COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 13 April 2015 CDPC (2015) 5
cdpc/docs 2015/cdpc (2015) 5

COMITE EUROPEEN POUR LES PROBLEMES CRIMINELS
(CDPC)

PROJET DU RAPPORT SUR L'IMPACT DES NOUVELLES TECHNOLOGIES SUR LES COMPORTEMENTS ET LES LOIS EN MATIERE PENALE

Document préparé par M. Yves Charpenel,
Premier avocat général à la Cour de cassation

Site web du CDPC : www.coe.int/cdpc
Adresse électronique du CDPC : dgi-cdpc@coe.int

1 Introduction

Depuis l'apparition de l'Arpanet en 1965 et de l'Internet dans les années qui ont suivi, la diffusion foudroyante et universelle de cette nouvelle technologie n'a pas cessé d'influencer nos comportements.

L'ampleur de ces transformations a naturellement eu des répercussions significatives sur l'Etat de droit, dont l'existence et l'objectif sont précisément de réguler les comportements humains.

Trois séries de raisons au moins rendent difficile mais nécessaire l'appréhension de ces changements :

D'une part, la dimension technologique sophistiquée de ces nouveaux outils, qui ne s'inscrit pas dans la culture juridique traditionnelle, faisant douter les juristes, ceux qui font les lois comme ceux qui les appliquent de pouvoir en maîtriser tous les enjeux.

Les différentes études prospectives conduites à travers le monde sur la technologie de l'information tendent à montrer que cette évolution n'est pas en voie de se ralentir.

L'émergence du cloud computing par exemple, comme celle des réseaux sociaux professionnels ou privés, ne cesse de susciter des comportements et des pratiques auxquels les réponses sociales et juridiques en place peinent et tardent à répondre.

La transposition à ces situations nouvelles des réponses juridiques classiques est aujourd'hui insuffisante pour garantir à tous un accès au droit et une sécurité des règles du jeu social économique et politique satisfaisants.

D'autre part, l'enthousiasme des utilisateurs, à travers le Monde, à s'approprier les produits commercialisés de ces nouvelles technologies, le plus souvent sans exploration ou conscience des conséquences sur les règles de la vie sociale.

L'importance du marché des nouvelles technologies, lié notamment à sa diffusion universelle et au succès de politiques commerciales planétaires est un facteur supplémentaire de développements dynamiques où la course en avant domine nettement la prise de recul et l'évaluation des conséquences.

Enfin, la rapidité des évolutions techniques et de leur mise sur le marché prend de court le temps juridique d'élaboration et de diffusion des normes juridiques et des pratiques judiciaires.

Au plan européen par exemple, engagé depuis plus de 60 ans dans un long processus de mise en commun des principes et des règles de droit, les nouvelles technologies créent la réalité ou l'apparence d'une unification des pratiques, étendue en outre à l'ensemble de la planète sans qu'ait pu être posé un cadre minimum d'observation et de contrôle des risques inhérents à ces changements.

Ces mutations a-synchroniques sont perceptibles dans tous les domaines de nos vies, que ce soit au cœur des familles, des écoles, des entreprises, des prétoires ou des arènes politiques, des réformes entreprises en matière de filiation, de création artistique.

Si aucun des aspects de nos sociétés ne paraît échapper à l'effet des nouvelles technologies, ces incertitudes sont particulièrement caractéristiques dans le champ pénal.

Celui-ci, qui vise à prévenir et à sanctionner la violation des règles sociales les plus importantes pour une société à un moment donné, a, en effet été radicalement transformé et amplifié par le développement spectaculaire de la cybercriminalité.

Dans ce domaine si sensible de l'activité criminelle, l'Internet, plus que toute autre technologie moderne, doit nous conduire à reposer les questions fondamentales qui justifient l'existence et la défense d'un État de droit.

Quand plus de 35% de la population mondiale devient internaute, il n'est pas surprenant que les règles nouvelles qui vont progressivement leur être appliquées doivent être appréciées et confrontées au regard de celles, le droit en vigueur, qui ont vocation à traiter l'ensemble de la population.

Entre espoirs et risques, entre confiance et résignation, les réponses de l'Etat de droit au triomphe des nouvelles technologies ne peuvent être éludées sauf à voir émerger la figure de la machine (et de ceux qui la créent) comme boussole d'une société en perte de repères, en déficit de valeurs, en panne de droit.

Le versant à l'ombre de la société en voie de numérisation généralisée, c'est l'apparition d'une cybercriminalité insolente qui met en danger les valeurs de nos démocraties.

Celles-ci ont commencé à réfléchir et à agir dans une perspective de conjugaison difficile d'efficacité et de respect des principes fondamentaux du droit pénal.

La question est d'autant stratégique dans l'espace européen où cohabitent et tentent de s'harmoniser des systèmes de droit pénal différents :

Alors que n'est pas achevé le complexe processus d'harmonisation des systèmes pénaux européens partagés, avec toutes les variantes possibles entre un droit « dur » continental fondé sur la loi écrite et un droit « mou » anglo-saxon davantage fondé sur l'examen pragmatique des solutions jurisprudentielles antérieures, le risque est bien présent d'être désormais confronté à un droit « liquide » qui désempare plus qu'il ne rassure.

Pour tenter de cerner au plus près l'état du champ pénal en proie à la révolution numérique, il convient de garder à l'esprit l'importance du principe de cohérence, qui suggère une réponse qui évite l'éparpillement des dispositifs, du principe de compatibilité, qui garantit la poursuite d'un développement de l'État de droit en accord avec les principes dégagés par les institutions européennes et le principe d'efficacité, sans lequel les impacts, prévisibles ou imprévus des nouvelles technologies resteront en marge du droit.

