DOI: https://www.doi.org/10.31178/AUBD-FJ.2025.1.13

Forum Juridic nr. 1 / 2025

ANALELE UNIVERSITĂȚII DIN BUCUREȘTI - SERIA DREPT

La prévisibilité de l'incrimination des actes commis dans le cyber espace

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

Résumé: *L'article analyse la prévisibilité de l'incrimination des actes commis dans le cyber espace par deux perspectives : par les règles de la partie générale du Code pénal roumain et par les règles établies pour protéger les droits de l'hommes. Dans la première partie, on discute les classifications des infractions pénales par l'élément matériel, on souligne les particularités pour le cyber espace, et après on présente les règles établies dans la jurisprudence de la Cour européenne des droits de l'homme pour l'article 7 de la Convention. Dans la seconde partie, on présente les modalités d'interprétation qui peuvent créer des problèmes dans la jurisprudence et on analyse les disputes qu'ont été réglées par la jurisprudence obligatoire de la Haute Cour de Cassation et de Justice. La conclusion à laquelle on est arrivé est que on doit toujours partir de la prémisse de l'existence d'une interaction inédite entre des institutions de droit traditionnelles, créées et façonnées depuis des dizaines voire des centaines d'années sur lesquelles fonctionne le droit pénal, et ce domaine relativement nouveau du cyber espace.*

Mots-clés: *cyber espace, infraction pénale, prévisibilité, interprétation, élément matériel, droits de l'homme.*

Previzibilitatea incriminării conduitelor comise în cyberspațiu

Rezumat: *Articolul analizează previzibilitatea incriminării actelor comise în cyberspațiu din două perspective: regulile părții generale a dreptului penal român și regulile stabilite pentru protejarea drepturilor omului. În prima parte, este discutată clasificarea infracțiunilor în funcție de elementul material, sunt subliniate particularitățile pentru cyberspațiu și apoi sunt prezentate regulile stabilite în jurisprudența Curții Europene a Drepturilor Omului în aplicarea articolului 7 din Convenție. În a doua parte, sunt prezentate modalitățile de interpretare care pot crea probleme în practica judiciară și se analizează disputele rezolvate prin jurisprudența obligatorie a Înaltei Curți de Casație și Justiție. Concluzia la care se ajunge este că trebuie să pornim întotdeauna de la premisa existenței unei interacțiuni inedite între instituțiile juridice tradiționale, create și modelate de-a lungul zecilor sau chiar sutelor de ani, pe baza cărora funcționează dreptul penal, și acest domeniu relativ nou al cyberspațiului.*

Cuvinte-cheie: *cyberspațiu, infracțiune, previzibilitate, interpretare, element material, drepturile omului.*

The predictability of the incrimination of the conducts committed in cyberspace

Abstract: *The article analyzes the predictability of the incrimination of acts committed in cyberspace from two perspectives: through the rules of the general part of Romanian criminal law and through the rules established to protect human rights. In the first part, we discuss the classification of offenses by their material element, highlights the particularities for cyberspace, and then presents the rules established in the jurisprudence of the European Court of Human Rights on article 7 of the Convention. In the second part, it presents the modalities of interpretation that can create problems in jurisprudence and analyzes the disputes resolved by the mandatory jurisprudence of the High Court of Cassation and Justice. The conclusion reached is that one must always start from the premise of an unprecedented interaction between traditional legal institutions, created and shaped over decades or even centuries on which criminal law operates, and this relatively new domain of cyberspace.*

Keywords: *cyberspace, criminal offence, predictability, interpretation, verbum regens, human rights.*

INTRODUCTION

Le droit pénal est créé par les normes d'incrimination prévues dans la Partie spéciale du Code pénal ou dans des lois spéciales, dans le cadre et les limites établies par la Partie générale du Code pénal. Ces affirmations décrivent le caractère unitaire du droit pénal[1].

L'existence de plusieurs catégories d'infractions n'affecte pas ces règles. Bien que certaines normes ou groupes de normes d'incrimination puissent avoir une spécificité imposée par l'objet juridique des infractions, elles devraient s'inscrire dans les mêmes schémas.

Les infractions informatiques et les infractions commises digitalement ne font pas exception. Dans un travail antérieur, nous avons défini ces concepts afin de faciliter l'analyse des infractions commises dans le cyber espace. Ainsi, nous avons montré que les infractions informatiques stricto sensu sont celles dont l'objet juridique protège principalement ou secondairement l'intégrité des systèmes informatiques ou des données informatiques, ainsi que celles pour lesquelles l'utilisation de tels systèmes est nécessaire pour réaliser le contenu constitutif de l'infraction. À l'inverse, les infractions commises digitalement sont celles dont l'essence ne réside pas dans l'utilisation d'un système informatique, pouvant être commises dans la réalité matérielle, mais qui ont été réalisées via un système informatique dans une situation donnée[2]. Nous attirons l'attention sur ces termes car ils seront très utiles dans notre démarche actuelle, où nous nous proposons d'analyser la prévisibilité des normes d'incrimination pour les actes commis dans le cyber espace. Dès à présent, nous

[1] Pour plus de détails sur le caractère unitaire, voir L.V. Lefterache, *Droit pénal. Partie générale*, 4e edition (Drept penal. Partea generală, Ediția a 4-a), Ed. Hamangiu, Bucarest, 2024, p. 14-15.

[2] *D. Herinean*, Les défis de la criminalité numérique pour le droit pénal. Le droit pénal dans la lutte contre la criminalité en ligne (Provocările criminalității digitale pentru dreptul penal. Dreptul penal în combaterea infracționalității în mediul online), dans la Revue Roumaine de Droit des Affaires (Revista Româna de Drept al Afacerilor) n° 3/2023.

précisons que ce problème doit être envisagé sous deux perspectives différentes selon les types d'infractions : infractions informatiques ou infractions commises digitalement.

Partie I. LA PRÉVISIBILITÉ APPARENTE DES NORMES D'INCRIMINATION EN MATIÈRE D'INFRACTIONS COMMISES DANS LE CYBER ESPACE

Le premier pas pour vérifier la prévisibilité doit partir de la fondation de toute relation juridique en droit pénal : la loi et les normes d'incrimination proprement dites. Pour cette raison, on commence par analyser les modalités selon lesquelles les actes de conduite peuvent être réglementés dans l'environnement en ligne, en discutant du caractère spécifique du cyber espace quand il apparaît. Ensuite, on passe en revue les règles établis de la jurisprudence de la Cour Européenne des Droits de L'homme concernant la réglementation des actes de conduite pour les infractions pénales.

A. L'acte de conduite - élément matériel et normes d'incrimination

L'élément matériel ou *verbum regens* est peut-être la condition la plus importante du contenu constitutif de l'infraction car il décrit précisément l'acte interdit au destinataire de la norme pénale. C'est pourquoi toute analyse comme celle que nous entreprenons doit partir de l'élément matériel.

Il faut premièrement mentionner les conditions attachées à l'élément matériel, qui bien qu'elles ne décrivent pas une action/inaction et ne constituent donc pas un *verbum regens* à proprement parler, complètent les détails nécessaires à la réalisation de l'élément matériel dans le cas de certaines infractions. Ces conditions attachées à l'élément matériel ne seront qualifiées comme telles que lorsqu'elles ne peuvent pas être intégrées dans les autres éléments du contenu juridique de l'infraction. Ainsi, l'objet matériel ne sera pas une condition attachée à l'élément matériel, pas plus que le lieu, le temps ou la situation prémisse, ceux-ci étant des conditions distinctes. Par exemple, une telle condition se retrouve dans l'art. 250 alin. (1) C.pén., où il est mentionné que l'exécution de l'opération financière doit être faite « sans le consentement du titulaire ».

1. Infractions de commission et infractions d'omission

La classification la plus courante concernant l'élément matériel distingue entre infractions de commission et d'omission selon que le *verbum regens* prévoit une action ou une omission.

Les infractions de commission. La règle en matière de normes d'incrimination concerne principalement *les infractions de commission*, qui soulèvent peu de difficultés dans leur application. En analysant les infractions prévues par la législation actuelle en Roumanie ayant pour objet juridique principal ou secondaire le bon fonctionnement des systèmes informatiques ou des données informatiques, on constate qu'il s'agit exclusivement d'infractions de commission. Dans cette perspective, nous verrons ci-après qu'est pertinente dans le contexte de ces infractions la classification suivante: celle des infractions sous forme fermée et des infractions sous forme libre.

Les infractions d'omission propres. Ces infractions se caractérisent par la stipulation d'une inaction dans le *verbum regens*, établissant ainsi une obligation d'agir directement

dans la norme d'incrimination. L'inaction ne doit pas toujours être perçue comme une passivité totale: une infraction commise par omission peut exister même si l'auteur a adopté un comportement actif[3], qui dénote toutefois son maintien dans la passivité par rapport à l'obligation établie. Dans le cas de ces normes, il est souvent nécessaire de réglementer également un délai jusqu'auquel la personne est tenue d'adopter le comportement contraire. Ce délai peut être très court, comme « immédiatement » dans le cas des infractions de non-assistance ou de non-dénonciation, ou plus long, comme celui de 10 jours pour l'infraction d'appropriation d'un bien trouvé ou reçu par erreur (infraction qui peut également être commise digitalement – en cas de refus de restitution d'une somme d'argent reçue par erreur sur un compte bancaire).

En analysant les normes d'incrimination existantes dans la législation actuelle de Roumanie, nous constatons qu'il n'existe pas d'infractions informatiques réglementées en tant qu'infractions d'omission propres. Par ailleurs, même dans les modèles internationaux, on ne trouve pas de recommandations d'incrimination en tant qu'infractions d'omission propres.

