DOI: https://www.doi.org/10.31178/AUBD-FJ.2026.2.10

Forum Juridic nr. 2 / 2026

ANALELE UNIVERSITĂȚII DIN BUCUREȘTI - SERIA DREPT

Les sanctions applicables pour les infractions pénales commises dans le cyber espace comme limitation des droits de l'homme

Asist. univ. dr. Dorel Herinean
Faculté de Droit, Université de Bucarest

Résume : *Toute sanction appliquée à une personne implique une limitation inhérente de ses droits et libertés. Les sanctions prévues par la loi et appliquées dans la pratique judiciaire doivent être individualisées tant par rapport à l'infraction qu'à la personne. Sous cet angle, on peut considérer que certaines catégories de faits présentent des éléments communs en matière de sanctions, et l'objet de la présente étude est d'examiner ces éléments communs aux infractions informatiques lato sensu. L'article analyse les sanctions applicables en droit pénal roumain et, surtout, l'effet qu'elles peuvent produire dans le cyberespace, en vérifiant également les limites et les exemples de bonnes pratiques analysés dans la jurisprudence de la Cour européenne des droits de l'homme, et en passant en revue quelques exemples retrouvés dans d'autres juridictions. L'article se termine par une réflexion sur l'efficacité des sanctions classiques en cas d'infractions commises exclusivement dans le milieu numérique et sur la nécessité d'adapter la législation actuelle afin que les peines atteignent réellement leur objectif préventif.*

Mots-clés: *sanctions de droit pénal; infractions informatiques; peines complémentaires; cyber espace; droits de l'homme.*

Sancțiunile aplicabile infracțiunilor comise în cyberspațiu - o limitare a drepturilor omului

Rezumat: *Orice sancțiune aplicată unei persoane implică o inerentă limitare a drepturilor și libertăților acesteia. Sancțiunile prevăzute de lege și aplicate în practica judiciară trebuie individualizate atât în raport de faptă, cât și în raport de persoană. Din această perspectivă, se poate considera că anumite categorii de fapte au elemente comune care influențează sancțiunile, iar scopul prezentului articol este să studieze acele elemente comune infracțiunilor informatice* lato sensu*. Articolul analizează sancțiunile reglementate în dreptul penal român și mai ales efectul pe care acestea îl pot produce în cyberspațiu, verificând totodată limitele și exemplele de bune practici analizate în jurisprudența CEDO și trecând în revistă câteva exemple regăsite în alte jurisdicții. Articolul se încheie cu o reflecție privind eficiența sancțiunilor clasice în cazul infracțiunilor comise exclusiv în mediul digital și necesitatea adaptării legislației actuale pentru ca pedepsele să își atingă în mod real scopul preventiv.*

Cuvinte cheie: *sancțiuni de drept penal; infracțiuni informatice; pedepse complementare; cyberspațiu; drepturile omului.*

The sanctions applicable for the crimes committed in cyberspace as limitations of human rights

Abstract: *Any sanction applied to a person entails an inherent limitation of that person's rights and freedoms. Sanctions provided for by law and applied in judicial practice must be individualised both in relation to the offence and to the offender. From this perspective, it may be considered that certain categories of facts share common sanctioning elements, and the aim of the present study is to examine those elements common to lato sensu cyber offences. The article analyses the sanctions applicable under Romanian criminal law and, above all, the effect they may produce in cyberspace, while also verifying the limits and the examples of good practice analysed in the case law of the European Court of Human Rights, and reviewing several examples found in other jurisdictions. The article concludes with a reflection on the effectiveness of classical sanctions in the case of offences committed exclusively in the digital environment and on the need to adapt the current legislation so that penalties genuinely achieve their preventive purpose.*

Keywords: *criminal law sanctions; cyber offences; ancilliary penalties; cyberspace; human rights.*

INTRODUCTION

La nécessité d'incriminer et de sanctionner certains comportements adoptés exclusivement dans l'environnement en ligne est une question sensible. En ce sens, le caractère *ultima ratio* du droit pénal impose un filtre important, le droit pénal ne devant intervenir que lorsqu'une atteinte significative est portée aux valeurs sociales par l'adoption d'un comportement tel que celui décrit par le modèle abstrait de l'incrimination. Parfois, la réponse à la question « à quel point significatif ? » est difficile à apporter et peut varier d'un cas à l'autre.

Il est donc nécessaire de procéder, tout d'abord, à une incrimination prudente des comportements commis dans l'environnement en ligne, en utilisant des termes suffisamment génériques pour permettre d'englober l'ensemble du spectre des comportements considérés comme socialement dangereux, mais en même temps suffisamment précis pour satisfaire aux exigences de prévisibilité.

Il revient ensuite à la pratique judiciaire d'interpréter et d'appliquer les normes d'incrimination. Comme il a été montré dans un travail antérieur[1], en matière de cybercriminalité et de comportements pouvant être adoptés dans le cyberespace, la pratique nationale a été confrontée à plusieurs problèmes, qui ont rendu nécessaire le prononcé de plusieurs décisions d'unification de la pratique judiciaire ou de résolution de questions de droit en la matière. Nous pensons que le développement de plus en plus rapide de la technologie, et en particulier de l'intelligence artificielle, catalysera à la fois le problème et la solution. D'une part, elle permet de s'informer et d'expliquer des concepts techniques difficiles de manière plus accessible, sous réserve que les explications fournies soient correctes. D'autre part, du fait de cette technologie, les problèmes deviennent de plus en plus

[1] *D. Herinean*, La prévisibilité de l'incrimination des actes commis dans le cyber espace, dans AUBD – Forum juridic n° 1/2025, disponible ici.

complexes d'un point de vue technique. Quoi qu'il en soit, et indépendamment de ces technologies, la tendance générale de la pratique judiciaire est d'encourager un afflux de décisions à caractère obligatoire, et l'utilisation de la technologie ainsi que le recours à des moyens d'information faciles et à portée de main conduiront, à notre avis, à une amplification de cette tendance à rechercher des certitudes et des réponses simples et tranchées, même à des questions complexes. Or, une telle tendance devrait finalement influencer la politique pénale de l'État et la manière dont le législateur entend rédiger les normes d'incrimination.

Au-delà de ces aspects préliminaires, nécessaires à la suite du développement du sujet, et avant d'aborder la question qui donne son titre à notre étude, à savoir la sanction de ces comportements, nous jugeons utile de consacrer quelques lignes de cette introduction à la situation inverse, à savoir l'absence de sanction de certaines infractions commises dans le cyberespace, afin d'en établir les limites extérieures.

L'absence de sanction peut, bien entendu, découler en premier lieu de l'absence d'incrimination, c'est-à-dire de l'absence de prévision d'un fait dans un modèle abstrait d'incrimination. En matière de cybercriminalité, la Convention de Budapest constitue la pierre angulaire des normes d'incrimination, et la Convention des Nations Unies contre la cybercriminalité représente l'état de l'art dans le domaine de la cybercriminalité[2]. Par ailleurs, la décision de criminaliser (ou non) certains comportements plus ou moins socialement dangereux est influencée par de multiples facteurs, tels que la politique pénale, la morale, la nécessité de protéger certaines catégories de personnes, etc. Ensuite, là où il existe des normes d'incrimination, d'autres sources d'absence de sanction peuvent apparaître, telles que les causes qui excluent le caractère pénal du fait (les causes justificatives et les causes de non-imputabilité) ainsi que les causes de non-punissabilité, générales et spéciales. De même, les tentatives inidoines et les infractions putatives ne sont pas sanctionnées *de lege lata*, le législateur ne les ayant pas incriminées. Nous ne traiterons cependant pas de tous ces éléments dans notre article, leur analyse dépassant largement l'objet que nous nous sommes fixés.

Une autre observation préliminaire est que les sanctions appliquées ne sont pas toujours directes, puisqu'il peut exister des mesures procédurales, des situations ou des circonstances qui interviennent au cours d'un procès et qui ont, par ricochet, un effet sanctionnateur. Dans ces cas, outre la prolongation excessive des mesures préventives, nous pensons en particulier à la durée excessive du procès pénal[3].