Les rapports publics sur l'évolution de la cybercriminalité se multiplient comme en témoignent par exemple le rapport d'EUROPOL en février 2014 ou celui en France de Marc Robert en février 2014 et celui de la Suisse en mars 2014.
Leurs conclusions rejoignent globalement celles des innombrables rapports émanant de sociétés privées qui font tous état d'une menace qui s'étend.

Il n'est naturellement pas possible de considérer comme une fatalité incompréhensible l'impact de ces technologies sur nos comportements et sur nos droits, ni d'ailleurs d'imaginer en assurer une complète maîtrise.

Le présent rapport se propose d'esquisser une vue synoptique des principaux enjeux et zones de fracture qui caractérisent l'intersection entre l'univers pénal et le développement des nouvelles technologies.

Sa seule ambition est de mieux cerner les contours d'une future régulation équilibrée entre liberté et contrainte qui ne saurait être éludée sans fragiliser davantage notre État de droit européen.

Plan du rapport

2. Les enjeux spécifiques de l'impact des nouvelles technologies sur le champ pénal

La collision possible entre la loi pénale et l'Internet est une menace toujours présente dès lors que l'Internet est, par définition, conçu et utilisé comme l'ultime espace de liberté, et que le juge pénal est celui qui vient inlassablement rappeler l'existence de limites à cette liberté. Naturellement, il n'est imaginable d'envisager une société régie intégralement par la loi pénale ou par la loi de l'Internet.

Comme toujours, les progrès ou les reculs de l'État de droit reposent sur notre capacité à trouver le point d'équilibre pertinent à un moment donné entre liberté et contrainte, intérêts privés et intérêt général.

Nos sociétés modernes, et notamment les pays du continent européen ont, dès l'apparition de l'Internet, tenté de donner toute sa place et rien que sa place, à l'approche pénale, conscients que l'un des ciments les plus nécessaires de nos communautés, le contrat social, cher au siècle des Lumières, repose sur le respect des lois pénales qui conditionnent notre capacité à vivre ensemble sur un même territoire.

2.1 Un problème de définition

La définition de la cybercriminalité doit être normalisée au plan européen pour faciliter les actions de coopération entre les États membres et placée au rang des priorités communautaires en priorisant les secteurs d'activité les plus concernés.

Définir précisément l'objet de cette priorité est une préoccupation partagée par tous les auteurs des rapports publics et privés qui se succèdent depuis plus de 10 ans.

S'en tenir à une conception générale qui fait de la cybercriminalité un phénomène polymorphe et évolutif regroupant l'ensemble des infractions susceptibles d'être commises ou facilitées par l'utilisation des technologies numériques peut présenter un double avantage ;

D'une part, renvoyer à des grandes typologies non figées qui se partagent entre infractions liées directement aux systèmes d'information et aux réseaux, et infractions classiques facilitées par l'usage de ces techniques ;

D'autre part, faire la part des comportements qui peuvent être qualifiés de criminels, c'est-à-dire définis par la loi comme une infraction pénale, de tous les autres impacts, civils, sociaux ou commerciaux qui ne relèvent pas directement de la loi pénale, celle-ci n'intervenant que pour en réprimer les abus et les dérives, dès lors qu'ils sont prévus en tant que tels comme des infractions.

La définition encore plus générale de la cybercriminalité proposée par l'ONU (« tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent ») doit ainsi permettre de se focaliser sur l'ensemble des faits de délinquance liés aux technologies numériques, principalement l'Internet.

Depuis l'entrée en vigueur de la Convention de Budapest, c'est moins de la question de la définition de la cybercriminalité, nécessairement souple et générale afin d'anticiper raisonnablement les évolutions des techniques et des comportements, que celle des stratégies pour la combattre qui doit focaliser les débats.

À la diversité des situations créées par ces nouvelles technologies répond la variété des réponses pénales possibles.

Il convient ainsi de relativiser également l'importance d'une définition des nouvelles technologies afin de se prémunir du risque de voir les réflexions être réservées aux seuls spécialistes de la haute technologie, alors même que l'enjeu majeur est celui de la protection de l'ensemble des ressortissants des États à l'occasion de l'usage quotidien extrêmement large qu'ils font de ces nouveaux outils.

Dans ce contexte où la détermination des enjeux et des priorités publiques est essentielle, il convient d'appliquer le même raisonnement pour délimiter le champ pénal concerné :

Au-delà des catégories juridiques savantes, la mesure de l'impact des comportements et des lois pénales doit nécessairement inclure les considérations liées au droit pénal matériel comme au droit pénal processuel, ainsi que les politiques pénales qui y sont associées.

L'état des lieux du droit pénal européen montre à cet égard que ces préoccupations sont largement partagées par l'ensemble des États membres qui, depuis la Convention de Budapest et son protocole additionnel, sont entrés dans un cycle d'échanges et de normalisation permanent.

La richesse et la variété de ces travaux qui, tous s'efforcent de trouver le point d'équilibre pertinent entre principes contraignants et mise en œuvre souple, entre impératifs de sécurité et de respect des libertés, doivent sans doute être davantage mises en perspective.

La succession des textes recherchant l'harmonisation de législations internes autour de lignes directrices affranchies des lourdeurs des états de l'art technologique en perpétuelle fusion est sans doute la première exigence pédagogique pour les institutions européennes :

Aux flous inévitables des contours du « cloud computing », du « big data » ou de « l'open data » caractéristiques du développement actuel des nouvelles technologies, il convient de répondre avec une plus grande lisibilité des principes et de leurs applications dans l'espace judiciaire européen.