De notre point de vue, la discussion pourrait devenir utile dans l'hypothèse où un changement de paradigme aurait lieu et où certaines obligations seraient créées pour les détenteurs de plateformes de réseaux sociaux / sites web en matière de prévention ou de lutte contre les comportements illicites dans l'environnement en ligne. À cet égard, pour ces comportements graves nécessitant l'intervention du droit pénal, des normes d'incrimination d'omission propres pourraient être créées afin de réglementer strictement les comportements que doivent adopter les détenteurs de ces plateformes pour prévenir la commission d'infractions.

Les infractions «d'omission par omission». Ces infractions, également appelées infractions d'omission impropres, supposent la stipulation d'une action dans le *verbum regens*. Cependant, en raison de l'existence d'une position de garant, l'auteur peut commettre l'infraction concernée y compris par omission. Toutes les infractions ne peuvent pas être commises de cette manière, étant nécessaire, conformément à l'article 17 du Code pénal, qu'il s'agisse d'infractions de résultat. En outre, la doctrine a justement indiqué qu'il doit s'agir d'infractions en forme libre[4].

La position de garant d'une personne peut découler des trois hypothèses expressément prévues à l'art. 17 C.pén. :

- L'existence d'une obligation légale d'agir;
- L'existence d'une obligation contractuelle d'agir;
- La création d'un état de danger facilitant la production du résultat par l'auteur de l'omission, par un comportement antérieur (action ou inaction), indépendamment de la forme de culpabilité avec laquelle l'auteur a créé cet état de danger.

Nous constatons donc que la position de garant peut apparaître très facilement, y compris dans l'environnement en ligne, soit par l'établissement des obligations légales, soit par celui des obligations contractuelles. Par ailleurs, le troisième cas ne doit pas non plus être exclu *de plano*, car il peut exister des situations où l'action/l'inaction d'une personne crée un état de danger important pour l'intégrité d'un système informatique ou des données

[3] F. Streteanu, D. Nițu, *Droit pénal. Partie générale*. (*Drept penal. Partea generală),* volume *I,* Ed. Universul Juridic, București, 2014, p. 283.
[4] F. Streteanu, D. Nițu, *op. cit.*, p. 282. Pour une analyse de la notion, voir infra, point 2.

informatiques, facilitant ainsi la réalisation d'un résultat, tel que celui prévu à l'art. 249 C.pén. pour l'infraction de fraude informatique, à savoir la production d'un préjudice.

Dans le contexte de la position de garant, son identification ne produit pas d'effets prédéterminés sur une forme de culpabilité. Par conséquent, surtout dans le cas de la création d'un état de danger, il est crucial d'établir la forme de culpabilité avec laquelle la personne se rapporte à l'existence de cet état. Nous avons démontré que la forme de culpabilité à la base de la génération du danger n'est pas pertinente, mais qu'elle l'est pleinement pour l'omission ultérieure. Ainsi, si la personne ne réalise pas que cet état de danger a été créé, nous pourrons discuter au plus d'une faute sans prévision par rapport à son omission.

De plus, si la personne ne devait pas (condition objective) ou ne pouvait pas (condition subjective) prévoir qu'elle a généré un état de danger, nous constaterons l'absence de culpabilité par rapport au résultat produit, même si un fait prévu par le droit pénal, un fait d'omission, sera commise. Ces observations s'imposent dans un contexte où, en discutant des cyberattaques complexes, il est possible que les auteurs ne prévoient pas toute la réaction en chaîne qu'elles génèrent.

Toutefois, si nous discutons de la création intentionnelle d'un état de danger, nous estimons que pour toute conséquence future, l'auteur agit avec une intention indirecte, surtout s'il ne prend pas certaines mesures de précaution. Ainsi, l'implication dans des activités particulièrement dangereuses via des systèmes informatiques – par exemple, une cyberattaque contre des infrastructures critiques – peut générer un paradigme similaire, celui de l'intention indirecte par rapport à toute conséquence possible, car en effet l'auteur/les auteurs agiraient avec indifférence et compteraient uniquement sur le hasard que les résultats non recherchés ne se produisent pas.

Les infractions « d'omission par commission ». Comme nous l'avons montré *de lege lata*, il n'existe pas des infractions informatiques d'omission propres dans la législation actuelle, la discussion ne peut donc être menée qu'au niveau théorique. Cependant, nous estimons cette démarche utile à notre analyse. En ce sens, nous soulignons qu'il existe des opinions selon lesquelles, dans le cas des infractions d'omission, l'inaction pourrait être accomplie par une action, ce qui générerait une infraction « d'omission par commission»[5]. Dans ces situations, l'action ne semble pas pertinente, mais plutôt l'inaction corrélative. Étant une question controversée en doctrine[6], nous exprimons également notre opinion selon laquelle, d'un point de vue théorique, une telle construction ne peut exister que lorsque la réalisation d'une action impliquerait automatiquement – d'une certaine perspective (logique, physique ou juridique) – l'omission prévue par la norme d'incrimination. Cependant, nous estimons que même dans ces cas, l'accent devrait être mis sur l'inaction réalisée plutôt que sur l'action qui l'a générée. Bien sûr, nous ne contestons pas qu'il puisse être utile de décrire l'action pour prouver une inaction de l'auteur, cette dernière étant toutefois déterminante pour la description des faits commis. L'importance de la discussion réside dans les possibilités d'invoquer une certaine cause susceptible d'éliminer le caractère pénal des faits (par exemple l'état de nécessité, la contrainte physique) ou des

[5] C. Bulai, *Manuel de droit pénal. Partie générale. (Manual de drept penal. Partea generală),* Ed. All Educațional S.A., Bucarest, 1997, p. 425.
[6] I. Nedelcu, L.V. Lefterache dans G. Bodoroncea, V. Cioclei, I. Kuglay, L.V. Lefterache, T. Manea, I. Nedelcu, F.-M. Vasile, G. Zlati, *Code pénal. Commentaire par articles*, 3e édition. (*Codul penal. Comentariu pe articole Ediția a 3-a),* Ed. C.H.Beck, Bucarest, 2021, p. 92.

circonstances atténuantes (telles que la provocation), dont les conditions seront analysées différemment selon qu'on discute d'une seule action, de deux actions ou d'une action et d'une omission. De plus, la question peut également présenter un intérêt dans les hypothèses où pourrait se poser le problème de la reconnaissance d'un concours idéal ou d'un concours réel entre les infractions concernées.

2. Infractions en forme fermée et Infractions en forme libre

Cette classification est particulièrement importante pour notre analyse et se base sur la manière dont l'action est établie dans la norme d'incrimination. Nous parlons d'actions car, dans le cas des infractions d'omission, celles-ci seront toujours en forme libre.

Les infractions en forme fermée décrivent avec une certaine précision une forme spécifique que l'action typique doit prendre[7], limitant ainsi les modalités de violation des valeurs sociales protégées. À l'opposé, les infractions en forme libre réglementent l'action par un lien direct avec la production du résultat visé (qui peut ou non, être la conséquence immédiate de l'infraction), celles-ci pouvant être commises par toute modalité permettant d'aboutir à un tel résultat.

Pour prendre deux exemples concrets dans le domaine des infractions numériques, nous parlons d'une infraction en forme fermée dans le cas de l'infraction d'effectuer des opérations financières de manière frauduleuse [8] et d'une infraction en forme ouverte dans le cas du transfert non autorisé de données informatiques[9].

Une infraction très intéressante de ce point de vue est celle de perturbation du fonctionnement des systèmes informatiques, réglementée à l'art. 363 C.pén., que, bien qu'elle commence comme une infraction en forme libre, l'élément matériel est ensuite fermé par une énumération concrète des modalités par lesquelles on peut arriver à ce résultat :

Le fait de perturber gravement, sans droit, le fonctionnement d'un système informatique (jusqu'ici, cela sonnerait comme une forme libre, mais ensuite viennent les explicitations : - notre soulignement, D.H.) par l'introduction, la transmission, la modification, l'effacement ou la détérioration des données informatiques ou par la restriction de l'accès aux données informatiques, est puni d'un emprisonnement de 2 à 7 ans.

De notre point de vue, cette classification revêt une importance majeure en ce qui concerne la prévisibilité des normes d'incrimination lorsque nous discutons des infractions commises dans l'environnement numérique, car elle met en question précisément la clarté

[7] F. Streteanu, D. Nițu, *op. cit.*, p. 282.

[8] Art. 250 C.pen.: « L'exécution d'une opération de retrait d'espèces, de chargement ou de déchargement d'un instrument de monnaie électronique, ou de transfert de fonds, de valeur monétaire ou de monnaie virtuelle, par l'utilisation, sans le consentement du titulaire, d'un instrument de paiement sans numéraire ou des données d'identification permettant son utilisation, est punie d'une peine d'emprisonnement de 2 à 7 ans. (*„Efectuarea unei operaţiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, valoare monetară sau monedă virtuală, prin utilizarea, fără consimţământul titularului, a unui instrument de plată fără numerar sau a datelor de identificare care permit utilizarea acestuia, se pedepseşte cu închisoarea de la 2 la 7 ani*”).

[9] Art. 364 C.pen.: « Le transfert non autorisé de données d' un système informatique ou d'un système de stockage de données informatiques est puni d'une peine d'emprisonnement de 1 à 5 ans. » (*„Transferul neautorizat de date dintr-un sistem informatic sau dintr-un mijloc de stocare a datelor informatice se pedepseşte cu închisoarea de la unu la 5 ani*”).

de la loi et les possibilités pour le destinataire des normes d'incrimination de comprendre exactement quelles conduites il est autorisé ou non à entreprendre.

D'une part, les infractions en forme libre semblent offrir un degré plus élevé de protection des valeurs sociales protégées, car elles ne créent pas le risque que certaines conduites échappent à l'attention du législateur au moment de l'adoption de la norme. Les infractions en forme fermée, prévoyant des actions concrètes, créent précisément ce risque et peuvent ainsi conduire à une protection moindre d'une valeur sociale ou à la nécessité d'adopter un plus grand nombre de normes d'incrimination pour couvrir toutes les hypothèses.

