcées à l'issue d'une procédure pénale ; Directive (UE) 2023/1544 du Parlement Européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales.

[11] Explanatory notes on the Updated draft text of the convention and the revised draft parquet Assembly resolution, 15 July 2024. P. 14; Discours lors de la reprise de la session finale du Comité spécial (New York, 29 juillet – 9 août 2024) : Interprétation du terme « enquête » ; Statement by the delegation of the Russian Federation at the resumed final session of the UN Ad Hoc Committee (New York, July 29-August 9, 2024): Interpretation of the term "Investigation."

[12] Consultez, par exemple: Posición del Ecuador respecto al texto aprobado. P. 1.

[13] Réception de l'intervention sur les connections qui ont eu lieu entre les abonnés et (ou) entre les terminaux des abonnés (article 186^1 du Code de procédure pénale de la Fédération de Russie), examen et collecte des messages électroniques ou autre messages transmis via les réseaux des communications électroniques (alinéa 7 de l l'article 185 du Code de procédure pénale de la Fédération de Russie), contrôle et enregistrement des conversations et autres communications ainsi que la réception de l'information sur les connections entre les abonnés ou les terminaux des abonnés en temps réel (articles 186-186^1 du Code de procédure pénale de la Fédération de Russie).

[14] Contrôle des messages, mis en écoute des conversations, captage des informations sur les canaux techniques, collecte des informations relatives aux ordinateurs (article 6 de la Loi fédérale № 144-ФЗ du 12.08.1995 sur la recherche et l'enquête).

[15] Note explicative du projet de loi fédérale N 280226-8 « Sur la modification des articles 453 et 456 du Code de procédure pénale de la Fédération de Russie » (sur la question de la fonction consulaire pour accomplir certaines actions procédurales dans les affaires pénales à la demande des autorités compétentes de l'État d'envoi) ; Procédure pénale en Russie et dans les pays européens : recherche juridique comparée : monographie / éditée par S.P. Chtcherba. M. : Prospekt, 2023. Pages 174-205.

[16] Consultez également : Déclaration de la délégation de la Fédération de Russie à la cinquième session du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles (Vienne, 11-21 avril 2023).

[17] Pour plus d'informations, consultez : *Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries*: Experiences and Problems: Monograph / editors S.P. Shcherba (Russian ed.) and P.A. Litvishko (English ed.). Moscow: Publishing House "Gorodets", 2024. P. 158–195.

[18] Transborder access to data and jurisdiction: Options for further action by the T-CY: Report prepared by the Ad-hoc Subgroup on Transborder Access and Jurisdiction adopted by the 12th Plenary of the T-CY (2-3 Dec. 2014) (T-CY (2014)16 of 3 Dec. 2014). P. 5, 10–11. Paras. 2.2.1, 2.4; Criminal justice access to data in the cloud: challenges: Discussion paper prepared by the T-CY Cloud Evidence Group (T-CY (2015)10 of 26 May 2015). P. 6. Para. 2.2.
Ci-après les documents provenant du site officiel du Comité de la Convention sur la cybercriminalité (Convention de Budapest): URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (date d'accès : 14.10.2024).

[19] Explanatory Report to the Convention on Cybercrime. Budapest, 23.XI.2001. P. 21. Para. 135.

[20] Voir: Déclaration de la délégation de la Fédération de Russie à la cinquième session du Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles (Vienne, 11-21 avril 2023).

[21] Voir aussi : Collecting electronic evidence... P. 81-157.

[22] Le projet de loi n° 462337-8 "L'amendement du Code pénal de la Fédération de Russie et de l'article 151 du Code de procédure pénale de la Fédération de Russie" (en ce qui concerne l'établissement de la responsabilité pour la mise en œuvre illégale d'actes d'enquête et d'autres actes de procédure et d'activités opérationnelles et d'enquête sur le territoire de la Fédération de Russie. Note explicative relative au projet.

[23] T-CY Guidance Note #10: Production orders for subscriber information (Article 18 Budapest Convention) adopted by the T-CY following the 16th Plenary by written procedure (28 Feb. 2017) (T-CY(2015)16 of 1 Mar. 2017). Para. 3.1.

[24] Déclaration de la Fédération de Russie au Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles sur l'ensemble du texte de la Convention (le 30 juillet 2024).

[25] T-CY Guidance Note # 3: Transborder access to data (Article 32) adopted by the 12th Plenary of the T-CY (2-3 Dec. 2014) (T-CY (2013)7 E of 3 Dec. 2014). P. 4–5, 7–8. Paras. 3, 3.6, 3.8.

[26] T-CY Guidance Note #10. Para. 3.1.

[27] La note d'orientation indique qu' « il faut tenir compte du fait que de nombreuses Parties [à la Convention] s'opposeraient à ce qu'une personne physiquement présentée sur leur territoire soit directement approchée par des forces de l'ordre étrangers désirant sa coopération ; certains pays considèrent même cette démarche comme une infraction pénale. ».

[28] Voir aussi : Accord entre le Gouvernement de la Fédération de Russie et le Gouvernement de la République de Tadjikistan sur la coopération visant à assurer la sécurité informatique internationale du 19.06.2023 (art. 7) ; Accord entre le Gouvernement de la Fédération de Russie et le Gouvernement de la République de l'union du Myanmar sur la coopération visant à assurer la sécurité informatique internationale du 05.12.2023 (art. 3).

[29] Pour plus de détails voir : *Collecting Electronic Evidence*...P. 195–209.

[30] *Ibid.* P. 81–126.

[31] Model Law on Mutual Assistance in Criminal Matters (2007), as amended with provisions on electronic evidence and the use of special investigative techniques (2022) (UN Doc. E/CN.15/2022/CRP.6 of 11 May 2022).

[32] Explanatory notes on the Updated draft text of the convention and the revised draft General Assembly resolution, 15 July 2024. P. 16.

[33] Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Strasbourg, 12.V.2022. Paras. 99, 128.

[34] Pour plus de détails voir: *Collecting Electronic Evidence*...P. 58–59, 210–221.

[35] Ainsi, conformément à la déclaration de la Fédération de Russie à l'article 24 de la Convention européenne d'entraide judiciaire en matière pénale de 1959, telle qu'amendée par l'article 6 du deuxième protocole additionnel de 2001, les tribunaux, les organes du Parquet, les organes d'enquête et d'instruction préliminaire sont considérés comme des organes judiciaires dans la Fédération de Russie (Loi fédérale du 06.06.2019 No. 120-FZ « Sur la ratification du deuxième protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale »).

[36] Литвишко П. Антикриминальное взаимодействие Российской Федерации с иностранными государствами и территориями, совершающими недружественные действия в отношении Российской Федерации, ее юридических и физических лиц // Законность. 2024. № 5(1075). С.26-35. [Litvichko P. L'interaction dans la lutte contre la criminalité entre la Fédération de Russie et les États et territoires étrangers qui commettent des actes inamicaux à l'encontre de la Fédération de Russie, de ses personnes morales et physiques // Légalité. 2024. N 5(1075). Pages 26–35.]