Cette ambition est d'autant plus stratégique que le champ pénal, au regard des principes consacrés par la Convention européenne des Droits de l'homme, ne peut s'accommoder, dans ses règles du jeu, d'une imprécision ou d'ambiguïtés persistantes.

A ce titre, le Conseil de l'Europe a vocation à rechercher la rédaction de nouveaux protocoles additionnels, en matière notamment de définition des cyber-infractions et de détermination des conditions de l'entraide répressive en la matière.
L'évaluation de l'impact des normes européennes qui se sont succédées dans différents secteurs de la criminalité transnationale, comme par exemple, les directives de l'Union du 8 juin 2000 sur le commerce électronique, celle de 2002 sur la vie privée, celle de 2006 sur la conservation des données ou encore le règlement 611/2013 dit « data breach » est une condition d'efficacité pour l'avenir immédiat de l'État de droit européen.

Les travaux menés dans ce contexte par la formation dédiée d'Europol (EC3) pourraient servir de base à un véritable observatoire opérationnel des lois pénales relatives à la cybercriminalité.

Un rapide regard sur le droit comparé extra-européen en matière de cybercriminalité montre la même effervescence normative et la nécessité d'un regard synoptique sur l'effectivité de ces règles avant d'envisager la poursuite d'un processus d'harmonisation universel encore bien timide.

Si l'on prend les exemples des USA et du Canada, pays essentiellement fédéraux, on retrouve à la fois la prolifération des lois spécifiques et la dispersion des services spécialisés dans la lutte contre la cybercriminalité.
La Chine populaire, au contraire, État centralisé, concentre ses textes de fond dans son Code pénal, qui consacre 3 articles à la cybercriminalité (à rapprocher par exemple des 248 cyber incriminations françaises), confie au Ministère de la sécurité publique le soin de mener les actions répressives.

Tous cependant partagent le souci de distinguer des grandes typologies de cybercrimes plutôt qu'un inventaire impossible de toutes les cyber-infractions.

Aucun en revanche ne présente un bilan précis des impacts sur la réalité de cyber infractions, ni ne propose un cadre spécifique de coopération internationale.

La principale incitation à une réflexion élargie au-delà de l'espace pénal européen peut être sans doute trouvée dans le constat de la répétition d'affaires judiciaires telles que Wikileaks ou PRISM, qui révèlent l'universalité des faits criminels et l'hétérogénéité des réponses pénales proposées.

2.2 Les enjeux de l'Internet pour l'État de droit en Europe

À partir des travaux de suivi de la Convention de Budapest et du plan Octopus qui s'efforce notamment d'adopter des positions convergentes à l'égard des sociétés de diffusion du net extracommunautaires, il est possible d'esquisser le constat suivant qui témoigne de l'importance des enjeux.

C'est d'abord le fait que la criminalité transnationale prospère et innovante, selon les bilans convergents de l'ONDC, de l'OCDE ou de l'OIT, a trouvé dans le cybermonde un élargissement de ses profits traditionnels et de sources nouvelles considérables qui sont naturellement un puissant moteur d'innovation criminelle potentiellement dévastatrice pour nos économies.

L'adoption de principes directeurs communs est à l'évidence la voie pertinente pour relever ce défi en cherchant à éviter l'écueil du choc des souverainetés juridiques qui caractérisent le domaine pénal.

La Convention sur la cybercriminalité du Conseil de l'Europe, qui est le seul instrument international contraignant concernant la question de la cybercriminalité, doit à ce titre rester la boussole des futures initiatives européennes visant à parvenir à l'adoption de lignes directrices pour tout pays élaborant une législation exhaustive en matière de cybercriminalité, mais aussi de cadre pour la coopération internationale contre la cybercriminalité parmi les États Parties.

La Convention est complétée par le Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques et est suivie par le Comité de la Convention sur la cybercriminalité (T-CY).

Le mécanisme prévu en l'état, qui consiste à procéder à des consultations régulières des Parties lors d'au moins une réunion annuelle du Comité de la Convention, doit pouvoir évoluer vers un système global d'évaluation mutuelle à l'instar de ce qui est prévu par exemple en matière de corruption ou de traite des êtres humains pour donner un nouvel élan à l'harmonisation des principes et des règles de procédure et de coopération.

Le premier des enjeux est donc vraisemblablement de continuer à renforcer les outils communs existants avant d'envisager la création de nouvelles structures à vocation contraignante.

La seconde étape devrait être un effort de sensibilisation des juridictions pénales européennes pour dégager progressivement une jurisprudence susceptible de proposer des réponses plus homogènes.

À ce titre, la constitution d'une base de données européenne des cyber-décisions pourrait contribuer à accélérer la connaissance des réponses proposées aux principes communs.

Cette communauté des juristes européens est d'autant plus importante que les progrès de la cybercriminalité s'inscrivent dans un contexte où l'ensemble des opérateurs échappent largement à l'application des normes européennes et sont pour le moins réticents à s'y soumettre.

Mark Zuckerberg (janvier 2012) : « *L'internet est l'outil le plus puissant dont nous disposons pour créer un monde plus ouvert et connecté. Nous ne pouvons laisser des lois mal pensées se mettre en travers du développement de l'Internet. Facebook s'oppose à SOPA et PIPA, et nous allons continuer à nous opposer à toute loi qui nuira à l'Internet* » avant d'ajouter, « *Aujourd'hui le monde a besoin de dirigeants politiques pro-internet. Nous avons travaillé pendant des mois avec nombre de ces gens sur des alternatives bien meilleures que les propositions actuelles. Je vous encourage à en apprendre d'avantage sur ces questions et dîtes aux membres du congrès d'être pour internet*. »

2.3 Un problème de chronologie

Une réflexion sur la capacité des dispositifs législatifs et réglementaires à anticiper ou suivre les différentes vagues technologiques qui induisent des modifications incessantes et parfois durables des comportements, doit être menée pour assurer une meilleure prise en compte des défis proposés à l'Europe.