D'autre part, les normes en forme libre peuvent générer des problèmes de prévisibilité, car elles mettent à la charge de leur destinataire la vigilance d'identifier les conduites qu'il ne peut pas adopter s'il souhaite ne pas léser l'objet juridique. De plus, les normes en forme libre peuvent conduire à des concours de qualifications et parfois à une pénalisation excessive de certaines conduites, lorsque les normes en forme libre sont réglementées sur différentes couches de protection. Nous mentionnons dès à présent que, de notre point de vue, les infractions informatiques réglementées aux articles 360-366 C.pén., bien qu'elles ne soient pas toutes en forme libre, créent précisément un tel système dans lequel la plupart des phénomènes de criminalité informatique relativement classiques seront qualifiés, en règle générale, comme un concours entre au moins deux de ces infractions.

3. Élément matériel unique et élément matériel alternatif

Une autre classification pertinente est celle entre les infractions ayant un élément matériel unique (qu'il s'agisse d'infractions en forme libre ou en forme fermée) et les infractions ayant plusieurs variantes de commission de l'élément matériel. Dans le contexte des infractions informatiques, il faut noter que plusieurs d'entre elles ont un élément matériel alternatif, pouvant être commises de plusieurs manières. Par exemple, les infractions prévues aux articles 360 C.pén., 361 C.pén., 364 C.pén. sont des infractions à élément matériel unique (accès / interception / transfert), tandis que d'autres ont un élément matériel avec des variantes alternatives de commission : l'article 362 C.pén. incrimine « *Le fait de modifier, effacer ou détériorer des données informatiques ou de restreindre l'accès à ces données, sans droit* », l'article 363 C.pén. « *Le fait de perturber gravement, sans droit, le fonctionnement d'un système informatique, par l'introduction, la transmission, la modification, l'effacement ou la détérioration des données informatiques ou par la restriction de l'accès aux données informatiques* ». De même, selon l'article 249 C.pén., la fraude informatique suppose « *L'introduction, la transmission, la modification ou l'effacement de données informatiques, la restriction de l'accès à ces données ou l'entrave de quelque manière que ce soit au fonctionnement d'un système informatique* », et l'article 250 C.pén. « *L'exécution d'une opération de retrait d'espèces, de chargement ou de déchargement d'un instrument de monnaie électronique ou de transfert de fonds, de valeur monétaire ou de monnaie virtuelle, par l'utilisation, sans le consentement du titulaire, d'un instrument de paiement sans numéraire ou des données d'identification permettant son utilisation* ». Dans tous ces exemples, nous parlons d'infractions à contenu alternatif, ce que détermine la rétention d'une seule infraction, commise dans une unité naturelle collective, dans le cas où plusieurs variantes de l'élément matériel sont commises dans la même

circonstance en relation avec le même sujet passif. De plus, dans le cas des infractions continues, il est possible de retenir l'accomplissement de la condition d'homogénéité juridique des actions réalisées à différents intervalles de temps, même si différentes variantes de l'élément matériel sont commises, tant que l'unité de résolution infractionnelle peut subsister.

4. Une classification spécifique au cyber espace?

Dans cette perspective, nous envisageons une classification de l'élément matériel en fonction de la manière dont il se rapporte au cyber espace. Ainsi, nous pouvons parler de conduites que ne peuvent pas être réalisées que dans le cyber espace, comme c'est le cas des infractions informatiques *stricto sensu* ; de conduites qui peuvent être réalisées à la fois dans le cyber espace et dans l'environnement physique (infractions commises de manière numérique) ; d'actes de conduite incompatibles avec leur réalisation dans le cyber espace.

Nous ajouterons également une autre classification, basée sur la spécificité des infractions commises dans le cyber espace, où, au moins en apparence, l'élément matériel peut décrire deux types d'actions :

- L'action directe, physique, que l'auteur réalise dans le monde matériel ; par exemple, l'accès illégal à un système informatique (« *l'accès, sans droit, à un système informatique* ») ;
- L'action médiatisée, qui décrit la conduite réalisée par l'intermédiaire de l'interface graphique/logique du système informatique, c'est-à-dire l'action dans le cyber espace et non dans le monde matériel ; par exemple, l'infraction de transfert non autorisé de données informatiques (« *le transfert non autorisé de données d'un système informatique ou d'un moyen de stockage* »).

On pourrait soutenir que même dans le premier cas, l'accès se réalise toujours par une interaction logique avec le système informatique (accès au logiciel), ce qui est vrai, mais il semble que l'accent soit mis sur l'action antérieure ou tout au plus concomitante à l'interaction avec l'interface graphique. Il est peut-être évident, mais nous ne parlons pas d'un accès à un système informatique si, par exemple, nous démontons les parties d'un ordinateur portable (matériel) sans l'allumer et interagir également avec ses programmes.

Dans l'autre exemple, le transfert de données d'un système informatique ne peut se faire qu'après l'accès. Nous pensons que ces affirmations peuvent être très utiles, y compris pour l'analyse et la différenciation du concours d'infractions du concours de qualifications, lorsqu'il faut vérifier si pour une certaine conduite seront retenues une seule ou plusieurs des normes d'incrimination qui semblent être incidentes en apparence.

Laquelle de ces types de description de l'acte de conduite est plus compatible avec les exigences de prévisibilité ? Nous ne pensons pas que l'une ou l'autre soulève ab initio des problèmes majeurs liés à la clarté et à la prévisibilité de la norme, mais des problèmes de prévisibilité peuvent apparaître, comme nous le disions, dans la manière dont plusieurs normes sont appliquées et dans la manière dont la qualification du fait en une ou plusieurs infractions est établie.

B. Points saillants de la jurisprudence de la Cour européenne des droits de l'homme concernant la création et l'application des normes d'incrimination

Suite à l'analyse de l'acte de conduite et des modalités selon lesquelles il peut être réglementé, nous nous proposons de passer en revue quelques-uns des repères issus de la jurisprudence de la Cour européenne des droits de l'homme concernant la clarté et la prévisibilité des normes d'incrimination, en ajoutant nos propres observations dans chaque cas. Nous diviserons cette discussion en modalité de réglementation et modalité d'application des normes d'incrimination.

Une première observation qui doit encore être faite à ce stade est que, en ce qui concerne les infractions commises dans le cyber espace, nous considérons qu'aucune règle spéciale n'a été développée dans la Convention européenne des droits de l'homme, n'existant pas de différenciations ni liées au droit matériel, ni liées au droit procédural pour cette catégorie d'infractions[10]. Par conséquent, nous suivrons les repères généraux, en mentionnant leur spécificité en ce qui concerne notre analyse.

1. Le principe de légalité – *lex scripta*

Au niveau interne, conformément au principe de légalité, les infractions et les peines doivent être expressément prévues par la loi, une condition sine qua non dans notre système juridique étant la *lex scripta*[11], c'est-à-dire leur inscription écrite dans une norme réglementaire, les règles des systèmes juridiques coutumiers ne pouvant pas être appliquées. L'applicabilité du principe de légalité ne se limite pas aux normes d'incrimination et aux peines, mais concerne toute mesure de restriction de l'exercice de certains droits[12]. Étant donné que les infractions ne peuvent être réglementées que par des lois organiques, il n'est pas permis à des entités privées ou non étatiques de déterminer les éléments essentiels d'une infraction. Cette affirmation est importante dans le contexte où, dans le cyber espace, il peut exister des acteurs très influents ayant une implication majeure dans la découverte et le signalement de certaines conduites, comme les détenteurs de plateformes de réseaux sociaux ou ceux qui gèrent des mondes virtuels en ligne. Les intérêts privés – toutes ces entreprises étant fondées sur un tel intérêt, principalement orienté vers la réalisation d'un profit – ne peuvent constituer la base de l'établissement de normes ayant un caractère pénal. Enfin, il convient toujours d'agir avec précaution lorsqu'il s'agit d'élargir le champ d'application du droit pénal, car, comme cela a été indiqué dans la doctrine, « *l'absolutisation de l'arme pénale est une erreur fondamentale* »[13].

[10] Dans le même sens, en lien avec les infractions économiques, voir *D. Pârgaru*, Limites procédurales en matière de droits de l'homme dans les enquêtes sur les crimes économiques, dans AUBD – Forum juridic n° 2/2023, p. 147.
[11] *F. Streteanu, D. Nițu,* op. cit., p. 37-38.
[12] *L.V. Lefterache*, op. cit. p. 44.
[13] *C.-L. Popescu*, La réincrimination par voie jurisprudentielle constitutionnelle de l'insulte et de la calomnie, (Reincriminarea pe cale jurisprudențială constituțională a insultei și calomniei), publie dans le Nouvelle Revue des Droits de l'Homme (Noua Revistă de Drepturile Omului) n° 1/2007, p. 7, consulte sur ceeol.com.

2. La possibilité te de connaître le contenu d'une norme d'incrimination – la clarté de la loi

L'article 7 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales crée un droit en matière pénale concernant, entre autres, la possibilité pour une personne de connaître le contenu d'une norme d'incrimination au moment de la commission de l'infraction afin qu'elle puisse être tenue pénalement responsable, avec des exigences qualitatives de la loi, telles que l'accessibilité et la prévisibilité, tant en ce qui concerne la législation que la pratique judiciaire[14]. En outre, ces mêmes exigences s'appliquent également au niveau infra-législatif de réglementation, comme cela a été établi dans une décision concernant un règlement d'organisation et de fonctionnement d'un établissement pénitentiaire[15]. Du point de vue de la qualité des lois, les exigences d'accessibilité et de prévisibilité s'imposent dans la définition des infractions prévues par le droit interne[16], et une définition insuffisamment qualitative de l'infraction ou une prédéfinition faible de la peine peuvent constituer des violations de l'article 7 de la Convention EDH[17]. L'accessibilité est réalisée de manière suffisante lorsque la loi est publiée. Par conséquent, l'accessibilité de la loi ne soulève pas raisonnablement des grandes difficultés. Les discussions peuvent toutefois porter sur la manière dont la jurisprudence applique une loi.