I. ANALYSE DES SANCTIONS APPLICABLES EN DROIT PÉNAL ROUMAIN, DES LIMITES QU'ELLES IMPOSENT AUX DROITS ET LIBERTÉS DE LA PERSONNE CONDAMNÉE, AINSI QUE DE LA MANIÈRE DONT CES DROITS PEUVENT INFLUENCER L'INDIVIDUALISATION, L'APPLICATION ET L'EXÉCUTION DE CES SANCTIONS

Une limite importante aux sanctions consiste naturellement dans la nécessité de protéger les droits et libertés humains fondamentaux. Le dictum *nullum poena sine lege* est la première étape éclairante à cet égard, imposant la nécessité que les sanctions soient expressément prévues dans la loi et interdisant la possibilité de créer des sanctions

[2] Pour une analyse de celle-ci, voir *G. Zlati*, Succinte considerații pe marginea Convenției Națiunilor Unite împotriva criminalității informatice, dans Revista Dreptul n° 10/2025, pp. 105-124

[3] Pour une analyse approfondie du délai raisonnable dans le procès pénal, voir *C. Bălan,* Termenul rezonabil în procesul penal român, Éd. Hamangiu, Bucarest, 2021.

prétoriennes sans fondement juridique, même à des fins nobles, telles que l'individualisation ou l'efficacité de la punition.

Ensuite, certains droits et libertés ne peuvent être interdits à titre de sanction, tels que le droit à la vie, l'interdiction de la torture ou de la soumission à des traitements inhumains ou dégradants, l'interdiction d'imposer un travail forcé, etc. D'autres droits ne bénéficient pas d'une protection absolue, mais leur existence impose l'établissement de certains filtres tant pour les normes d'incrimination[4] que pour les sanctions.

Ce qui intéresse notre étude, c'est de savoir s'il existe de telles limites spécifiques imposées par les droits de l'homme dans le cas des infractions commises dans le cyberespace et, surtout, si les effets des sanctions imposées pour ces infractions peuvent comporter des limitations en ce qui concerne l'activité dans l'environnement en ligne. En analysant sous cet angle la Convention européenne des droits de l'homme, on constate qu'elle ne consacre pas directement de droits spécifiques à l'environnement numérique (ce qui s'explique aisément, compte tenu de l'époque de sa rédaction), mais il existe de multiples droits dont l'applicabilité a été et est étendue, y compris à cet environnement. Pour n'en citer que quelques-uns : les droits liés à la vie privée et à la correspondance, à la liberté d'expression et d'information, à la non-discrimination, ainsi que la légalité des délits et des peines.

En ce qui concerne la légalité des délits et des peines, il existe certaines situations dans lesquelles les sanctions imposées par différentes plateformes, qui entraînent des conséquences pécuniaires importantes, une limitation de la liberté d'expression et l'interdiction d'utiliser la plateforme concernée, pourraient être considérées comme équivalentes à certaines sanctions de nature pénale, voire plus graves que celles-ci, même si elles sont imposées par des entités privées. Certes, une telle approche peut facilement être réfutée en faisant valoir qu'en réalité, il n'existe pas de *droit* d'une personne d'accéder à une plateforme donnée ou d'utiliser un service donné dans des conditions autres que celles imposées par son titulaire. Même si, *ad absurdum*, on considérait qu'un tel droit devrait exister ou qu'il pourrait être déduit d'autres droits (l'interdiction de la discrimination, par exemple), un tel droit ne serait certainement pas absolu, de sorte qu'il permettrait des limitations, y compris par les mesures adoptées par le titulaire de l'espace virtuel, la nécessité même que ces mesures soient prévisibles étant, à l'heure actuelle, discutable.

Par ailleurs, en analysant une modification législative récente concernant les infractions informatiques, nous ne pouvons manquer de relever l'approche de notre législateur au regard de la hiérarchie et de l'importance abstraite des droits et libertés fondamentaux, approche qui peut être jugée bizarre : avant la loi n° 123/2026, entrée en vigueur en juillet 2026, qui a introduit l'article 365[1] dans le Code pénal, l'intégrité des systèmes informatiques et des données informatiques était considérée comme une valeur sociale inviolable au regard des finalités (nobles) susceptibles de justifier une ingérence et d'entraîner l'absence de typicité du fait, alors que tant la vie privée que le secret de la correspondance admettaient des exceptions et des justifications fondées sur des circonstances liées au fait et/ou au but ou au mobile de l'action. Nous ne pouvons manquer de relever l'ironie du fait que les données informatiques, protégées de manière absolue jusqu'à récemment, pouvaient précisément contenir des éléments et des informations

[4] Par exemple, pour une analyse de la configuration juridique du droit à la vie privée comme limite de la répression pénale, voir *F.C. Bobei*, Consimțământ, autonomie și viață privată în dreptul penal – 2021, dans le volume « Dreptul crizei. Crizele dreptului », Éd. Universul Juridic, Bucarest, 2021, pp. 765-766.

relevant de la vie privée de la personne et/ou de sa correspondance. Toutefois, même dans le paradigme législatif actuel, la situation reste la même s'agissant de l'autorisation légale de commettre des infractions : celui qui veut prouver une infraction est autorisé à violer le secret de la correspondance (uniquement de celle stockée physiquement) et à enregistrer une personne se trouvant dans un espace privé[5] sans son consentement, mais il ne peut pas accéder au téléphone de la personne qui détient des preuves à charge stockées sous forme de données informatiques. Or, ce « deux poids, deux mesures », bien qu'il puisse s'expliquer *pro causa* ou *pro jure* à l'aide de nombreux arguments plus ou moins abstraits et plus ou moins fondés, contredit le bon sens juridique, puisqu'il protège une subdivision du droit de propriété (si l'on peut encore considérer aujourd'hui que l'intégrité des systèmes informatiques et des données informatiques – privés, et non étatiques – se réduit à cela) avec une force plus grande que la vie privée et le secret de la correspondance, qui sont des valeurs intimes et personnelles.

Cela dit, dans ce qui suit, nous examinerons les sanctions applicables et analyserons chaque cas individuellement.

Analyse des sanctions existantes en droit pénal en roumain

Les peines principales occupent toujours la première place dans toute discussion relative à la sanction en droit pénal, même si, dans le contexte de notre analyse, elles ne suscitent pas autant de discussions que les autres. L'amende est une sanction éminemment pécuniaire, dont l'application entraîne des conséquences patrimoniales classiques, les conséquences par ricochet sur d'autres aspects de la vie de la personne condamnée n'étant pas interdites. Ainsi, il n'existe aucun élément spécifique en ce qui concerne les infractions commises dans le cyberespace. Il convient peut-être de mentionner, toutefois, que même dans le cas des infractions commises dans le cyberespace, lorsque l'auteur poursuit l'obtention d'un avantage patrimonial, l'amende accompagnant la peine d'emprisonnement peut être appliquée, sur le fondement de l'art. 62 du Code pénal, même si la peine d'amende n'est pas prévue par la norme d'incrimination. L'applicabilité de cette peine ne dépend toutefois pas de l'obtention effective de cet avantage patrimonial, mais seulement de la possibilité de l'obtenir par la commission du fait. Toujours en ce qui concerne la peine d'amende, il convient de préciser que, lors de son individualisation, le montant correspondant à un jour-amende est fixé, conformément à l'art. 61 al. (3) deuxième phrase du Code pénal, en tenant compte de la situation matérielle du prévenu, ses actifs numériques, tels que les cryptomonnaies, pouvant également être pris en considération à cet égard, pour autant, évidemment, qu'ils soient connus des organes judiciaires[6].