L'objectif est de faire un choix de stratégie normative, entre principes généraux intemporels, régulation plus technique des nouveaux outils à venir et simple réactivité.

Les dernières années ont montré une réalité où la technologie et les comportements se développent plus vite que les lois en la matière : s'il n'est pas exceptionnel que le gendarme coure moins vite que le voleur, encore faut-il veiller à ce que la course ne soit pas considérée comme perdue d'avance.

Les handicaps sont bien connus, entre une technique évolutive et dominante qui ne fait qu'accentuer le développement de comportements imprévisibles et réactifs, des législations hétérogènes appliquées de manière non moins incertaine.

La radicale nouveauté de l'impact sur les lois et sur les comportements en matière pénale est illustrée en la matière par l'émergence de deux phénomènes très perturbants pour l'application de la loi pénale :

La question de la **territorialité,** qui fonde les principes nécessairement restrictifs de compétence du juge pénal, est désormais confrontée au défi d'un univers virtuel où le criminel et sa victime, qui eux sont bien réels, se rencontrent à tout instant, et potentiellement pour toujours, sur l'ensemble du cyber monde, c'est-à-dire partout, rendant compétent n'importe lequel des juges exerçant dans un pays où l'Internet est accessible.

Désormais, le cloud computing contribue à complexifier de manière exponentielle les problématiques traditionnelles de règlement des conflits de compétence juridictionnelle.

La question de **l'identité numérique** n'est pas moins épineuse pour le pénaliste respectueux des principes pénaux européens de procédure pénale, dès lors que la nouvelle technologie peut faire peser un doute raisonnable sur la personne physique ou morale qui a réellement entendu commettre une infraction, sauf à s'en remettre aveuglément aux arbitrages techniques qui s'appliquent aux adresses IP et aux différents protocoles de données.

Face à cette instabilité chronique de la loi pénale dans nos démocraties, aggravée par une tendance à remettre en cause régulièrement des lois promulguées, la réponse pénale doit tenir compte, particulièrement en matière de nouvelles technologies, du glissement irrésistible du droit dur vers le droit mou, au risque de devoir faire avec un « droit liquide » où le flux des données, par son ampleur, sa rapidité et sa fluidité, met en échec les réponses traditionnelles et leur objet essentiel qui est d'assurer la sécurité juridique de tous.

La question de la compatibilité entre temps judiciaire et temps numérique restera posée, mais doit être présente à l'esprit à l'occasion des évaluations des dispositifs mis en place, en veillant à ne pas déséquilibrer davantage les rapports entre impératifs de stabilité et de liberté.

2 .4 Les 3 points faibles de la réponse pénale

Une bonne prise en compte des réponses pénales aux aléas de la nouvelle technologie implique de bien évaluer les principales zones de fractures que le numérique peut imposer à nos systèmes juridiques et judiciaires.

Ceux-ci sont, en tout état de cause, mis en demeure de bien anticiper, accompagner ou corriger les comportements susceptibles de recevoir une qualification pénale.

Force est de constater que l'impact des nouvelles technologies contribue à relativiser encore l'effectivité des lois sur les comportements sociaux.
La difficulté s'accroît encore de la considération, inévitable, que l'efficacité de tout dispositif n'est forte qu'à la mesure de ses maillons les plus faibles.
En conséquence, toute avancée légale ne peut prétendre, en matière pénale, à répondre à ses missions qu'à la condition de ne sous-estimer aucune des trois exigences de tout système pénal :

D'abord, mener la **prévention** de la cybercriminalité qui ne peut être méconnue, sauf à se résoudre à en subir les atteintes croissantes.
Une telle politique de prévention est compliquée par l'étendue du champ concerné, c'est-à-dire l'ensemble des comportements individuels et collectifs faisant appel à ces technologies.

Elles se compliquent encore en ce qu'elles doivent démontrer au public le plus large que les facilités immenses qui lui sont offertes comprennent néanmoins des risques et donc, des limites.

Enfin, ces politiques devant être à la mesure de l'universalité du cyber monde, se doivent d'être transnationales ou au moins inscrites dans un contexte de recherche d'harmonisation des politiques étatiques.

Les investigations, ensuite, sont l'un des domaines le plus fortement impacté par les nouvelles technologies, notamment sous l'angle de la détermination de la preuve pénale.

La diffusion généralisée des outils numériques dans la société se traduit logiquement par la présence généralisée d'éléments de preuve disponibles sous forme numérique.

Les exigences propres à la matière pénale, que sont la loyauté et la fiabilité des preuves recevables devant un juge aux fins d'établir la culpabilité d'un suspect, sont d'autant plus fortes que l'appréhension technique de ces preuves numériques n'est pas encore inscrite dans la culture des enquêteurs et des juges.

Il importe donc, pour tirer de la nouvelle technologie des avantages au moins comparables à ceux dont les criminels se sont emparés dès leur apparition sur le marché, que la loi soit au clair, autant dans la définition des méthodes de recueil de ces preuves que dans leur définition normative.

La fuite en avant technologique sans contrôle étant, en effet, interdite aux enquêteurs, il est indispensable que la loi définisse avec précision et certitude les preuves numériques recevables.