Comme les lois impliquent intrinsèquement un certain degré d'abstraction, leur formulation ne peut pas être extrêmement précise dans tous les cas, de sorte que leur champ d'application soit excessivement restreint et qu'un très grand nombre de normes d'incrimination soient nécessaires. À cet égard, il a été établi que l'interprétation et l'application des lois peuvent dépendre de la pratique judiciaire[18], mais aussi que l'utilisation de notions trop vagues ou de critères de délimitation pour l'interprétation qui sont équivoques peut conduire à ne pas respecter le standard de clarté et de prévisibilité imposé par la Convention[19]. Cependant, si dans la plupart des cas la loi s'avère suffisamment claire, il n'y aura pas de violation de la Convention même si la technique législative laisse certaines zones d'incertitude quant à l'applicabilité d'une notion[20].

3. La clarification de la loi dans la jurisprudence

En outre, la Cour a établi que l'apport de clarifications à des normes d'incrimination par des modifications législatives ne constitue pas automatiquement une reconnaissance du caractère incertain antérieur de la norme, tant que l'interprétation en question pouvait être

[14] Del Río Prada c. Espagne, requête n° 42750/09, jugement du 21 octobre 2013 (GC), pt. 91; S.W. c. Royaume-Uni, requête n° 20166/92, jugement du 22 novembre 1995, pt. 35. G.I.E.M. S.R.L. et al. c. Italie requêtes n° 1828/06, 34163/07 et 19029/11, jugement du 28 juin février 2018 (GC), pt. 242; Cantoni c. France, requête n° 17862/91, jugement du 15 novembre 1996, pt. 29

[15] Kafkaris c. Chypre, requête n° 21906/04, jugement du 12 février 2008 (GC), pt. 145-146.

[16] Jorgic c. Allemagne, requête n° 74613/01, jugement du 12 juillet 2007, pt. 103-114.

[17] Kafkaris c. Chypre, requête n° 21906/04, jugement du 12 février 2008 (GC), pt. 150 et 152.

[18] Kokkinakis c. Grèce, requête n° 14307/88, jugement du 25 mai 1993, pt. 40, pour la notion de «prosélytisme»; Cantoni c. France, requête n° 17862/91, jugement du 15 novembre 1996, pt. 31, pour la notion de « produit médicamenteux ».

[19] Liivik c. Estonie, requête n° 12157/05, jugement du 25 juin 2009, pt. 96-104.

[20] Cantoni c. France, requête n° 17862/91, jugement du 15 novembre 1996, pt. 32.

réalisée de manière raisonnable avant les modifications[21]. Cependant, la Cour a également établi dans d'autres affaires qu'il peut y avoir une violation de l'exigence liée à la prévisibilité d'une norme d'incrimination si l'interprétation repose sur un développement jurisprudentiel ultérieur à la commission des faits[22].

Par exemple, une telle interprétation a été donnée dans notre législation par la décision RIL n° 7/2023, par laquelle il a été établi que « *L'acte de vol commis à l'aide d'un dispositif improvisé qui bloque l'activation du système de verrouillage centralisé des portes d'un véhicule, en brouillant le signal correspondant à ce système, remplit les conditions de typicité de l'infraction de vol qualifié commis à l'aide d'une fausse clé, prévue à l'article 228 alin. (1) du Code pénal en relation avec l'article 229 alin. (1) lit. d), dernière phrase du même code* ». Ainsi, la nécessité de l'intervention de la Haute Cour de Cassation et de Justice, même dans le contexte d'un début de pratique non uniforme, n'a pas conduit à considérer la norme d'incrimination comme étant imprécise ou contraire au principe de légalité. Ces cas doivent être abordés avec précaution, car la jurisprudence de la Cour a révélé qu'une décision rendue en application des dispositions imprécises peut être considérée comme une violation de l'article 7 de la Convention si des interprétations divergentes ont existé dans l'État concerné, car une jurisprudence incohérente ne permet pas aux destinataires des normes un degré suffisant de prévisibilité quant à leurs comportements[23].

De plus, dans l'affaire Khodorkovskiy et Lebedev contre Russie[24], il a été établi que bien qu'il puisse y avoir une dépénalisation *de facto* de certains actes prévus par la loi pénale lorsque l'État a laissé inappliquées des normes d'incrimination et a ainsi toléré certains comportements, la simple non-application des normes d'incrimination à d'autres personnes qui n'ont pas été poursuivies ou condamnées avant la personne concernée, ne conduit pas *de plano* à un manque de prévisibilité de la norme d'incrimination. Nous pensons que ces repères sont importants dans notre contexte.

4. La prévisibilité du lieu de commission des infractions dans l'environnement en ligne

Une autre problématique intéressante à discuter dans ce contexte est la mesure dans laquelle le lieu de commission des infractions dans l'environnement en ligne devrait être prévisible, du point de vue de l'implication juridictionnelle d'un État ou d'un autre. Si, en principe, dans l'environnement physique, le droit pénal permet, du point de vue de la territorialité, qu'une personne pratique ce que l'on appelle un *forum shopping* - choisisse le lieu où elle commet une infraction de vol ou de meurtre, nous nous demandons dans quelle mesure cela caractérise également l'environnement en ligne.

La prévisibilité du lieu de commission de l'infraction relève plutôt du droit procédural pénal que du droit matériel. Bien entendu, seuls les États ayant un lien territorial avec la commission de l'infraction pourront attirer et exercer leur compétence basée sur le principe de territorialité. À cet égard, nous faisons référence aux dispositions de l'article 8 alin. (3)-(4)

[21] Voir Georgouleas et Nestoras c. Grèce, requêtes n° 44612/13 et 45831/13, jugement du 28 mai 2020, pt. 66.
[22] Contrada c. Italie (n° 3), requête n° 66655/13, jugement du 14 avril 2015, pt. 64-76.
[23] Žaja c. Croatie, requête n° 37462/79, jugement du 4 octobre 2016, pt. 99-106.
[24] Khodorkovskiy et Lebedev c. Russie, requêtes n° 11082/06 et 13772/05, jugement du 25 juillet 2013, pt. 816-820.

du Code pénal[25], qui établissent les limites dans lesquelles une infraction est considérée comme commise sur le territoire roumain. Des dispositions similaires se retrouvent dans la Convention de Budapest[26] sur la cybercriminalité, où l'article 22 établit l'obligation pour les États signataires d'avoir juridiction sur les infractions faisant l'objet de la Convention commises sur leur territoire, sur un navire battant pavillon roumain ou sur un aéronef immatriculé en Roumanie, ainsi que conformément au principe de personnalité, si l'infraction a été commise par un citoyen roumain lorsque l'infraction est incriminée également dans l'État où elle a été commise ou lorsqu'elle a été commise dans un territoire sans juridiction. En outre, une règle concernant l'universalité du droit pénal est instituée, plus précisément celle selon laquelle l'État signataire, la Roumanie dans notre analyse, doit s'assurer qu'il a juridiction pour les actes commis en dehors de son territoire lorsqu'il refuse d'extrader un citoyen en raison de sa nationalité. Toutes ces règles sont conformes à celles établies dans la législation interne.

Dans la jurisprudence de la Cour apparaissent quelques repères qui, selon nous, tranchent ce dilemme, même s'ils se réfèrent à la situation de compétence extraterritoriale ou universelle d'un État et non à la territorialité. Plus précisément, il a été établi que l'application du droit pénal dans l'espace (du point de vue de l'universalité et de l'extraterritorialité) n'entre pas dans le champ d'application de l'article 7 de la Convention[27], mais plutôt des droits régis par l'article 6 par. 1 et l'article 5 par. 1, selon la procédure invoquée[28]. Ainsi, nous ne pensons pas que la prévisibilité du lieu de commission de l'infraction du point de vue du principe de territorialité soulève des problèmes particuliers dans ce contexte.

Partie II. LA PRÉVISIBILITÉ LIMITÉE D'APPLICATION DES NORMES D'INCRIMINATION EN MATIÈRE D'INFRACTIONS COMMISES DANS LE CYBER ESPACE

La réglementation de certaines normes d'incrimination n'est que le premier pas à accomplir conformément aux principes généraux et aux règles établies dans l'application des droits de l'homme. En dépassant cette fondation absolument nécessaire, consistant en une réglementation correcte, surgit la deuxième étape, que nous considérons comme la plus

[25] « (3) Par infraction commise sur le territoire de la Roumanie, on entend toute infraction commise sur le territoire mentionné à l'alinéa (2) ou sur un navire battant pavillon roumain ou sur un aéronef immatriculé en Roumanie.
(4) L'infraction est également considérée comme commise sur le territoire de la Roumanie lorsque, sur ce territoire, ou sur un navire battant pavillon roumain, ou sur un aéronef immatriculé en Roumanie, un acte d'exécution, d'instigation ou de complicité a été réalisé, ou lorsque le résultat de l'infraction s'y est produit, même en partie. » *[„(3) Prin infracţiune săvârşită pe teritoriul României se înţelege orice infracţiune comisă pe teritoriul arătat în alin. (2) sau pe o navă sub pavilion românesc ori pe o aeronavă înmatriculată în România.
(4) Infracţiunea se consideră săvârşită pe teritoriul României şi atunci când pe acest teritoriu ori pe o navă sub pavilion românesc sau pe o aeronavă înmatriculată în România s-a efectuat un act de executare, de instigare sau de complicitate ori s-a produs, chiar în parte, rezultatul infracţiunii.”]*

[26] Conseil de l'Europe, Convention on Cybercrime, Budapest, 23.11.2001 (rm.coe.int).

[27] Ould Dah c. France, requête n° 13113/03, décision sur la recevabilité du 17 mars 2009: *„Eu égard à ce qui précède, la Cour estime, en l'espèce, que la loi d'amnistie mauritanienne n'était pas de nature, en soi, à empêcher l'application de la loi française par les juridictions françaises saisies des faits au titre de la compétence universelle, et que la solution retenue par les juridictions françaises était fondée*”.