L'emprisonnement et la détention à perpétuité[7], par la privation de liberté que chacun

[5] Cette notion a fait l'objet de débats récents dans la littérature spécialisée, suscités par une décision rendue par la Haute Cour de cassation et de justice dans le cadre de la résolution d'une question de droit. À cet égard, voir *F. C. Bobei, Efectele colaterale ale Deciziei HP nr. 18 din 22 aprilie 2024 a I.C.C.J.,* dans le volume Persoana în centrul dreptului penal: între libertate și răspundere Studii dedicate Profesorului Valerian Cioclei, Éd. C.H. Beck, Bucarest, 2026, pp. 60-69.

[6] À ce sujet, voir *A.-R. Trandafir, G. Zlati*, Monedele virtuale: între obținerea datelor privind tranzacțiile financiare și luarea măsurilor asigurătorii în procesul penal, publié dans AUBD – Forum juridic n° 1/2022, disponible ici.

[7] La discussion est plutôt théorique dans le cas de cette peine, la détention à perpétuité ne pouvant être appliquée pour la commission exclusive d'infractions informatiques.

d'eux implique, portent également atteinte à d'autres droits et libertés fondamentaux, outre celui, évident, qui concerne la liberté de circulation, et, surtout de nos jours, une partie d'entre eux concerne même la *vie numérique* de ces personnes et la possibilité d'accéder au cyberespace. Cette limitation inhérente des droits et libertés fondamentaux pendant la privation de liberté, notamment en ce qui concerne les possibilités de communication avec le monde extérieur et le libre échange d'informations et d'idées, a également été mise en évidence dans la jurisprudence de la Cour EDH, en particulier dans les affaires Kalda c. Estonie et Jankovskis c. Lituanie, que nous présenterons *infra*, la Cour ayant en outre précisé que l'article 10 de la Convention n'oblige pas les États à accorder aux détenus un droit d'accès à Internet si une telle possibilité n'est pas prévue par le droit interne.

Dans la législation roumaine, l'art. 66 de la loi n° 254/2013 a le contenu suivant : « *Art. 66 : Droit aux communications en ligne (1) Pour certaines catégories de personnes condamnées, la communication en ligne avec les membres de la famille ou d'autres personnes peut être facilitée. (2) Les catégories de personnes condamnées, le nombre et la durée des communications en ligne, ainsi que les modalités de leur octroi, sont établis par le règlement d'application de la présente loi* ». Selon les art. 134 et suivants du Règlement de 2016 d'application de la loi n° 254/2013[8], la communication en ligne peut être utilisée par les détenus « *en vue du maintien d'un lien constant et de l'augmentation des chances d'amélioration des relations avec l'environnement de soutien* », avec l'approbation préalable du directeur du pénitencier et sur rendez-vous, au maximum 4 fois par mois, chaque communication ne pouvant dépasser 30 minutes, en règle générale, certaines situations exceptionnelles étant toutefois prévues ; il est même possible de communiquer de cette manière avec des détenus d'autres pénitenciers.

Le matériel existant dans les pénitenciers se compose, selon l'art. 135 al. (2) du Règlement de 2016, d'ordinateurs, de webcams ou de caméras vidéo, de microphones et d'alimentations sans interruption (onduleurs), cet équipement devant être sécurisé contre le vandalisme et contre l'accès direct du détenu aux ordinateurs et aux périphériques. Par ailleurs, une limite importante figure à l'al. (4) du même article, qui prévoit que « *la connexion à Internet ne peut être utilisée à d'autres fins que celle pour laquelle elle a été mise en place* ». Il résulte de l'ensemble de ces dispositions que le droit d'accès à Internet, sous cet angle, est strictement limité au maintien des relations familiales.

Par ailleurs, l'article 59 de la loi n° 254/2013 régit le droit à l'information, en ce qui concerne les informations d'intérêt public, en précisant que ce droit « est également assuré par des publications, des émissions de radio et de télévision ou par tout autre moyen autorisé ». Il est en outre prévu que les personnes condamnées sont autorisées à communiquer avec les médias, dans le respect des mesures de sécurité du pénitencier et uniquement en l'absence de motifs fondés de l'interdire pour des raisons tenant à la protection des victimes, des autres personnes condamnées ou du personnel pénitentiaire.

L'observation qui ressort de toutes ces dispositions est que la législation roumaine ne prévoit pas, *de lege lata*, de droit pour les personnes condamnées d'accéder à Internet à des fins autres que celles strictement liées à la communication avec leurs proches par appel vidéo. Par conséquent, la législation roumaine restreint indirectement, pour les personnes détenues, la possibilité d'avoir une *vie numérique*.

[8] M. Of. n° 271/11.04.2016.

Observations sur la peine complémentaire d'interdiction d'exercer certains droits et sur les peines accessoires

Nous traiterons ensemble ces peines, car le régime des peines accessoires est déterminé par rapport aux peines complémentaires appliquées en cas de peine d'emprisonnement. Il est d'ailleurs communément admis que ce régime implique que les premières reprennent des secondes leur contenu en ce qui concerne les droits interdits, la seule différence résidant dans le droit prévu à la lettre c), à savoir le droit de l'étranger de se trouver sur le territoire de la Roumanie, qui ne peut être interdit à titre de peine accessoire en cas de peine d'emprisonnement. Le rôle des peines complémentaires est de parfaire et de compléter la répression assurée par la peine principale, les peines accessoires découlant de la peine principale et de la peine complémentaire[9]. Les peines complémentaires peuvent être appliquées, à titre facultatif, même lorsqu'elles ne sont pas prévues par les normes d'incrimination, sous réserve que le juge en constate la nécessité[10]. Nous apporterons ci-après quelques précisions ponctuelles sur les droits dont l'exercice peut être interdit à titre de peine complémentaire/accessoire et qui présentent un intérêt pour l'activité dans le cyberespace.

c) le droit de l'étranger de se trouver sur le territoire de la Roumanie ;

Ce droit concerne exclusivement le territoire physique de la Roumanie. Par conséquent, il ne pourrait pas être appliqué afin d'interdire l'accès au « cyberespace » roumain, à savoir aux sites portant l'extension .ro, aux sites des autorités publiques roumaines ou à ceux proposant des contenus destinés aux Roumains, quelle que soit, du reste, la manière dont un tel espace virtuel pourrait être délimité. La même observation vaut pour le droit prévu à la lettre j), à savoir le *droit de quitter le territoire de la Roumanie*, étant évident que la personne condamnée conserve la possibilité de quitter le cyberespace roumain en accédant à des sites étrangers.

g) le droit d'occuper la fonction, d'exercer la profession ou le métier ou de mener l'activité dont il s'est servi pour commettre l'infraction ;

En lien avec ce droit, l'exercice de professions ou d'activités spécifiques peut être interdit, telles que celles d'opérateur de bases de données, d'auditeur informatique, de développeur web, de spécialiste en cybersécurité, etc. De même, si cela s'avère nécessaire au regard de l'infraction commise, des activités telles que l'utilisation de certaines catégories de biens (drones, robots, etc.) peuvent également être interdites.

Il est intéressant de se demander dans quelle mesure une activité de type *influenceur* sur les réseaux sociaux pourrait être interdite. Le problème qui se pose à cet égard est que cette activité recouvre un large éventail d'activités variées, qui dépendent des centres d'intérêt et du public propres à la personne concernée. À notre avis, pour qu'une telle activité puisse être interdite, le juge ne pourrait pas se limiter à mentionner qu'il interdit l'activité d'*influenceur* de la personne ayant commis une infraction au moyen d'une telle activité (par exemple l'escroquerie, l'instigation publique, l'incitation à la haine et à la discrimination, etc.), mais il faudrait déterminer aussi concrètement que possible les limites dans lesquelles ces

[9] *C. Mitrache, Cr. Mitrache*, Drept penal român. Partea generală, VIe édition, Éd. Universul Juridic, Bucarest, 2025, p. 233.
[10] *L.V. Lefterache,* Drept penal. Partea generală, 4e édition, Éd. Hamangiu, Bucarest, 2024, p. 311.

interdictions s'appliquent et les activités concrètes qui sont interdites, en premier lieu pour des raisons de prévisibilité, mais aussi pour éviter d'aboutir à une interdiction trop générale ou trop étendue.