Si le principe de liberté de la preuve pénale et la notion de faisceau d'indices suffisants permettent de garder à la preuve numérique une souplesse susceptible d'accompagner les progrès technologiques à venir, il n'en reste pas moins nécessaire de prévoir dans la loi les règles de recueil, sur la base notamment des travaux menés par le Conseil de l'Europe à partir de son guide sur le recueil de la preuve numérique.

La **répression,** enfin, est l'aboutissement logique de la lutte contre la cybercriminalité, et les principes qui la gouvernent ont naturellement vocation à être appliqués identiquement.

Cependant, le champ pénal reste l'un des plus liés aux particularités politiques, sociales et culturelles de chacun des Etats, y compris au sein du continent européen.

C'est dire que le défi de l'impact pénal des nouvelles technologies ne peut être relevé qu'à la double condition ambitieuse de ne pas sous-estimer le choix de réponses répressives adaptées à l'extraterritorialité des nouvelles technologies qui impose, on l'a vu, de prendre en compte simultanément le risque de méconnaître le principe non bis in idem, et celui de favoriser un « court shopping » par le constat de l'existence de véritables « paradis répressifs numériques », dévaluant toute exemplarité de la réponse pénale.

On mesure également que les peines encourues, à supposer résolues les questions de compétence territoriale, de définition de l'infraction et d'imputabilité à un mis en cause, aient elles-mêmes un impact sur le comportement critiquable.

Les peines de prison étant réservées aux violations les plus graves commises par des personnes physiques, et les peines d'amende n'ayant de sens que si elles peuvent être effectivement recouvrées, il reste à déterminer les mesures pénales pertinentes telles que la fermeture de site, le déréférencement, la publication des condamnations par voie de médias ou la confiscation des outils ayant permis l'infraction.

Une réflexion sur la nature, le sens et la portée de la peine numérique est à approfondir.

3. Des domaines inégalement impactés

Le Conseil de l’Europe doit avoir vocation à pointer les secteurs d’activité où la menace cybercriminelle est la plus forte, afin de recenser et d’illustrer l’ampleur des comportements impactés, en évaluant le degré d’inadaptation des réponses normatives existantes, au plan des États comme au plan des institutions européennes.

Quatre secteurs principaux peuvent être signalés comme justifiant une vigilance prioritaire au regard des infractions déjà constatées et de la mesure de l'efficacité des réponses déjà expérimentées.

Il est à noter que la constante diversification de l'offre commerciale en la matière contribue paradoxalement à enrichir le potentiel criminel, ce qui traduit autant la capacité des nouvelles technologies à impacter les comportements humains de plus en plus variés que celle des criminels à tirer parti d'outils nouveaux.

3.1 Les atteintes à la personnalité

La définition d'une doctrine et de principes durables communs est particulièrement stratégique dans le domaine où l'impact pénal des nouvelles technologies est sans doute le plus universel, celui des droits liés à la personnalité ;

Ces droits, que depuis la déclaration fondatrice des Droits de l'homme et du citoyen, les différentes institutions européennes n'ont cessé de réaffirmer, sont particulièrement impactés par la généralisation d'outils permettant des échanges et des stockages d'information apparemment illimités.

Si les avantages pour la liberté de communication sont considérables, les abus qui ont en ont découlé ne le sont pas moins.

Les Gouvernements se sont, en général, efforcés d'apporter des réponses et de poser des limites, mais le plus souvent en ordre dispersé et de manière plus réactive que proactive.

C'est également ici que la pertinence des lois destinées à réguler les nouveaux comportements générés par les nouvelles technologies est la plus stratégique, en raison de l'ampleur et la rapidité de l'impact sur les mœurs sociales et les pratiques criminelles.

Trois domaines étroitement liés à la personnalité de chaque citoyen sont, depuis plusieurs années, le champ privilégié où se développe une criminalité prospère :

Ce sont, d'une part, les atteintes à la vie privée, d'autre part, les violations des secrets légitimes, enfin, les discriminations.

La **vie privée** est, par définition, ce qui touche à l'intimité de chacun, que les lois pénales ont partout érigé en valeur dont la protection est essentielle à la vie en société.

Les institutions européennes et les institutions judiciaires nationales n'ont cessé, au fur et à mesure du déploiement généralisé des nouvelles technologies, de légiférer en posant le respect de la vie privée comme limite à la liberté de circulation et d'accès aux données.

Les nouvelles technologies ont fait émerger, en raison de leur facilité d'emploi, de stockage et de communication, la notion de données personnelles.

Les potentialités nouvelles de l'open data, qui marque une volonté forte de permettre un accès le plus large à un nombre de données de plus en plus nombreuses, ont en outre comme effet collatéral de multiplier les possibilités de violation de cet espace privilégié.

Ces violations ont pour particularité d'être le fait d'auteurs très divers, mus soit par le désir de nuire personnellement à des victimes précises, soit motivés par l'appât de profits illicites sans risques personnels.

En tout état de cause, les règles de conservation et de communication qui ont été déterminées par les directives successives de l'Union européenne doivent faire l'objet d'un suivi renforcé et du rappel de l'équilibre qui reste à trouver et à faire respecter entre le potentiel technique des outils numériques et les limites indispensables qui sont constamment à repréciser.

Un des impacts préoccupants de l'accessibilité grandissante des données personnelles est celui de la survie des **secrets légitimes** :

Certains secrets résistent à l'aspiration universelle à plus de transparence, dès lors qu'ils protègent des intérêts que la loi consacre comme essentiels aux équilibres de toute démocratie, comme le secret médical, le secret bancaire, le secret des cultes, le secret professionnel, celui des affaires ou encore le secret de la défense nationale.