[28] Jorgic c. Allemagne, requête n° 74613/01, jugement du 12 juillet 2007, pt. 64-72.

importante, à savoir la manière dont ces règles sont comprises et appliquées dans la pratique judiciaire. À cet égard, nous commencerons par présenter quelques repères concernant l'interprétation et l'application des normes d'incrimination spécifiques au cyber espace, puis nous analyserons l'évolution de la jurisprudence obligatoire de la Haute Cour de Cassation et de Justice, en tirant les conclusions qui découlent tant des éléments établis que du fait que la résolution de ces problèmes était nécessaire.

A. L'interprétation judicaire de la loi et la nécessité de faire appel à des spécialistes pour comprendre les conduites incriminées dans le cyber espace

En passant à l'interprétation de la loi, nous indiquons que la loi, étant d'application générale, comporte un élément d'abstraction élevé, puisqu'elle doit pouvoir être appliquée dans le plus grand nombre de situations possible. La prévisibilité de l'interprétation judiciaire concerne également les éléments constitutifs de l'infraction[29], car ce n'est qu'en comprenant ces éléments que le destinataire de la norme peut savoir s'il s'engage ou non dans une activité criminelle.

Il a été indiqué dans la jurisprudence de la Cour européenne des droits de l'homme qu'il est permis de clarifier progressivement les normes d'incrimination par l'interprétation dans les affaires des tribunaux, tant que cette interprétation est conforme au texte de l'infraction et peut être raisonnablement prévue par les destinataires de la norme[30].

Dans la littérature de spécialité et dans la jurisprudence, plusieurs modalités d'interprétation des normes d'incrimination se sont dégagées au fil du temps[31], parmi lesquelles nous analyserons seulement deux dans le présent travail: l'interprétation par analogie et l'interprétation évolutive.

1. L'interprétation par analogie dans la jurisprudence

Bien que l'utilisation de l'analogie soit en principe interdite en droit pénal[32], et que les règles imposées par l'article 7 de la CEDH consacrent également le principe selon lequel la loi pénale ne devrait pas être appliquée de manière extensive au détriment de l'accusé, notamment par analogie[33], il est parfois possible d'utiliser l'interprétation par analogie, généralement par le biais de clauses légales d'analogie homogène établissant cette

[29] Pessino c. France, requête n° 40403/02, jugement du 10 octobre 2006, pt. 35-36; Dragotoniu et Militaru-Pidhorni c. Roumanie, requêtes n° 77193/01 et 77196/01, jugement du 24 mai 2007, pt. 43-47; Dallas c. Royaume-Uni, requête n° 38395/12, jugement du 13 juin 2012, pt. 72-77.

[30] Voir, par exemple, S.W. c. Royaume-Uni, requête n° 20166/92, jugement du 22 novembre 1995; Streletz, Kessler et Krenz c. Allemagne, requêtes n° 34044/96, 35532/97 et 44801/98, jugement du 22 mars 2001 etc.

[31] Voir, par exemple, *L.V. Lefterache*, op. cit., p. 69 et suivantes; *C. Mitrache, Cr. Mitrache*, Droit pénale roumaine (Drept penal român), Ed. Universul Juridic, Bucharest, 2023, p. 74 et suivantes ; *F. Streteanu, D. Nițu*, op. cit., p. 49 et suivantes.

[32] En Roumanie, l'analogie a été réglementée au niveau légal entre 1949 et 1965, lorsque l'article 1, alinéa (3), introduit par le Décret n° 187/1949, stipulait que « Les actes considérés comme dangereux pour la société peuvent être punis même lorsqu'ils ne sont pas expressément prévus par la loi comme des infractions, le fondement et les limites de la responsabilité étant déterminés dans ce cas conformément aux dispositions prescrites par la loi pour des infractions similaires ». Voir *C. Mitrache, Cr. Mitrache,* op. cit., p. 47.

[33] Del Río Prada c. Espagne, requête n° 42750/09, jugement du 21 octobre 2013 (GC), pt. 78; Vasiliauskas c. Lituanie, requête n° 35343/05, jugement du 20 octobre 2015 (GC), pt. 154; Kokkinakis c. Grèce, requête n° 14307/88, jugement du 25 mai 1993, pt. 52.

possibilité au niveau législatif[34]. À l'opposé, un caractère hétérogène de la clause légale d'analogie – qui ne permet pas de définir une catégorie commune à laquelle appartiennent les normes énumérées – violerait le principe de légalité, plus précisément l'exigence de clarté qui doit caractériser les normes de droit pénal[35].

De même, la Cour européenne des droits de l'homme a établi que l'interprétation des textes légaux doit être conforme tant à la substance de l'infraction[36] qu'à son essence[37], et que la loi ne peut être appliquée de manière extensive en dépassant ces limites.

Dans la jurisprudence de la Cour européenne des droits de l'homme, d'autres limites à l'application de l'interprétation de la loi ont également été établies. Tout d'abord, dans les célèbres arrêts Pessino contre France et Dragotoniu et Militaru-Pidhorni contre Roumanie, il a été constaté une violation de l'exigence de prévisibilité lorsque l'interprétation extensive de la loi s'est fondée sur un revirement jurisprudentiel qui ne pouvait être prévu par le destinataire de la norme au moment de la commission de l'infraction, conférant ainsi un caractère rétroactif aux normes d'incrimination. Par ailleurs, comme cela a été indiqué dans la littérature de spécialité, le principe de stabilité des relations juridiques impose que les revirements jurisprudentiels soient réalisés avec soin et solidement motivés[38].

En ce qui concerne les infractions informatiques, *de lege lata*, il n'existe pas de telles clauses légales d'analogie dans le contenu constitutif des infractions, toutes les énumérations utilisées dans ces normes d'incrimination étant fermées. Ainsi, toute extension du texte des lois d'incrimination pourrait être considérée comme une analogie défavorable à l'accusé.

2. L'interprétation évolutive dans la jurisprudence

Une autre méthode d'interprétation des normes d'incrimination est celle évolutive, qui prend en compte le développement technologique imprévu au moment de l'incrimination et, même sur la base d'une interprétation téléologique, conduit à la conclusion qu'un cas particulier doit être inclus dans le champ d'application de la disposition.

La classification mentionnée ci-dessus, entre les infractions dont l'élément matériel peut être réalisé uniquement dans le cyber espace et celles où l'élément matériel peut être réalisé à la fois dans le cyber espace et dans l'environnement physique[39], peut nous être utile. Les problèmes de prévisibilité peuvent surtout être soulevés dans le deuxième cas. À cet égard, la possibilité de commettre certaines conduites dans le cyber espace peut être discutable en termes de prévisibilité si l'interprétation de la norme permettant cette

[34] *F. Streteanu, D. Nițu,* op. cit., pp. 44-45.
[35] *F. Munoz Conde. M. Garcia Aran,* Derecho penal. Parte general. Ed. Tirant lo Blanch, Valencia, 1998, p. 113 *apud F. Streteanu, D. Nițu,* op. cit., pp. 44-45.
[36] Vasiliauskas c. Lituanie, requête n° 35343/05, jugement du 20 octobre 2015 (GC), pt. 179-186.
[37] Navalnyye c. Russie, requête n° 101/15, jugement du 17 octobre 2017, pt. 68; Parmak et Bakir c. Türkiye, requêtes n° 22429/07 et 25195/07, jugement du 3 décembre 2019, pt. 76; Tristan c. République de Moldavie, requête n° 13451/15, jugement du 4 juillet 2023, pt. 67.
[38] L'auteur fait référence aux revirements réalisés dans la jurisprudence de la CEDH et de la CCR, mais nous pensons que ces affirmations pourraient également être étendues aux revirements jurisprudentiels dans les décisions de cas. Voir *C.-L. Popescu*, op. cit., p. 10.
[39] La troisième forme, celle des infractions incompatibles avec leur réalisation dans le cyberespace, ne concerne pas l'objet de notre analyse et n'a donc pas été incluse ici.

possibilité est nouvelle et n'a pas encore été appliquée aux infractions commises dans le cyber espace, et sous cet angle, l'interprétation évolutive peut devenir utile.

Un exemple à cet égard, de quoi on a déjà dit une fois, est la décision prononcée par la Haute Cour de Cassation et de Justice dans le cadre du RIL n° 7/2023, mentionnée également ci-dessus, par laquelle il a été établi que « *L'acte de vol commis à l'aide d'un dispositif improvisé qui bloque l'activation du système de verrouillage centralisé des portes d'un véhicule, en brouillant le signal correspondant à ce système, remplit les conditions de typicité de l'infraction de vol qualifié commis à l'aide d'une fausse clé, prévue à l'article 228 alin. (1) du Code pénal en relation avec l'article 229 alin. (1) lit. d), dernière phrase du même code* »[40]. La décision concerne une interprétation évolutive et téléologique d'un cas classique d'aggravation du vol qualifié, commis d'une manière distincte en raison de l'évolution technologique. Dans cette décision, la Haute Cour indique (par. 143-144) que « *par le biais de l'interprétation évolutive des réalités technologiques actuelles, dans le sens de "fausse clé", est également inclus le dispositif artisanal de type télécommande pour brouiller (ondes radio qui copient le code d'accès de la clé électronique) en bloquant le système de commande de verrouillage-déverrouillage centralisé d'une voiture, qui sécurise les portes d'un véhicule, celles-ci restant ouvertes sans que le système de verrouillage soit détruit ou endommagé, excluant ainsi de plano l'interprétation analogique visant à étendre l'application d'une norme au-delà des significations possibles des notions utilisées dans le précepte de la norme. En d'autres termes, le dispositif mentionné ci-dessus ne représente pas un autre élément circonstanciel distinct dépassant le champ d'application de l'aggravation prévue par l'article 229 alin. (1) lit. d), dernière phrase du Code pénal, "fausse clé", mais au contraire, il se subsume à sa définition telle qu'établie par la doctrine et la jurisprudence contemporaines* ».