Lorsque l'on parle de professions ou d'activités dont l'exercice suppose une formation poussée et une ultra spécialisation, ce qui peut également être affirmé des spécialistes des technologies, surtout si l'on porte la discussion sur le terrain de l'intelligence artificielle, la sanction ayant le plus grand effet dissuasif est peut-être l'interdiction d'exercer cette activité ou cette profession, qui ne serait parfois ni dans l'intérêt de la personne, ni dans celui de la société, à laquelle profiterait également l'utilisation des compétences de l'auteur à des fins positives[11].

h) le droit de détenir, de porter et d'utiliser toute catégorie d'armes ;

Ce droit concerne exclusivement les armes dans l'environnement physique, et non les armes dans les jeux/mondes virtuels, compte tenu de la définition des armes existant dans la législation pénale[12].

i) le droit de conduire certaines catégories de véhicules déterminées par le tribunal ;

Comme dans le cas précédent, il est évident que ce droit ne concerne que les véhicules pouvant être conduits sur la voie publique, tels que définis par la législation routière. Quelques observations supplémentaires s'imposent toutefois dans le contexte du développement et de la mise en service, dans certains pays, des véhicules autonomes, qui se conduisent seuls. L'interdiction de ce droit viserait-elle également la possibilité pour la personne d'utiliser de telles voitures ? Selon nous, la réponse dépend de leur degré d'autonomie. S'il s'agit de voitures entièrement autonomes, qui se conduisent seules sans que l'intervention du passager soit nécessaire ou possible[13], cette interdiction ne serait pas applicable, la personne étant, en réalité, un simple passager de ce véhicule. En revanche, s'il s'agit d'une autonomie partielle, où la voiture se conduit seule en principe, mais où le passager a accès aux commandes et peut reprendre le contrôle en cas de besoin, de sorte qu'il est en réalité un conducteur subsidiaire, nous estimons que l'interdiction est applicable.

l) le droit de se trouver dans certaines localités établies par le tribunal + m) le droit de se trouver dans certains lieux ou lors de certaines manifestations sportives, culturelles ou d'autres rassemblements publics, établis par le tribunal + o) le droit de s'approcher du domicile, du lieu de travail, de l'école ou d'autres lieux où la victime exerce des activités sociales, dans les conditions établies par le tribunal.

Comme pour les obligations relatives au territoire de la Roumanie, l'interdiction est, dans ce cas également, d'ordre physique : elle interdit à la personne condamnée de se déplacer personnellement, dans l'environnement physique. Une telle obligation ne vise pas, en principe, les hypothèses dans lesquelles la personne pourrait envoyer un drone dans la

[11] Pour une analyse portant également sur l'interdiction de ces droits à l'égard du personnel médical, voir *T. Manea,* De la voința legiuitorului la pixul magistratului - despre sancționarea luării de mită comisă în cadrul sistemului medical, dans AUBD – Forum juridic n° 2/2024, disponible ici.

[12] Pour un bref développement du sujet, voir *D. Herinean*, Înțelesul unor termeni și expresii din dreptul penal în cyberspațiu, dans AUBD – Forum juridic n° 2/2024, disponible ici.

[13] Voir, par exemple, les robotaxis en Chine : https://www.reuters.com/business/autos-transportation/china-targets-mass-deployment-self-driving-vehicles-by-2030-2026-09-11/.

localité concernée (dans le respect des conditions légales d'autorisation et d'exploitation) ou un autre dispositif électronique doté de fonctions de filmage/enregistrement/lecture ou autres, tant qu'aucune autre infraction n'est commise par leur intermédiaire. Ainsi, pour prendre un exemple, même si une personne s'est vu interdire le droit de se trouver dans le stade d'une équipe de football, si, le jour d'un match, est diffusé sur l'écran du stade un *livestream* dans lequel la personne condamnée prononce un discours d'encouragement à l'adresse des supporters et de l'équipe, nous ne pensons pas que l'on puisse considérer que cette obligation a été violée, puisque, en réalité, la personne ne s'y trouve pas. Dans le même sens, un robot piloté par cette personne et se trouvant dans le stade ne saurait être considéré comme représentant une présence physique de la personne condamnée.

n) le droit de communiquer avec la victime ou avec des membres de sa famille, avec les personnes avec lesquelles le condamné a commis l'infraction ou avec d'autres personnes, établies par le tribunal, ou de s'approcher de celles-ci ;

Enfin, en ce qui concerne ce dernier droit, la communication interdite est à la fois directe et par voie de communication à distance, le tribunal pouvant établir concrètement, le cas échéant, la manière et les limites dans lesquelles la communication est autorisée ; l'absence de distinction conduit à une interdiction totale de la communication, par tous les moyens, écrits, audiovisuels, analogiques, numériques, etc.

Observations sur les autres peines complémentaires

Parmi les autres peines complémentaires, celle qui est pertinente pour notre discussion est la publication de la décision de condamnation, tant dans le cas des personnes physiques que dans celui des personnes morales. Bien que la nécessité de l'appliquer puisse sembler évidente dans le cas d'infractions commises publiquement dans l'environnement en ligne[14], nous nous demandons dans quelle mesure le contenu de cette mesure, dans sa réglementation actuelle, est apte à atteindre ses objectifs. Cette interrogation repose sur le constat qu'aujourd'hui, la presse traditionnelle ne parvient pas toujours à toucher le plus large public ou, s'agissant des infractions commises sur les réseaux sociaux, que le public concerné se trouverait plutôt sur ces réseaux sociaux que dans la presse traditionnelle. Par ailleurs, la réponse pourrait également varier selon que prévaut la finalité sanctionnatrice de la peine complémentaire (sanctionner davantage la personne condamnée) ou le besoin de faire connaître et de prévenir les méthodes infractionnelles, qui peut constituer un effet indirect de cette peine complémentaire, parfois au moins aussi important que l'effet sanctionnateur. Ainsi, nous pouvons envisager ce problème sous deux angles.

D'une part, s'agissant d'infractions commises par des influenceurs ou d'autres personnes sur les réseaux sociaux à l'encontre des utilisateurs de ces réseaux, la publication de la décision de condamnation dans le même environnement que celui où l'infraction a été commise devrait effectivement être la plus efficace, tant du point de vue de la sanction que d'un point de vue éducatif et préventif.

D'autre part, dans le cas d'infractions commises dans le cyberespace ou par téléphone à l'encontre de personnes qui n'utilisent pas régulièrement les réseaux sociaux, la presse traditionnelle pourrait être pertinente. À titre d'exemple, nous pensons à la désormais

[14] Pour une analyse du caractère public des faits commis en ligne, voir *D. Herinean*, Infracțiunile comise în mediul online – infracțiuni comise în public?, dans AUBD – Forum juridic n° 2/2024, disponible ici.

célèbre méthode dite « de l'accident » ou aux courriels/messages d'hameçonnage (*phishing*) par lesquels on crée la fausse impression que les auteurs sont des représentants de banques/sociétés de livraison de colis et on demande les données des cartes bancaires. Dans le cas de ces schémas infractionnels, l'éducation de la population quant à leur existence et aux méthodes de prévention peut s'avérer aussi efficace dans la presse traditionnelle que sur les réseaux sociaux.

Par conséquent, *de lege ferenda*, nous estimons qu'il serait utile d'introduire la possibilité pour le juge d'ordonner, lorsqu'il individualise cette peine complémentaire à la suite de la commission d'une infraction par des moyens numériques, également la publication de la décision de condamnation en ligne ou sur les réseaux sociaux, d'une manière équivalente à celle dont l'infraction a été commise. Bien entendu, même en l'absence d'une telle modification législative, il est déjà possible que le quotidien local ou national désigné par le tribunal publie la décision de condamnation également sur son site web ou sur ses comptes de réseaux sociaux, sans y être obligé par le tribunal. L'absence d'une obligation imposée par le tribunal n'empêche évidemment pas ce quotidien ou tout autre de reprendre l'information, dans le respect des dispositions applicables en matière de presse.