Mais la fascination de notre société pour l'absence de contraintes, notamment dans l'accès à l'information quelle qu'elle soit, rend bien friables toutes les digues successives que la loi sur les secrets ne cesse d'édifier.

Il faut y ajouter la perplexité des juristes face aux arcanes des nouvelles technologies qui les font hésiter à appliquer à des techniques qui leur sont largement étrangères, des raisonnements juridiques conçus pour un monde non-numérique.

Comment, dès lors, se satisfaire de voir de véritables lignes Maginot juridiques sans cesse contournées par l'envahissante marée de données numériques ?

Comment ne pas avoir le tournis quand, chaque année, le monde numérique accumule plus de données que tout ce qui avait été rassemblé de connaissances depuis le début de l'Histoire ?

Notre question n'est-elle pas en réalité de savoir si la vie privée est soluble dans le « big data », et si « big brother » ne règne pas déjà sans partage sur le royaume du « cloud » ?

Le troisième domaine où la fluidité et le partage des données personnelles est devenu problématique est celui des **discriminations** :

Cette forme de criminalité avait été marquée dès le protocole additionnel de la Convention de Budapest comme un sujet clé pour l'usage des nouvelles technologies.

Les domaines concernés étaient et sont restés immenses et leurs victimes potentielles ou avérées sont aujourd'hui innombrables : propos haineux, sexistes, racistes dont la répression est largement incapable d'endiguer le flux.

Les premiers bilans des plateformes de signalement sur Internet ont montré à quel point l'intuition était juste tant le nombre des messages discriminatoires paraît en constante expansion.

Les institutions européennes doivent ici faire davantage pour assurer le respect effectif des lois nombreuses directement inspirées par les principes de la Convention européenne des Droits de l'homme.
Il conviendrait par exemple de généraliser les outils de prévention, de détection et de répression qui sont disponibles, et d'intensifier le dialogue avec les États, les associations habilitées à lutter contre toutes les formes de discrimination et les entreprises du Net, pour réduire les contradictions normatives en la matière et favoriser une coopération plus efficace.

Au total, les multiples atteintes aux personnes que l'usage incontrôlé du net, a fortiori quand il s'agit du « darknet » où la dérégulation est aujourd'hui la règle, imposent de ne pas céder à la résignation.

Si des constats simples ont pu être faits, leurs conséquences se sont complexifiées et doivent plus que jamais être traitées dans le cadre d'une stratégie globale de lutte.
L'examen des jurisprudences et des normes adoptées depuis l'adoption de la Convention de Budapest montre la récurrence de questions qui sont autant de thèmes d'étude et d'échanges à venir :

-un statut juridique de l'identité numérique est-il envisageable ?
-comment conjuguer protection de la vie privée et responsabilisation des utilisateurs ?
-l'inéluctabilité d'une connexion à Internet
-la traçabilité permanente
-le piège des profils personnels
-le contrôle incertain des données mises en ligne
-l'inadaptation des réponses classiques aux atteintes à la vie privée
-quel équilibre peut être satisfaisant entre protection de la vie privée et impératifs de l'ordre public ?

On le voit, les nouvelles technologies ont d'ores et déjà marqué un changement profond de la définition du droit à la vie privée.

Le rôle de la loi est de dire jusqu'à quel point le droit de savoir doit primer sur le droit à l'oubli. La légitimité discutée du secret montre à quel point le difficile équilibre entre liberté d'expression et protection de la vie privée est déterminant pour nos démocraties.

Le suivi à cet égard de la recommandation (2012)3 du Comité des Ministres du Conseil de l'Europe qui traite de la liberté d'expression dans ce cadre confrontée à l'existence de moteurs de recherches universels, pourrait être enrichi des parallèles à faire avec la réforme en chantier aux USA sur la neutralité du Net autour d'un projet de réglementation du Net proposé par la commission fédérale des communications pour tenter de favoriser le « neutrality net », sans qu'il soit encore possible de deviner si ce sont les internautes ou les fournisseurs d'accès qui en tireront le plus grand profit.

« La vie privée sera anormale » Vinton Cerf futurologue chez Google

3.2 Le crime organisé

Pour s'en tenir aux études les plus récentes, comme le Livre blanc sur le crime organisé transnational réalisé en octobre 2014 par le CDPC, la menace que font peser les 3600 groupes criminels recensés s'étend d'autant plus fort et plus vite que le recours aux cyber-outils est devenu ordinaire au sein de ces organisations.

L'évolution des données numériques de tous ordres et les facilités d'accès et de regroupement des données offertes par le développement récent de l'open data et du big data n'ont pas échappé aux criminels qui y trouvent, à la fois une plus grande latitude à exercer leurs activités illégales, à identifier les secteurs vulnérables et à blanchir leurs profits, avec un taux de risque pénal personnel considérablement plus faible que celui encouru dans les activités criminelles « classiques » .

Les typologies récemment proposées par Europol montrent l'importance de connaître la diversité des attaques et des attaquants, d'identifier là où se trouvent les principales failles de

sécurité et d'assurer une collecte et un traitement compatible avec les exigences du droit pénal européen.

Deux des contraintes les plus fréquemment rencontrées dans ces enquêtes sont la difficulté à surmonter l'anonymisation des flux et la porosité croissante des réseaux sociaux dont le détournement est devenu un cheval de Troie privilégié des cybercriminels.