On ne pense pas que l'interprétation évolutive constitue un obstacle à la prévisibilité des normes, mais elle doit être réalisée avec précaution afin d'éviter des analogies défavorables aux accusés.

3. La nécessite d'un spécialiste pour comprendre les conduites incriminées dans le cyber espace. L'utilisation d'Internet et la présence en ligne

En analysant la réalité quotidienne de l'utilisation d'Internet et de la présence en ligne, nous pouvons dire sur des bases empiriques que l'implication dans des activités criminelles ne peut pas se produire accidentellement et que, si vous ne souhaitez pas vous engager dans des activités dangereuses en tant qu'auteur, vous ne serez pas en danger de commettre des activités dans l'environnement en ligne. Bien sûr, dans l'hypothèse où vous travaillez dans le domaine de la cybersécurité, les choses peuvent changer, mais à ce stade,

[40] L'élément circonstanciel aggravant prévu à l'article 229, alinéa (1), lettre d), dernière phrase du Code pénal, consiste en l'utilisation sans droit d'une fausse clé. Dans le même sens, la Décision RIL n° 6/2020 a établi que « L'acte de vol commis par le retrait ou l'arrachement du système de sécurité placé sur un bien remplit les éléments de typicité de l'infraction prévue à l'article 228, alinéa (1), en relation avec l'article 229, alinéa (1), lettre e) du Code pénal », où l'élément circonstanciel aggravant prévu à l'article 229, alinéa (1), lettre e) du Code pénal consiste en la mise hors service du système d'alarme ou de surveillance. Dans ce cas, il ne s'agit pas nécessairement d'une interprétation évolutive (les systèmes de surveillance étant également des inventions technologiques relativement récentes, sans différence technologique significative entre les deux), mais plutôt d'une interprétation téléologique.

vous agissez déjà en tant que professionnel et il existe donc une obligation d'information appropriée, qui peut également être réalisée en faisant appel aux conseils de spécialistes dans le domaine du droit ou même du droit pénal. Cependant, comme cela a été indiqué dans l'affaire Pessino c. France, cette possibilité ne doit pas conduire à une conclusion claire de prévisibilité, car même pour un professionnel (M. Pessino travaillant dans le domaine de la construction) qui pouvait recevoir des conseils juridiques, il peut exister des problèmes de prévisibilité de la loi, notamment lorsqu'il s'agit d'une réorientation jurisprudentielle par exemple.

Comme nous l'avons montré précédemment, la jurisprudence est importante pour établir les limites d'application de la loi. Or, pour connaître la jurisprudence, il sera le plus souvent nécessaire de faire appel à un spécialiste, étant peu probable qu'une personne sans connaissances juridiques puisse rechercher la jurisprudence et la comprendre d'une manière raisonnable, même si celle-ci est accessible gratuitement et anonymisée pour la majorité des infractions[41]. Dans la doctrine, il a été indiqué qu'en plus de l'accessibilité de la jurisprudence, une interprétation accessible et raisonnablement prévisible des textes légaux est également nécessaire pour respecter l'article 7 de la Convention[42].

Les exigences concernant la prévisibilité de la loi ne s'opposent pas à ce que le destinataire de la norme soit tenu de recourir aux conseils d'experts pour évaluer, dans une mesure raisonnable, les conséquences pouvant découler de l'adoption d'une certaine conduite[43]. Une telle diligence peut être particulièrement requise de la part des professionnels, habitués aux exigences de prudence dans l'exercice de leur profession, et il est raisonnable d'attendre d'eux qu'ils évaluent et évitent les risques liés à leur activité professionnelle[44]. Lorsqu'il s'agit du cyber espace, il faut réfléchir à qui sont ces professionnels. Tout d'abord, les professionnels seront ceux qui travaillent dans le domaine de la cybersécurité et ceux qui développent les plateformes, applications ou programmes sur lesquels repose le fonctionnement du cyber espace. Ensuite, les professionnels incluront également ceux qui gèrent les mondes virtuels, les plateformes de médias sociaux et autres espaces numériques où des infractions peuvent être commises en ligne. De leur part, on peut donc attendre une certaine diligence pour comprendre les normes d'incrimination spécifiques ou applicables au cyber espace, surtout si à l'avenir des infractions-obstacles ou des infractions créant pour eux des rapports juridiques de conformité pour éviter la criminalité dans le cyber espace étaient réglementées. À l'opposé, nous ne pensons pas que de telles exigences pourraient être imposées à de simples utilisateurs en ligne, ceux-ci étant les clients du service, et non les professionnels qui le développent, l'utilisent où le vérifient.

Lorsqu'il s'agit de l'implication de spécialistes, un problème général qui peut survenir n'est pas seulement la connaissance de l'implication dans une activité criminelle, mais également la possibilité de prévoir toutes ses conséquences – y compris le type et le nombre d'infractions qui seraient commises. Ainsi, du point de vue de la législation interne, une

[41] Ces affirmations prouvent le respect des standards établis dans l'affaire Kokkinakis c. Grèce, requête n° 14307/88, jugement du 25 mai 1993, pt. 40.
[42] *M. Udroiu, O. Predescu*, La protection européenne des droits de l'homme et la procédure pénale roumaine (Protecția europeană a drepturilor omului și procesul penal român), Ed. C.H. Beck, Bucarest, 2008, p. 161.
[43] Tolstoy Miloslavsky c. Royaume-Uni de Grande-Bretagne, requête n° 18139/91, jugement du 13 juillet 1995, pt. 37; Vasiliauskas c. Lituanie, requête n° 35343/05, jugement du 20 octobre 2015 (GC), pt. 157.
[44] Dragotoniu et Militaru-Pidhorni c. Roumanie, requêtes n° 77193/01 et 77196/01, jugement du 24 mai 2007, pt. 35.

discussion possible concerne l'apparente sur-réglementation des infractions informatiques ou de celles commises digitalement, qui génère un concours de qualifications dans une grande partie de la pratique judiciaire.

4. La qualification juridique des infractions pénales dans le cyber espace – une multitude de possibilités

Nous nous demandons donc dans quelle mesure il est réellement prévisible pour une personne la manière de déterminer la qualification juridique dans le cas d'actes relativement similaires. Pour prendre un exemple, une personne qui vole un billet de 100 lei avec lequel elle achète ensuite des biens, commettra une infraction de vol (punie d'une peine d'emprisonnement de 6 mois à 3 ans ou d'une amende), le fait de dépenser l'argent n'ayant pas une valeur criminelle distincte.

En revanche, selon l'orientation actuelle de la pratique, si cette même personne vole une carte bancaire avec laquelle elle effectue un paiement de 100 lei (autorisé sans utiliser le code PIN de la carte), elle commettra à la fois l'infraction de vol concernant la carte bancaire, ainsi que l'infraction d'exécution d'opérations financières frauduleuses[45] (par le paiement avec ladite carte au terminal POS) et une infraction d'accès illégal à un système informatique[46] (le terminal POS ayant été accédé via la carte pour effectuer le paiement).

Ainsi, bien que le préjudice causé à la victime soit également de 100 lei, la deuxième activité criminelle sera qualifiée comme un concours de trois infractions, générant un traitement pénal beaucoup plus sévère sous cet angle.

Dans cette perspective, pour répondre aux exigences de prévisibilité concernant l'étendue des accusations pouvant être portées en cas de commission d'infractions informatiques ou d'infractions commises digitalement, une assistance juridique spécialisée peut parfois être nécessaire. À cet égard, la question du concours de qualifications, qui peut survenir le plus souvent dans le cas des infractions informatiques, peut se poser, la logique étant celle d'une sanction « stratifiée » des conduites, chaque étape infractionnelle représentant une nouvelle infraction – par exemple, l'accès illégal à un système informatique

[45] Art. 250 C.pen.: L'exécution d'une opération de retrait d'espèces, de chargement ou de déchargement d'un instrument de monnaie électronique, ou de transfert de fonds, de valeur monétaire ou de monnaie virtuelle, par l'utilisation, sans le consentement du titulaire, d'un instrument de paiement sans numéraire ou des données d'identification permettant son utilisation, est punie d'une peine d'emprisonnement de 2 à 7 ans. (Efectuarea unei operaţiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, valoare monetară sau monedă virtuală, prin utilizarea, fără consimţământul titularului, a unui instrument de plată fără numerar sau a datelor de identificare care permit utilizarea acestuia, se pedepseşte cu închisoarea de la 2 la 7 ani.)

[46] Art. 360 C.pen.: (1) L'accès, sans droit, à un système informatique est puni d'une peine d'emprisonnement de 3 mois à 3 ans ou d'une amende. (2) L'acte prévu au paragraphe (1), commis dans le but d'obtenir des données informatiques, est puni d'une peine d'emprisonnement de 6 mois à 5 ans. (3) Si l'acte prévu au paragraphe (1) a été commis à l'égard d'un système informatique dont l'accès est restreint ou interdit pour certaines catégories d'utilisateurs au moyen de procédures, dispositifs ou programmes spécialisés, la peine est une peine d'emprisonnement de 2 à 7 ans.
[(1) Accesul, fără drept, la un sistem informatic se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă. (2) Fapta prevăzută în alin. (1), săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoarea de la 6 luni la 5 ani. (3) Dacă fapta prevăzută în alin. (1) a fost săvârşită cu privire la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, accesul este restricţionat sau interzis pentru anumite categorii de utilizatori, pedeapsa este închisoarea de la 2 la 7 ani.]

suivi du transfert non autorisé de données informatiques constituera un concours d'infractions. L'approche différente par rapport au monde matériel, où l'intrusion dans le domicile d'une personne suivie du vol de biens sera une infraction complexe, ne justifie cependant pas automatiquement des critiques liées à la prévisibilité. Il ne faut pas perdre de vue non plus, que l'infraction complexe de vol qualifié par violation de domicile est une forme d'unité légale, mais repose sur deux conduites qui seraient retenues en concours en son absence : une infraction de vol et une infraction de violation de domicile.