Observations sur les mesures de sûreté

L'interdiction d'occuper une fonction ou d'exercer une profession, la confiscation spéciale et la confiscation élargie présentent un intérêt pour notre sujet, les mesures de sûreté à caractère médical ne soulevant pas de discussions spécifiques, raison pour laquelle nous ne les aborderons pas.

En ce qui concerne l'interdiction d'occuper une fonction ou d'exercer une profession, la dénomination marginale simplifie à l'excès sa portée, puisque la mesure vise la possibilité d'interdire l'exercice du droit d'occuper cette fonction ou d'exercer cette profession, ce métier ou cette activité lorsque l'auteur a commis le fait en raison de son incapacité, de son manque de préparation ou d'autres causes qui le rendent inapte à l'activité en question, et non seulement une fonction ou une profession. Comme nous l'avons déjà montré *supra* à propos de la peine complémentaire correspondante quant à son contenu, les activités, métiers et professions d'une personne peuvent être exercés en tout ou en partie dans le cyberespace, de sorte que leur exercice doit également pouvoir être interdit.

Cependant, si, dans le cas d'une activité telle que la conduite d'un véhicule, il est aisé de comprendre comment on peut en arriver à cette inaptitude, les choses sont moins claires en ce qui concerne notre sujet et les exemples sont plus difficiles à fournir, d'autant qu'il doit également exister un lien de causalité entre cette incapacité et la commission du fait prévu par la loi pénale. Dans cette perspective, nous considérons que l'applicabilité de cette mesure de sûreté aux infractions commises en ligne serait extrêmement limitée, car ce n'est pas l'incapacité, mais l'indignité qui devrait fonder l'imposition d'une sanction, plus précisément de la peine complémentaire. Des exemples pourraient toutefois apparaître s'agissant du pilotage à distance de drones ou de robots, auquel cas on pourrait facilement imaginer la commission d'infractions en raison d'une inaptitude causée par un manque de préparation, une incapacité, une maladie, etc.

La confiscation spéciale implique le transfert forcé de certains biens[15] du patrimoine de l'auteur dans la propriété de l'État. Ainsi, à titre de première observation, pourront être confisqués les systèmes informatiques tels que les téléphones, tablettes, ordinateurs portables, etc., les supports de stockage (y compris les données informatiques qu'ils contiennent) et d'autres composants ayant une matérialité physique. En pratique, tout ce qui relève du matériel peut être confisqué, mais la partie logicielle ne peut pas l'être, pas plus que les données informatiques en tant que telles (séparément du support sur lequel elles sont stockées). Par conséquent, il n'est pas possible d'ordonner la confiscation de fichiers se trouvant dans un système informatique, de publications sur les réseaux sociaux ou de lignes de code, même s'ils ont été utilisés pour commettre l'infraction ou constituent la représentation (la *matérialisation*) numérique d'une infraction. En ce qui concerne ces derniers, par exemple les publications sur les réseaux sociaux, les lignes de code, les fichiers conservés dans un compte ou dans le *cloud*, il convient de noter que, *de lege lata*, il n'existe aucune sanction ni mesure que les organes judiciaires ou les juridictions pénales puissent ordonner pour obliger le prévenu/la personne condamnée à les supprimer. En pratique, le tribunal peut interdire certaines activités pour l'avenir (par le biais des peines complémentaires), mais il ne peut pas obliger le prévenu à en accomplir – comme celles de l'exemple ci-dessus –, en dehors de celles qui peuvent faire l'objet de peines complémentaires ou de mesures de sûreté, ainsi que des obligations et mesures de surveillance lorsqu'est ordonnée une forme d'individualisation de l'exécution de la peine autre que l'exécution effective.

En ce qui concerne la confiscation élargie, il convient de noter que, dans une analyse abstraite, les infractions informatiques (*lato sensu*) peuvent être de nature à procurer un avantage matériel, et que la peine prévue par la loi pour la plupart d'entre elles est l'emprisonnement supérieur à 4 ans. Toutefois, une analyse *in concreto* des infractions informatiques commises dans chaque cas est également nécessaire, afin de vérifier si le mode de commission vise ou permet l'obtention de tels avantages, et ce n'est que dans les cas où la réponse à cette question est affirmative que cette mesure de sûreté pourra être ordonnée.

II. LES PERSPECTIVES DE COUR EDH ET LES SOLUTIONS D'AUTRES ÉTATS EN CE QUI CONCERNE LES SANCTIONS APPLICABLES DANS LE CYBERESPACE

Les questions fondamentales dont part ce chapitre sont de savoir dans quelle mesure la peine d'emprisonnement est nécessaire et efficace en ce qui concerne la cybercriminalité et les infractions commises exclusivement en ligne, et si la législation actuelle, y compris au regard des règles existant au niveau international, est adaptée à l'application de telles sanctions.

Pour répondre à ces questions, nous analyserons dans le premier chapitre la jurisprudence pertinente de la Cour EDH en la matière, puis nous rechercherons des exemples de bonnes ou de mauvaises pratiques dans d'autres législations, pour aboutir enfin à une conclusion fondée sur les éléments examinés.

[15] Pour une analyse de la notion de *bien meuble* en ce qui concerne les objets numériques, voir *G. Zlati*, Dematerializarea obiectului material al infracțiunii în contextul evoluției tehnologice și consecințele acesteia, dans Dreptul, n° 9/2013 ; *D. Herinean*, Înțelesul unor termeni și expresii în cyberspațiu, op. cit., pp. 190-13.

Les sanctions appliquées ou les conséquences de ces sanctions en lien avec l'environnement numérique à la lumière de la jurisprudence de la CEDH

Parmi les droits et libertés fondamentaux de l'homme consacrés par la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, l'accès à Internet semble être le plus souvent analysé comme une composante de la liberté d'expression protégée par l'article 10. Certes, certaines composantes des activités pouvant être menées dans l'environnement virtuel relèveraient également du champ d'autres droits, tels que ceux prévus à l'article 8 (droit au respect de la vie privée), à l'article 9 (liberté de pensée, de conscience et de religion), à l'article 11 (liberté de réunion et d'association) et à l'article 2 du Protocole n° 1 (droit à l'instruction). Dans ce qui suit, nous passerons en revue la jurisprudence de la Cour EDH identifiée en la matière, en présentant d'abord les situations dans lesquelles des violations de la Convention ont été constatées, puis celles dans lesquelles il a été constaté qu'il n'avait pas été porté atteinte aux droits de l'homme.

Situations dans lesquelles des violations des dispositions de la Convention ont été constatées du fait des sanctions appliquées en lien avec le cyberespace

L'article 10 de la Convention constitue, de notre point de vue, le *sedes materiae* le plus important à cet égard, plusieurs arrêts ayant examiné son applicabilité et constaté sa violation. La plupart des situations concernent des cas dans lesquels des personnes se sont vu interdire l'accès à certains sites web qui leur étaient nécessaires, sans aucune justification ou sans motivation raisonnable. Ainsi, en ce qui concerne l'accès à Internet en milieu carcéral, dans l'affaire Kalda c. Estonie[16], une violation de cet article a été constatée parce que le détenu s'était vu refuser l'accès demandé à des sites web contenant des informations juridiques (appartenant à l'État et au Conseil de l'Europe), sans justification raisonnable. Dans cette affaire, la Cour a jugé que, bien que la Convention n'oblige pas les États à accorder aux détenus l'accès à Internet, si l'État accorde ce droit (comme c'était le cas de l'Estonie), la limitation de l'accès à certains sites ne peut intervenir qu'avec une motivation raisonnable, l'invocation vague des coûts impliqués et de motifs de sécurité abstraits n'étant pas considérée comme une motivation suffisante, notamment en ce qui concerne les sites d'information juridique et compte tenu de l'existence de moyens de surveillance de l'activité en ligne[17]. Une conclusion similaire a été retenue dans l'affaire Jankovskis c. Lituanie[18], dans laquelle un détenu s'était vu refuser *de plano* l'accès à un site contenant des informations sur les programmes d'études nécessaires à la poursuite de sa formation, au motif qu'il était interdit aux détenus d'utiliser des moyens de communication électroniques en prison, sans que les autorités aient évalué la possibilité d'un accès contrôlé. Dans le même sens, dans un autre arrêt[19], une violation de l'article 10 (sous l'angle du libre échange d'informations et d'idées) a été retenue dans une affaire où un avocat placé en détention provisoire avait demandé à être autorisé à accéder aux sites web de la Cour EDH, de la Cour constitutionnelle de Turquie et du Journal officiel, afin de préparer sa propre défense et de suivre les dossiers dont ses clients l'avaient chargé. Le contexte était qu'en Turquie, les personnes condamnées