Quatre secteurs sont particulièrement investis par ces groupes criminels protéiformes et doivent justifier des contre-mesures spécifiques :

C'est d'abord le domaine en pleine expansion des **fraudes aux paiements** dont l'origine et le mécanisme sont liés principalement à la récupération des données bancaires, leur revente ou leur manipulation.

Ces procédés illicites, généralement mis en œuvre à l'insu de leurs victimes, voient leur impact démultiplié par la généralisation des paiements par cartes bancaires, le succès de l'e-commerce et des instruments de stockage électroniques.

Le caractère international du champ d'activité de la criminalité organisée se prête parfaitement à l'organisation des captures de données financières et à leur recyclage instantané, compliquant gravement la traçabilité des flux et l'identification des auteurs, a fortiori lorsque les pays et les institutions concernés n'ont pas mis en place un dispositif de prévention réduisant les failles de sécurité et un système de coopération national et transnational opérationnel.

L'évolution d'un marché criminel de plus en plus poreux à l'égard du marché légal, compte tenu notamment de réinvestissements massifs possibles des profits criminels dans l'économie, ne peut que rendre vigilant sur la tentation exprimée cyniquement par certains d'intégrer les profits criminels dans le calcul des richesses nationales.

La créativité des groupes criminels en la matière, dont témoigne par exemple l'apparition récente de logiciels de type virus « ransomware », qui renouvelle et à grande échelle l'art du chantage financier devrait imposer la mise en place d'observatoires de nouvelles formes de fraudes numériques (comme l'usage de botnets) et la diffusion de typologies actualisées accompagnées de modes d'emploi pour les prévenir et les combattre.

Le domaine de la **Traite des êtres humains** est sans doute l'un des plus préoccupants, comme le montrent les études de plusieurs institutions comme l'OIT, qui montre en 2014 que le marché de la personne humaine, qu'il soit relatif à la prostitution, au travail forcé ou au trafic d'organes, dégage chaque année plus de 150 milliards d'euros de bénéfices.

L'ONUDC, qui en fait l'un des trafics les plus rentables, avec celui des stupéfiants, montre à quel point le recours aux nouvelles technologies a amélioré les perspectives de profit et la sécurité des trafiquants, que ce soit pour détecter les victimes, mais aussi les mettre en rapport avec les clients, organiser les actes d'exploitation et en blanchir les revenus.

Ces tendances préoccupantes, qui sont clairement identifiées au fil des rapports d'évaluation du GRETA, pourraient faire l'objet d'observations et d'analyses spécifiques dans les prochains mois.

L'exemple de la **contrefaçon** est également typique du versant pénal de l'utilisation principalement des sites de ventes en ligne qui mettent à la portée de tous, et partout, des objets contrefaits, mettant en péril, non seulement l'économie, mais de plus en plus la santé et la sécurité des consommateurs, comme la généralisation de la contrefaçon des médicaments et des pièces de rechange.

Ce marché très prospère n'est plus l'apanage de quelques « bricoleurs » individuels, mais est désormais géré comme un véritable marché criminel transnational avec le concours intéressé de sites de diffusion qui y trouvent leur compte en termes d'abonnements ou de publicité.

Il est donc nécessaire de mieux percevoir les enjeux et les réalités de ces atteintes massives aux droits de propriété intellectuelle, comme de progresser dans la mise à jour de règles plus effectives de responsabilité des intermédiaires d'Internet.

Le besoin de cette nouvelle régulation est d'autant plus impératif que la plupart des lois adoptées en la matière étaient plutôt tournées vers la répression du téléchargement illégal, avec un impact réel mais limité, laissant le champ libre aux groupes criminels, faute d'harmonisation des règles internationales.

L'exemple du **terrorisme** n'a pas manqué d'être relevé par nos démocraties qui, dans la lignée des mesures pénales prises après le 11 septembre et les attentats de Londres et Madrid, avaient commencé à envisager des procédures exceptionnelles proportionnées aux menaces.

Comme celles, comparables à celles qui ont été adoptées pour lutter contre la cyber-pédophilie, ces mesures prévoient des dérogations aux limites procédurales d'accès aux données privées et imposant aux opérateurs du Net un principe de précaution qui les responsabilise particulièrement.

Ni les institutions européennes, ni les États membres ne peuvent désormais sous-estimer le rôle que peut jouer l'Internet comme réseau de communication des terroristes et comme moyen de propagande.

Il ne leur est pas davantage permis aujourd'hui de sous-estimer les risques de cyber attaques, voire les cyber-guerres menaçant leurs intérêts fondamentaux.

La volonté de lutter plus efficacement contre le terrorisme moderne pose inévitablement la question du blocage des sites, qui se heurte, dans la pratique à l'extrême réactivité des internautes et à la possibilité qui leur est offerte d'utiliser les réseaux privés virtuels et de profiter des facilités du darknet.

Néanmoins, la démonstration de l'utilisation des plates-formes sociales pour faire le prosélytisme de leurs actions ouvre des perspectives de contre-mesure au moins en terme de surveillance.

L'ensemble de ces thèmes révèle un point commun, qui est l'universalisation et la diversification de l'activité des groupes criminels qui ne pourront être combattus efficacement sous le seul angle de l'espoir, très incertain, d'une future harmonisation des législations européennes et internationales.

Le salut, une fois encore, devrait plutôt être recherché dans la mise en place de formations d'équipes d'investigation spécialisées, d'un réseau opérationnel d'acteurs répressifs et d'experts européens, ainsi que dans la mise en exergue des résultats obtenus par la rédaction de guide de bonnes pratiques thématiques, dans la continuité des expériences actuellement menées autour d'Europol.