Une autre discussion possible concernant la nécessité éventuelle de faire appel à un spécialiste peut être liée à l'infraction d'accès illégal à un système informatique. La question soulevée dans plusieurs affaires pratiques était de savoir si l'utilisation d'un système informatique auquel le titulaire a droit d'accès, mais à des fins autres que celles pour lesquelles cet accès lui est accordé ou en dehors des attributions professionnelles, est qualifiée comme un accès illégal à un système informatique ou non.

Bien que le problème semble simple à première vue, il existait une disposition dans l'ancienne réglementation – l'article 35 alin. (2) de la Loi n° 161/2003 – qui stipulait que : « *(2) Aux fins du présent titre, agit sans droit la personne qui se trouve dans l'une des situations suivantes: a) elle n'est pas autorisée, en vertu de la loi ou d'un contrat ; b) elle dépasse les limites de l'autorisation ; c) elle n'a pas la permission, de la part de la personne physique ou morale compétente selon la loi, d'utiliser, d'administrer ou de contrôler un système informatique ou de mener des recherches scientifiques ou toute autre opération dans un système informatique* ».

Il convient de mentionner que toutes les infractions informatiques réglementées dans le Code pénal ont été reprises du Titre III (Prévention et lutte contre la criminalité informatique) de la Loi n° 161/2003.

En lien avec ce texte, certaines questions pertinentes se posent, telles que dans quelle mesure ce texte issu d'une loi spéciale peut compléter/interpréter le contenu constitutif d'une infraction prévue dans le Code pénal, sans qu'il y ait une référence directe ou explicite à cette norme. En l'absence d'une telle référence, nous pensons que l'application *de lege lata* des dispositions de la Loi n° 161/2003 pourrait constituer une violation des exigences de prévisibilité de la loi. Bien que les destinataires des normes aient en principe la possibilité de consulter des spécialistes pour identifier les risques pénaux liés à leurs conduites et qu'ils puissent éventuellement être informés par leur fiche de poste ou d'autres actes administratifs/internes des limites dans lesquelles ils peuvent accéder aux systèmes informatiques concernés, nous ne pensons pas que cela devrait permettre d'ajouter aux dispositions de la loi pénale. Malgré ces aspects, il semble que l'approche contraire a été adoptée par la Cour Constitutionnelle, qui a indiqué que les dispositions de la Loi n° 161/2003 devraient rester applicables : « *même si le Code pénal n'a pas repris toutes les définitions de la Loi n° 161/2003, celle-ci reste un repère pour comprendre les éléments de contenu de l'infraction critiquée* »[47].

De plus, l'hypothèse du « *dépassement des limites de l'autorisation* » est équivoque, car elle ne réglemente pas de manière suffisamment claire ce que ce dépassement implique. Par exemple, il a été retenu dans une affaire que le dépassement des limites de l'autorisation peut être constaté lorsqu'un compte auquel une personne a légalement accès

[47] Cour Constitutionnelle du Roumanie, Décision n° 183 du 29 mars 2018, M. Of. n° 486 du 13.06.2018.

est utilisé à d'autres fins[48]. À l'opposé, il peut être retenu qu'un utilisateur existant dépasse les limites de l'autorisation uniquement lorsqu'il utilise une partie du système informatique à laquelle il n'avait pas accès. Par exemple, un utilisateur avec des pouvoirs limités accède à des fonctionnalités spécifiques à l'administrateur réseau.

Dans la même affaire, il a été retenu par la cour d'appel qu'il ne faut pas confondre l'accès à un système informatique avec l'interrogation de la base de données contenue dans ce système informatique, l'interrogation étant postérieure. Le texte de loi incrimine l'accès, et non l'interrogation sans droit d'un système informatique[49]. De la motivation de la Cour d'appel ressort clairement la manière dont cette norme doit être interprétée, une interprétation que nous estimons être tout à fait prévisible : « Dans la mesure où le législateur n'a pas incriminé l'utilisation sans droit d'un système informatique ou l'accès sans droit aux données informatiques, la conduite de l'accusé ne correspond pas à l'action incriminée par l'article 360 du Code pénal »[50].

B. La nécessité de l'intervention de la Haute Cour de Cassation et de Justice pour clarifier certaines situations spécifiques à la criminalité dans le cyber espace

Comme cela a déjà été observé à plusieurs reprises dans ce qui précède, la pratique judiciaire de notre pays a rencontré plusieurs problèmes concernant l'application de certaines normes d'incrimination dans le cyber espace. Le simple besoin de résoudre de telles situations peut soulever des questions sur la prévisibilité de l'application des normes d'incrimination. Bien que dans certains cas la solution semblait relativement évidente, la pratique judiciaire a été contradictoire et il y a eu différentes interprétations, ce qui a conduit à la nécessité de trancher le problème par des décisions contraignantes rendues par la Haute Cour de Cassation et de Justice. Bien que certaines de ces décisions puissent paraître simples et logiques, dans un contexte où des opinions divergentes ont émergé concernant certains des problèmes soulevés, nous pensons que ces solutions sont les bienvenues. À cet égard, nous rappelons les conclusions auxquelles est parvenue la Cour européenne des droits de l'homme, qui a constaté qu'une jurisprudence incohérente, générée par des opinions divergentes sur l'application de certaines normes juridiques, peut entraîner un manque de prévisibilité pour les destinataires des normes d'incrimination, ce qui serait contraire à l'article 7 de la Convention[51].

Nous analyserons quelques-unes de ces décisions dans un ordre chronologique, en fonction du moment où elles ont été rendues.

1. L'utilisation des cartes bancaires dans des activités criminelles

L'une des problématiques qui a le plus préoccupé la pratique judiciaire en matière d'infractions commises par des moyens informatiques a été celle de l'utilisation non autorisée de cartes bancaires pour effectuer des paiements.

La première discussion de ce type est apparue dans le contexte d'une pratique non

[48] Trib. Ialomița, Section pénale, sentence n° 61/2022 du 22.07.2022, code RH deee9763g (rejust.ro), *annulée dans la voie d'appel – décision mentionnée dans la suivante note de bas de page.*
[49] C. Ap. Bucarest, Section I pénale, Décision n° 455/2023 du 17.02.2023, code RJ 98dggg695 (rejust.ro).
[50] *Ibidem.*
[51] Žaja c. Croatie, requête n° 37462/79, jugement du 4 octobre 2016, pt. 103.

uniforme sous l'empire de l'ancienne réglementation, qui était similaire en termes de normes d'incrimination, conduisant à la nécessité de prononcer la décision RIL n° 15/2013, par laquelle la Haute Cour de Cassation et de Justice a établi que : *« L'utilisation d'un distributeur automatique de billets (DAB) avec une carte bancaire authentique, sans le consentement de son titulaire, dans le but d'effectuer des retraits d'espèces, constitue l'infraction d'exécution d'opérations financières de manière frauduleuse par l'utilisation d'un instrument de paiement électronique, y compris les données d'identification permettant son utilisation, prévue à l'article 27 alin. (1) de la Loi n° 365/2002, en concours idéal avec l'infraction d'accès, sans droit, à un système informatique commise dans le but d'obtenir des données informatiques en violation des mesures de sécurité, prévue à l'article 42 alin. (1), (2) et (3) de la Loi n° 161/2003 »*[52].

Bien que cette décision ait été tout à fait claire, quant à la nécessité d'un concours d'infractions entre les deux, la pratique judiciaire a de nouveau rencontré des difficultés lorsqu'il s'est agi de l'utilisation de cartes informatiques falsifiées.

À cet égard, par la décision HP n° 2/2021, la Haute Cour de Cassation et de Justice a rejeté comme irrecevable la demande portant sur la question suivante : « *Si le retrait d'espèces avec des cartes falsifiées, en utilisant les données des cartes copiées, remplit les éléments constitutifs de l'infraction d'exécution d'opérations financières de manière frauduleuse prévue par l'art. 250 alin. (1) et (2) du Code pénal en concours idéal avec l'infraction d'accès illégal à un système informatique prévue par l'art. 360 du Code pénal ou seulement l'infraction d'exécution d'opérations financières de manière frauduleuse, prévue par l'art. 250 alin. (1) et (2) du Code pénal* »[53]. Dans les considérants, il a été retenu que la question avait déjà été tranchée par la Décision RIL n° 15/2013 mentionnée, aucun problème supplémentaire n'ayant été soulevé par rapport à l'hypothèse précédemment analysée. En accord avec les considérants de la Haute Cour, de notre point de vue, la différence entre les deux questions – carte bancaire authentique utilisée sans le consentement du titulaire dans le premier cas et carte bancaire falsifiée dans le second – peut tout au plus conduire à retenir une infraction supplémentaire, celle qui incrimine la détention/utilisation d'un instrument de paiement falsifié, mais en aucun cas réduire le nombre d'infractions retenues précédemment.