[16] Affaire Kalda c. Estonie, 19 janvier 2016 (requête n° 17429/10).
[17] *Ibidem.*
[18] Affaire Jankovskis c. Lituanie, 17 janvier 2017 (requête n° 21575/08).
[19] Affaire Ramazan Demir c. Turquie, 9 février 2021 (requête n° 68550/17).

avaient accès à certains sites web à des fins de formation professionnelle et de réinsertion, de sorte qu'il a été retenu que l'interdiction faite à ce détenu d'accéder aux sites en question constituait une restriction arbitraire du droit en cause, les juridictions nationales n'ayant pas suffisamment expliqué pourquoi les objectifs de l'avocat ne pouvaient pas être qualifiés comme relevant de la formation professionnelle et de la réinsertion, et le détenu n'ayant pas été classé parmi les cas d'une gravité particulière dans lesquels l'accès peut être interdit. Dans cette perspective, la Cour a estimé que l'ingérence n'était ni nécessaire ni proportionnée dans une société démocratique.

Dans une autre affaire[20], une personne assignée à résidence s'était vu imposer, entre autres, l'interdiction *de recevoir ou d'envoyer toute forme de correspondance, lettres, télégrammes, colis ou courriels, et d'utiliser toute forme de communication et Internet*. Ces interdictions étaient prévues par la loi en vigueur. Dans sa requête devant la Cour EDH, le requérant a soutenu que la restriction de l'accès à Internet constituait une mesure disproportionnée, qui limitait son accès à l'information sans reposer sur un intérêt légitime. Bien que la Cour ait constaté une violation des articles 5, 10 et 18 en l'espèce, son analyse ne s'est pas spécifiquement concentrée sur la limitation de l'accès à Internet, la Cour ayant retenu que cette interdiction (à la différence d'autres) était prévue par le droit interne et pouvait être ordonnée tant qu'elle était nécessaire aux fins pour lesquelles elle avait été ordonnée, ce qui, en l'espèce (conjointement avec les autres obligations), n'a pas été jugé être le cas, les motifs étant soit génériques, soit infondés. Par conséquent, s'agissant d'une question d'individualisation et non de légalité, il convient d'observer que la prévision légale d'une telle interdiction absolue d'accéder à Internet, attachée à une mesure préventive, n'a pas été jugée excessive par la Cour (du moins en 2019).

Dans une autre série d'affaires[21], la Cour a jugé que, pour être conformes à l'article 10 de la Convention (et à l'article 13 dans certains cas), les dispositions légales permettant le blocage de sites web par les autorités publiques, à la demande du procureur et sans décision d'une juridiction susceptible de recours, doivent offrir des garanties suffisantes contre une application excessive et arbitraire ainsi qu'une possibilité effective de contester ces mesures, afin qu'il existe des mécanismes de protection contre les abus de la part de l'État.

Un autre droit dont la violation a été constatée est celui prévu à l'article 2 du Protocole n° 1, à savoir le droit à l'instruction, la Cour EDH ayant constaté sa violation du fait du refus d'accorder à des personnes détenues l'accès à un ordinateur et à Internet pour suivre ou, selon le cas, poursuivre des études supérieures à distance auxquelles l'un des requérants détenus était déjà inscrit et l'autre souhaitait s'inscrire[22]. Ainsi, en l'absence de justifications objectives fondées sur des raisons de sécurité pénitentiaire, la Cour EDH a constaté qu'aucun juste équilibre n'avait été ménagé entre l'objectif d'assurer la sécurité en prison et le droit à l'instruction, ce dernier ayant été sacrifié sans justification suffisante[23].

Dans d'autres affaires, des violations de l'article 8 de la Convention ont été constatées, mais elles concernent l'absence de protection accordée aux victimes par l'État, et non les sanctions appliquées à l'auteur. En pratique, on peut les envisager sous l'angle inverse : c'est

[20] Affaire Navalnyy c. Russie (n° 2), 9 avril 2019 (requête n° 43734/14)
[21] Affaires Vladimir Kharitonov c. Russie (requête n° 10795/14), OOO Flavus et autres c. Russie (requêtes n° 12468/15, 23489/15 et 19074/16), Bulgakov c. Russie (n° 20159/15) et Engels c. Russie (n° 61919/16).
[22] Affaire Mehmet Reşit Arslan et Orhan Bingöl c. Turquie, 18 juin 2019 (requêtes n° 47121/06, 13988/07 et 34750/07).
[23] *Ibidem.*

précisément l'absence de sanction qui a été considérée comme une violation des dispositions de la Convention. Ainsi, dans l'affaire K.U. c. Finlande[24], il a été jugé que l'État n'avait pas rempli son obligation positive de mettre en place une procédure permettant d'identifier l'auteur qui avait publié en ligne une annonce utilisant l'identité d'un mineur âgé de 12 ans (photo, adresse e-mail et numéro de téléphone, ce dernier étant toutefois erroné d'un chiffre), annonce qui suggérait que celui-ci cherchait à nouer des relations intimes avec des garçons de son âge ou des hommes plus âgés. Dans le même sens, dans une autre affaire[25], une violation de l'article 8 a été constatée parce que l'État n'avait pas protégé la victime d'un harcèlement en ligne, qui avait consisté dans la mise en ligne de ses données (y compris une photographie de son passeport) et d'images à caractère sexuel explicite sur un profil de réseau social à son nom, par son ancien concubin qui souhaitait se réconcilier avec elle. Des situations relativement similaires se retrouvent également dans les affaires Buturugă c. Roumanie[26] et M.Ș.D. c. Roumanie[27], dans lesquelles il a été jugé que ce que la législation actuelle a ultérieurement dénommé *cyberviolence* doit également être qualifié de forme de violence domestique. Toutes ces affaires ont été présentées afin de montrer que les modes de commission des infractions en ligne prennent parfois de court les législations nationales ou les pratiques des organes judiciaires, qui ne sont pas toujours adaptées aux dernières tendances.

Affaires dans lesquelles les sanctions appliquées ayant restreint des droits et libertés dans l'environnement digitale ont été jugées conformes à la Convention

À l'opposé, nous présenterons ci-après quelques situations dans lesquelles diverses sanctions (directes ou indirectes) appliquées à des personnes n'ont pas conduit au constat de violations de la Convention en ce qui concerne l'applicabilité de l'article 10. Par exemple, dans l'affaire Delfi AS c. Estonie[28], il a été constaté qu'il n'y avait pas de violation de la liberté d'expression lorsque la responsabilité civile d'un important portail d'information avait été engagée (des dommages-intérêts de 320 euros, qui ne peut être considérée comme excessive) pour des propos diffamatoires à l'encontre d'une entreprise publiés par des utilisateurs anonymes dans les commentaires d'un article, la Cour ayant établi que les grandes plateformes commerciales ont des obligations étendues et qu'une telle sanction était proportionnée[29]. Partant de cet arrêt, nous soulevons la question de savoir dans quelle mesure, à l'avenir, des sanctions pénales pourraient être instituées pour des comportements de type *failure to prevent* ou si des comportements omissifs des plateformes sociales en lien avec la modération des contenus qu'elles hébergent pourraient être directement incriminés.

Dans une autre affaire, les fondateurs du célèbre site de torrents *The Pirate Bay* ont dénoncé une violation de la liberté d'expression du fait de leur condamnation pour des infractions en matière de droit d'auteur, invoquant le libre échange d'informations comme incluant également des contenus protégés par le droit d'auteur, même dans un but lucratif ; bien que la Cour ait constaté que la liberté d'expression inclut effectivement ces

[24] Affaire K.U. c. Finlande, 2 décembre 2008 (requête n° 2872/02).
[25] Volodina c. Russie (n° 2), 14 septembre 2021 (requête n° 40419/19).
[26] Buturugă c. Roumanie, 11 février 2020 (requête n° 56867/15).
[27] M.Ș.D. c. Roumanie, 3 décembre 2024 (requête n° 28935/21).
[28] Affaire Delfi AS c. Estonie, 16 juin 2015 (Grande Chambre, n° 64569/09).
[29] *Ibidem.*

composantes, elle a estimé que les juridictions internes avaient correctement mis en balance ces droits avec la nécessité de protéger le droit d'auteur au moment où elles ont décidé de la condamnation, la requête ayant été rejetée comme manifestement irrecevable[30]. À l'opposé, toutefois, la Cour EDH a sanctionné à deux reprises la pratique des autorités hongroises consistant à engager la responsabilité des portails pour des commentaires publiés par des lecteurs sous des articles, qui, bien que diffamatoires, n'incitaient pas à la haine et à la discrimination[31], ou pour la simple publication d'un lien vers une vidéo YouTube au contenu diffamatoire à l'égard d'une personne[32], les violations constatées étant toutefois fondées sur le fait que les autorités n'avaient pas procédé à une analyse effective ni mis en balance les intérêts en jeu, la Cour ayant même établi, dans la seconde affaire, que la forme de responsabilité des plateformes découlant de la réglementation nationale était une responsabilité objective, qui ne permet pas une analyse *in concreto*.

S'agissant de l'article 8 de la Convention, dans l'affaire M.L. et W.W. c. Allemagne, il a été établi qu'il n'y avait pas eu de violation du droit au respect de la vie privée du fait du refus des autorités de l'État d'obliger la presse à anonymiser les archives en ligne relatives à la condamnation pénale des requérants, la mise en balance des valeurs sociales en jeu penchant en faveur du droit du public à l'information[33]. De même, la Cour a jugé qu'il n'y avait pas de violation de l'obligation positive de protéger le droit au respect de la vie privée lorsque l'État n'a pas sanctionné l'ONG propriétaire d'un blog sur lequel, dans la section des commentaires, avaient été publiés des messages anonymes diffamatoires à l'encontre d'une personne, le commentaire étant resté en ligne environ 9 jours et ayant été supprimé le lendemain du jour où la personne visée avait signalé son existence aux propriétaires du blog[34].

L'expérience d'autres États en matière de sanctions numériques

Afin de donner une base pratique à notre discussion et en l'absence de telles discussions dans le droit national, nous avons décidé d'analyser certaines solutions trouvées dans différentes juridictions à l'étranger. Bien sûr, notre analyse ne prétend pas être exhaustive et se limite aux États disposant d'un système de droit continental.

Dans la législation de la Fédération de Russie, l'interdiction d'utiliser Internet, bien qu'elle ne constitue pas une peine susceptible d'être appliquée, est une mesure qui peut être attachée aux obligations imposées dans le cadre de l'assignation à résidence[35]. L'utilisation d'Internet peut être interdite *de plano* en vertu de ces dispositions, pour autant qu'il existe une justification et une motivation raisonnables au regard du but pour lequel la mesure est ordonnée. Comme nous l'avons déjà montré, l'existence de cette disposition a même passé avec succès le contrôle de la Cour EDH, dans l'affaire Navalnyy c. Russie (n° 2). La doctrine russe a souligné l'apparition, dans la pratique, de décisions restreignant l'activité numérique d'une personne à titre de peine complémentaire, fondées sur l'article 47 du Code pénal russe, qui permet l'interdiction d'exercer certains droits, à l'instar de la peine complémentaire

[30] Affaire Neij et Sunde Kolmisoppi c. Suède, 19 février 2013 (décision d'irrecevabilité, n° 40397/12)
[31] Affaire Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt c. Hongrie, 2 février 2016 (requête n° 22947/13).
[32] Affaire Magyar Jeti Zrt c. Hongrie, 4 décembre 2018 (requête n° 11257/16).
[33] M.L. et W.W. c. Allemagne, 28 juin 2018 (requêtes n° 60798/10 et 65599/10).
[34] Pihl c. Suède, 7 février 2017 (décision d'irrecevabilité, requête n° 74742/14).
[35] Article 105.1 du Code de procédure pénale de la Fédération de Russie.

homonyme en droit roumain, prévue à l'article 66 du Code pénal, avec toutefois cette différence que ces dispositions ne précisent pas expressément quelles activités peuvent être interdites, leur formulation étant vague : « interdiction d'exercer des activités professionnelles ou toute autre activité ». Ainsi, les auteurs cités font état de deux décisions judiciaires ayant prononcé, l'une, *l'interdiction du droit de s'engager dans des activités impliquant l'utilisation d'Internet* (tribunal de Staryi Oskol, 15.10.2017) et, l'autre, *l'interdiction de la possibilité/opportunité*[36] *d'utiliser Internet* (tribunal de Khasavyurt, République du Daghestan, 22.11.2017)[37].

En Croatie, l'interdiction d'accès à Internet pour une période déterminée (de 6 mois à 2 ans) est réglementée comme mesure de sûreté (à des fins préventives), appliquée lorsque le tribunal estime qu'il existe un risque que la personne condamnée commette à nouveau une infraction en utilisant Internet à des fins malveillantes.

En Espagne, à la suite d'une décision d'espèce dans laquelle la juridiction avait étendu la portée de l'interdiction faite à une personne de se trouver dans certains lieux, en y incluant l'interdiction de se trouver dans certains « lieux » numériques, des « espaces » virtuels du cyberespace (en l'espèce, il s'agissait de la plateforme YouTube), solution critiquée comme contraire au principe de légalité et finalement annulée par l'arrêt du Tribunal suprême espagnol (*Sentencia del Tribunal Supremo*) n° 547/02.06.2022, au motif que la peine appliquée n'était pas prévue par la loi, un projet de loi a été élaboré en vue d'introduire dans la législation actuelle des peines permettant d'interdire l'accès ou la communication par le biais des réseaux sociaux, des forums ou d'autres plateformes de l'espace numérique, lorsque l'infraction est commise dans de tels espaces virtuels[38].

Une modalité de restriction des droits dans l'environnement numérique est également apparue en France à la suite de la loi n° 2024-449 du 21 mai 2024 (dite « loi SREN »), qui ne permet l'application de cette peine complémentaire qu'à des infractions spécifiquement désignées au II de l'article 131-35-1 du Code pénal français. Par souci d'exactitude et parce qu'il constitue un modèle de réglementation efficace, nous reproduisons intégralement le paragraphe I :

> « *I. - Pour les délits mentionnés au II, le tribunal peut ordonner à titre de peine complémentaire la suspension des comptes d'accès à des services en ligne ayant été utilisés pour commettre l'infraction. Le présent alinéa s'applique aux comptes d'accès aux services de plateforme en ligne définis au 4 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.*
> *La suspension est prononcée pour une durée maximale de six mois ; cette durée est portée à un an lorsque la personne est en état de récidive légale.*
> *Pendant l'exécution de la peine, il est interdit à la personne condamnée d'utiliser les comptes d'accès aux services de plateforme en ligne ayant fait l'objet de la suspension ainsi que de créer de nouveaux comptes d'accès à ces mêmes services.*

[36] Dans l'article original, c'est le terme anglais « opportunity » qui est utilisé.
[37] Pour toutes ces références, voir *V. Lapshin, S. Khokhrin*, Theoretical Justification for Conducting Research on the Issue of Restrictions on Mobile Communications and Other Means of Communication as an Alternative to Imprisonment, (DOI : 10.46741/2686-9764.2025.71.3.005), publié dans Penitentiary Science 2025, vol. 19, n° 3 (71), p. 273, disponible ici, consulté le 23 septembre 2026.
[38] À cet égard, voir l'exposé des motifs du projet de loi, disponible ici, consulté le 23 septembre 2026. D'après les vérifications effectuées, il ne semble pas que cette loi ait été adoptée au moment de la rédaction du présent article.