Dans le même sens, plus récemment, par la décision HP n° 53/2022, la Haute Cour de Cassation et de Justice a rejeté comme irrecevable la demande portant sur la question suivante: « *L'utilisation sans droit d'une carte bancaire, en mode sans contact, sur un terminal POS, pour le paiement de produits, réunit-elle les éléments constitutifs de deux infractions, à savoir l'accès à un système informatique, prévu par l'art. 360 alin. (1) C.pén. et l'exécution d'opérations financières de manière frauduleuse, prévue par l'art. 250 alin. (1) C.pén. (sous forme tentée ou consommée, selon l'exécution effective de la transaction) ou seulement les éléments constitutifs de l'infraction d'exécution d'opérations financières de manière frauduleuse, prévue par l'art. 250 alin. (1) C.pén. (sous forme tentée ou consommée, selon l'exécution effective de la transaction) ?* »[54]. La motivation du rejet comme irrecevable

[52] HCCJ, Formation pour le règlement des recours dans l'intérêt de la loi, Décision n° 15 du 14 octobre 2013, M. Of. n° 760 du 6 décembre 2013.
[53] HCCJ, Formation pour le règlement de certaines questions de droit en matière pénale, Décision n° 2 du 20 janvier 2021, M. Of. n° 293 du 24 mars 2021.
[54] HCCJ, Formation pour le règlement de certaines questions de droit en matière pénale, Décision n° 53 du 28 septembre 2022, M. Of. n° 1120 du 21 novembre 2022.

a consisté, à nouveau, en l'absence d'un réel problème de droit, compte tenu de l'applicabilité mutatis mutandis de la décision RIL n° 15/2013 y compris dans cette situation, en indiquant que « *la technologie sans contact assure la même fonction de la carte bancaire, celle-ci pouvant être utilisée sur un terminal POS ou ATM, par simple approche de la carte de ceux-ci étant accédés les mêmes systèmes informatiques* »[55].

Même si aucune de ces décisions n'a conduit à un changement de paradigme, on observe un sentiment d'incertitude par rapport à la manière dont les normes d'incrimination devraient être appliquées dans ces cas. Il est possible que la raison réelle de ces saisines subséquentes soit la tentative de réaliser un revirement jurisprudentiel, étant donné la nécessité de retenir un concours d'infractions, avec des limites de peine qui révèlent une grande gravité des faits.

2. Création de comptes fictifs sur les réseaux sociaux

Par la décision HP n° 4/2021, la Haute Cour de Cassation et de Justice a établi que « *Le fait d'ouvrir et d'utiliser un compte sur un réseau social ouvert au public, en utilisant comme nom d'utilisateur le nom d'une autre personne et en introduisant des données personnelles réelles permettant son identification, remplit deux des exigences essentielles de l'infraction de faux informatique prévue à l'article 325 du Code pénal, à savoir que l'action d'introduction des données informatiques soit réalisée sans droit et que l'action d'introduction des données informatiques ait pour résultat des données non conformes à la vérité* »[56]. Par cette décision, la Haute Cour de Cassation et de Justice a procédé à une analyse des éléments constitutifs de l'infraction de faux informatique, tranchant la discussion sur deux d'entre eux et montrant que la qualification juridique finale sera établie à condition que « *le but des activités menées sans droit et qui ont pour résultat des données non conformes à la vérité soit celui d'utiliser les données informatiques en vue de produire des conséquences juridiques, ceci devant être vérifié en fonction des circonstances concrètes de chaque affaire* »[57]. On observe les multiples comparaisons effectuées par la Haute Cour dans ses considérants entre la situation de falsification de documents et l'introduction de données informatiques non conformes à la vérité, ce qui, à notre avis, offre un plus de prévisibilité à la solution donnée, afin de ne pas s'éloigner des voies déjà tracées concernant les infractions classiques de faux.

3. L'Escroquerie commisse en ligne

Par la décision HP n° 37/2021, la Haute Cour de Cassation et de Justice a établi que « *la publication d'annonces fictives en ligne ayant entraîné la production d'un préjudice, sans que cette activité n'intervienne sur le système informatique ou sur les données informatiques traitées par celui-ci, réalise les conditions de typicité de l'infraction d'escroquerie, prévue par l'art. 244 du Code pénal* »[58]. Nous ne contestons en aucun cas cette solution, mais au

[55] *Idem*.
[56] HCCJ, Formation pour le règlement de certaines questions de droit en matière pénale, Décision n° 4 du 25 janvier 2021, M. Of. n° 181/19 février 2021.
[57] *Ibidem.*
[58] HCCJ, Formation pour le règlement de certaines questions de droit en matière pénale, Décision n° 37 du 7 juin 2021, M. Of. n° 797/16 juillet 2021.

contraire, nous exprimons notre étonnement quant à la nécessité de prononcer cette solution, la qualification juridique d'une telle conduite comme fraude informatique étant difficile à accepter de notre point de vue, car l'essence des annonces en ligne ne réside pas dans les données informatiques introduites, mais dans les informations erronées qu'elles représentent.

4. Le dépassement des limites de l'autorisation dans le cas de l'infraction d'accès illégal à un système informatique

Un autre exemple est donné par la décision HP n° 68/2021, par laquelle la Haute Cour de Cassation et de Justice a rejeté comme irrecevable la demande portant sur la question suivante: « *Dans l'interprétation des dispositions de l'article 360, paragraphe (1) du Code pénal concernant l'accès illégal à un système informatique, dans le cas des personnes pouvant interroger à tout moment une base de données contenant des informations non publiques, une telle interrogation non suivie de la réalisation ultérieure d'actes spécifiques à l'exercice des fonctions liées à l'interrogation effectuée, peut-elle représenter un dépassement des limites pour lesquelles l'autorisation a été accordée ?* »[59]. Comme nous l'avons déjà discuté ci-dessus, le rejet de la question comme irrecevable résulte de la considération selon laquelle le problème est clair du point de vue de la loi, car la conduite ultérieure de l'auteur par rapport aux informations obtenues en accédant au système informatique n'est pas pertinente en termes d'utilisation ou de non-utilisation de celles-ci ou du but dans lequel elles ont été effectivement utilisées (dans le cadre des fonctions ou sans lien avec celles-ci), étant donné que cela intervient après le moment où l'infraction est consommée, et ne pourrait donc pas déterminer son incidence[60]. Cependant, une critique qui pourrait être adressée à cette décision de la Haute Cour de Cassation et de Justice est que, bien qu'il semble être suggéré dans les motifs de rejet que la solution au problème juridique se trouve déjà dans la législation, elle ne tranche pas suffisamment clairement la direction dans laquelle cette solution devrait aller. À notre avis, lorsqu'une décision est rendue pour rejeter comme irrecevable une résolution d'une question juridique parce que la solution existe déjà dans la législation ou dans la pratique, nous pensons qu'elle devrait être rédigée, au niveau des motifs, d'une manière qui montre clairement quelle est cette solution, car inclure seulement des repères qui peuvent être considérés comme équivoques n'est pas conforme aux exigences de prévisibilité qui devraient caractériser une norme d'incrimination.

CONCLUSIONS

D'après notre analyse, nous pensons que quelques observations peuvent être faites à titre de conclusions. La réglementation des infractions informatiques et des infractions pouvant être commises digitalement ne crée pas de problèmes particuliers du point de vue de la prévisibilité. Les normes d'incrimination sont dans leur grande majorité assez claires, s'inscrivent dans les lignes classiques du point de vue de la description de l'acte de conduite

[59] HCCJ, Formation pour le règlement de certaines questions de droit en matière pénale, Décision n° 68 du 29 septembre 2021, M. Of. n° 56 du 19 janvier 2022.
[60] C. Ap. Bucarest, Section I pénale, Décision no. 455/2023, *cit. supra*.

sous forme d'élément matériel et par leur réglementation, le législateur ne crée pas la prémisse d'une approche extensive. Les normes d'incrimination sont également claires conformément au standard relatif aux droits de l'homme, même si des clarifications jurisprudentielles sont parfois nécessaires pour déterminer l'étendue de leur contenu. De plus, les normes d'incrimination ne sont pas trop techniques, mais peuvent être comprises de manière acceptable, même dans le contexte du recours à des spécialistes, ce qui a été établi dans la jurisprudence européenne en matière de droit de l'homme comme étant conforme.

Cependant, même si du côté de la réglementation les exigences de prévisibilité peuvent être considérées comme remplies, autant du point de vue de la législation nationale que du point de vue des règles imposées par la jurisprudence de la Cour Européenne des Droits de L'Homme, du côté de l'application des normes nos appréciations ne seront pas aussi élogieuses. Premièrement, on observe une incertitude au niveau de la pratique judiciaire concernant la qualification de certaines conduites comme infractions spécifiques à l'environnement numérique ou comme infractions classiques commises dans l'environnement numérique, comme c'est le cas de la délimitation entre les infractions de fraude informatique et d'escroquerie. De manière égale, la méthode principale d'interprétation utilisée dans la jurisprudence pour déterminer la portée des normes d'incrimination, l'interprétation évolutive, telle qu'elle a été appliquée dans les affaires que nous avons analysées dans le présent travail, est conforme aux standards de clarté et de prévisibilité de l'application du droit pénal établis dans la jurisprudence de la Cour Européenne des Droits de L'Homme

Deuxièmement, d'un point de vue pratique, l'absence de réglementation par le législateur d'infractions complexes pour les infractions informatiques, comme dans le cas des infractions classiques, peut créer une apparence d'excès dans la rétention en concours de plusieurs normes d'incrimination. Cependant, le choix du législateur de créer des infractions complexes dans certaines matières et de laisser place au concours d'infractions dans d'autres, est une question de politique pénale, qui ne peut représenter *eo ipso* un motif de manque de prévisibilité sous l'aspect des qualifications juridiques ou des sanctions auxquelles une personne peut être soumise après avoir commis une infraction, si une telle approche est constante au niveau jurisprudentiel et prévisible pour les destinataires des normes d'incrimination, conformément aux règles établies par la Cour Européenne des Droits de l'Homme.

Enfin, comme nous avons observé que la Haute Cour de Cassation et de Justice l'a fait dans les décisions prononcées pour résoudre certaines questions de droit citées, nous devons toujours partir de la prémisse de l'existence d'une interaction inédite entre des institutions de droit traditionnelles, créées et façonnées depuis des dizaines voire des centaines d'années sur lesquelles fonctionne le droit pénal, et ce domaine relativement nouveau du cyber espace et de l'environnement en ligne. Ainsi, partant des repères classiques et établis, nous devons envisager de manière évolutive l'application des normes d'incrimination classiques dans le cyber espace, au moins jusqu'au moment (incertain) où pourrait se poser la question d'un changement fondamental de paradigme concernant les conduites infractionnelles commises dans l'environnement en ligne.