La décision de condamnation mentionnée au premier alinéa du présent I est signifiée aux fournisseurs de services concernés. A compter de cette signification et pour la durée d'exécution de la peine complémentaire, ces derniers procèdent au blocage des comptes faisant l'objet d'une suspension et peuvent mettre en œuvre, dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, des mesures strictement nécessaires et proportionnées permettant de procéder au blocage des autres comptes d'accès à leur service éventuellement détenus par la personne condamnée et d'empêcher la création de nouveaux comptes par la même personne.

Le fait, pour le fournisseur, de ne pas procéder au blocage des comptes faisant l'objet d'une suspension est puni de 75 000 euros d'amende.

Pour l'exécution de la peine complémentaire mentionnée au premier alinéa du présent I et par dérogation au troisième alinéa de l'article 702-1 du code de procédure pénale, la première demande de relèvement de cette peine peut être portée par la personne condamnée devant la juridiction compétente à l'expiration d'un délai de trois mois à compter de la décision initiale de condamnation ».

Nous observons donc une réglementation qui prévoit la possibilité d'une interdiction spécifique, et non générique et totale comme celles existant en Russie ou en Croatie. On remarque également la responsabilisation des opérateurs de plateformes en ligne, auxquels incombe l'obligation de veiller au blocage des comptes d'accès du condamné à leurs plateformes et d'empêcher celui-ci de créer de nouveaux comptes sur la plateforme. L'amende applicable lorsque l'opérateur ne respecte pas ces obligations est très élevée, s'élevant à 75 000 euros. Pour la personne condamnée, le non-respect de cette interdiction, comme celui des autres peines complémentaires, constitue une infraction distincte, prévue à l'article 434-41 du Code pénal français.

EN GUISE DE CONCLUSION : L'EFFICACITÉ DE LA PRIVATION DE LIBERTÉ ET DES SANCTIONS CLASSIQUES DANS LE CAS DES INFRACTIONS INFORMATIQUES. L'OPPORTUNITÉ DE SANCTIONS NUMÉRIQUES SUPPLÉMENTAIRES

Cette dernière partie part de deux observations, chacune basée sur l'un des types de cybercriminalité existants.

Premièrement, en ce qui concerne les infractions destinées à protéger l'intégrité des systèmes et des données informatiques et qui ne peuvent être commises que par leur intermédiaire ou en lien avec ceux-ci (infractions dites cyberdépendantes – *cyber-dependent crimes*), on peut soutenir l'idée que le danger social que représente l'auteur existe strictement dans le cyberespace et qu'il ne constitue pas un danger dans l'environnement physique de nature à rendre nécessaire son isolement physique de la société.

Deuxièmement, si l'on pense aux infractions qui ne sont commises qu'incidemment par l'intermédiaire de systèmes ou de données informatiques ou en lien avec ceux-ci (infractions dites cyberfacilitées – *cyber-enabled crimes*), si le *modus operandi* de l'auteur consiste à agir uniquement de cette manière et s'il n'a pas une activité infractionnelle mixte, à la fois en ligne et dans l'environnement physique, la même conclusion pourrait être tirée à son égard : le danger qu'il représente pour la société se situe exclusivement dans l'environnement en ligne.

Les choses se compliquent[39] encore davantage si l'on pense aux mineurs qui développent des compétences techniques exceptionnelles dès leur plus jeune âge et qui parviennent à pénétrer des systèmes informatiques extrêmement bien protégés, avant d'avoir une boussole morale suffisamment développée pour distinguer le bien du mal[40]. Au regard de l'âge de la responsabilité pénale, toute discussion est inutile avant l'âge de 14 ans, compte tenu de la présomption absolue d'absence de discernement. Après 14 ans, en revanche, nous estimons qu'il faut faire preuve de prudence dans le cas des mineurs qui commettent des infractions informatiques complexes (qu'il s'agisse de la présomption relative d'absence de discernement avant l'âge de 16 ans ou de la présomption de son existence après cet âge), car il ne faut pas établir, de manière automatique, un lien direct et proportionnel entre le développement exceptionnel des capacités techniques d'un mineur et son développement psycho-cognitif. Ces deux formes de développement ne sont pas interdépendantes, et les mineurs peuvent exceller sur le plan technique tout en restant sous-développés sur le plan socio-moral[41].

Toutes ces observations ne sont pertinentes que dans l'hypothèse d'auteurs spécialisés, dont l'activité infractionnelle se déroule exclusivement en ligne. Nos observations ne s'appliquent qu'à eux, et non à ceux qui ont un portefeuille varié d'infractions, comprenant certes des infractions informatiques, mais aussi des infractions commises dans l'environnement physique.

Bien entendu, ces observations sont également influencées par le stéréotype, créé par le cinéma et la télévision, de la personne timide, antisociale et évitante dans l'environnement physique, mais qui est un génie de l'informatique et qui exerce (notamment) des activités plus ou moins délictueuses. Nous ne considérons pas qu'une telle personne représente une menace physique et directe nécessitant son isolement de la société dans un pénitencier, comme cela est nécessaire, par exemple, dans le cas des personnes violentes. Évidemment, un tel auteur présente une dangerosité sociale qui peut être élevée, mais les valeurs sociales qu'il met en danger de manière abstraite – l'intégrité des systèmes et des données informatiques – pourraient, du moins sur le plan théorique, être protégées autrement que par la privation de liberté de l'auteur. Pour atteindre le but des peines, à savoir la défense de la société par la prévention de la commission de nouvelles infractions, il est fait appel aux fonctions de contrainte, de rééducation, d'exemplarité et d'élimination des peines[42]. Or, dans le cas des infractions informatiques et des auteurs spécialisés que nous avons envisagés, la fonction d'élimination du milieu social physique ne sert pas le but préventif lorsque la personne condamnée n'est pas encline à commettre des infractions en dehors de l'environnement numérique, son élimination de l'environnement en ligne pouvant en revanche s'avérer nécessaire. C'est précisément pour cette raison qu'il nous paraît opportun, *de lege ferenda*, de prévoir, pour les infractions informatiques, la peine d'amende à titre

[39] La complication n'est pas seulement théorique, la pratique connaissant de multiples difficultés sur le plan probatoire, même lorsqu'il s'agit uniquement de l'évaluation du discernement. Pour une analyse en ce sens, voir *Ș.-I. Sorohan, Provocările administrării probatoriului pentru răspunderea penală a minorilor,* dans AUBD – Forum juridic n° 2/2023, disponible ici.

[40] Pour une approche *de lege ferenda* qui propose que, même dans le cas des jeunes âgés de plus de 18 ans insuffisamment développés sur le plan moral, des mesures éducatives spécifiques aux mineurs puissent également être ordonnées, voir *G.-C. Ioan*, Sancționarea faptelor comise de minori. Spre un model european, Éd. Hamangiu, Bucarest, 2025, p. 263 et s.

[41] D'ailleurs, dans certains contextes, on peut en dire autant des adultes.

[42] *L.V. Lefterache*, op. cit., p. 297.

alternatif à la peine d'emprisonnement, et d'instituer parallèlement de nouvelles peines complémentaires visant des interdictions propres à l'environnement numérique, inspirées ou non des solutions législatives existant dans d'autres États, mais dans le respect des limites inhérentes imposées par les droits et libertés fondamentaux de l'homme, tels qu'ils ont été développés dans la jurisprudence de la Cour EDH.