3.3 La sphère des mœurs et des loisirs

Il n'est pas surprenant que les nouvelles technologies aient particulièrement impacté les comportements humains les plus caractérisés par la recherche de la plus grande liberté possible, c'est-à-dire la sphère des mœurs intimes et celle des loisirs.

Le défi est à la mesure d'une réalité qu'alimente sans cesse la chronique des affaires judiciaires pénales qui montrent avec quelle facilité les limites légales peuvent être franchies par les citoyens ordinaires.

La difficulté pour le législateur est d'autant plus grande ici que la recherche du curseur entre les droits liés aux libertés fondamentales et les abus inadmissibles de cette liberté est délicate à faire aboutir.

Trois exemples peuvent illustrer ce décalage manifeste entre la norme pénale pourtant démocratiquement imposée et les comportements illicites qu'il convient de prévenir :

Le premier exemple est celui des **téléchargements** illicites qui sont particulièrement répandus dans l'espace économique européen pourtant très protecteur des droits liés à la production littéraire et artistique.

Les leçons qui peuvent être tirées des impacts des lois pénales en la matière invitent, d'une part, à réfléchir à des campagnes de sensibilisation à long terme sur le grand public, la simple menace répressive ayant eu à ce stade peu d'effet sur des consommateurs qui ne perçoivent pas leur action comme relevant du champ pénal.

D'autre part, à rechercher une stratégie globale à l'égard des acteurs de l'Internet et des titulaires de droits.

Le second exemple est celui des **jeux en ligne** qui, profitant de la multiplication des joueurs individuels sont de plus en plus exposés aux appétits du crime organisé déjà fortement investi dans le domaine des paris sportifs en ligne qui propose, via l'internet, l'accès à des « sites sauvages », dans un domaine où les législations nationales, communautaires et extra-communautaires sont hétérogènes.

Le dernier exemple est celui de la **« cyber sexualité** » qui a vu se multiplier les sites de rencontres tarifées qui banalisent les nouveaux « trottoirs du Net », devenus le nouvel eldorado de la prostitution.

Ceux-ci ne poseraient que la question générale des mœurs, qui ne peut être résumée à la question pénale, s'ils ne révélaient, au-delà la modification sensible des comportements humains, l'émergence de véritables infractions dont il est impossible de se désintéresser dès lors qu'elles touchent à des valeurs fondamentales, comme la protection des mineurs, cibles privilégiées des pédophiles comme des trafiquants d'êtres humains.

Tous ces exemples, une fois encore, montrent l'importance d'une réelle pédagogie de l'usage du net avec le rappel des valeurs communes susceptibles de justifier que la loi pénale cherche une limitation des libertés multiples offertes par la technologie.

3.4 Le monde de l'entreprise

Il est spécialement impacté par les nouvelles technologies, qu'il les produise, les gère ou les utilise, dans le même temps où il est l'objet d'une délinquance à visages multiples.

Les nouvelles frontières de la délinquance économique doivent faire l'objet d'une attention particulière pour espérer réduire l'impact désastreux pour nos économies :

Qu'il s'agisse des délits informatiques qui visent spécifiquement les systèmes technologiques utilisés par les entreprises, ou des délits de droit commun renforcés par les nouvelles technologies, les menaces actuelles sont considérables, qu'elles concernent les flux financiers illicites liés aux cartes de paiement prépayées, à la monnaie électronique ou virtuelle (les bitcoins par exemple), le trading haute fréquence qui rendent inopérants les contrôles effectifs.

Sont aussi liées au développement du numérique dans l'entreprise les atteintes au patrimoine informationnel, mais aussi les dérives liées aux relations de travail où sont posées avec la même acuité la question de l'intelligence économique ou celle de l'accès par l'employeur aux données personnelles de l'employé.

La vulnérabilité de l'économie largement numérisée est sans doute le prix à payer pour les gains de productivité que les nouvelles technologies ont permis de réaliser.

Pour éviter un jeu trop inégal entre des cyber délinquants libres de toute contrainte juridique et trop faiblement exposés aux rigueurs pénales, et des entreprises soumises aux légitimes contraintes légales de l'usage de ces technologies, l'objectif doit être de mieux cerner la voie étroite entre une dérégulation incompatible avec un véritable État de droit, et une pénalisation excessive (vraisemblablement inefficace) des rouages économiques.

4. Des acteurs inégalement concernés

La diversité des situations impactées et l'éparpillement des réponses normatives doivent inciter les États à recenser l'ensemble des acteurs concernés par la cybercriminalité pour rechercher les synergies et justifier les solutions spécifiques.

Les considérables différences d'intérêt et de positionnement d'acteurs si divers rendent d'autant plus nécessaires des initiatives transnationales favorisant la constitution d'observatoires et de groupes d'experts chargés de réfléchir aux connexions possibles pour bâtir des stratégies nécessairement pluridisciplinaires.

4.1 Les victimes d'infraction

Elles sont naturellement les premières concernées.Innombrables et inégalement averties des risques et des chemins à prendre pour s'en protéger, elles doivent être encouragées à mieux cerner les domaines principaux qui sont déterminants pour prévenir, réduire ou réparer leur vulnérabilité face aux dérives pénales associées aux nouvelles technologies.

Dans cette perspective, doivent être encouragées les politiques susceptibles d'encourager la détection de ces dérives, et de faciliter la prise de décision de porter plainte.

Un travail important reste à conduire sur la compréhension des conduites imprudentes qui caractérisent les usagers de ces technologies communicantes et des moyens d'élever sensiblement le niveau de vigilance de chacun.

Des échanges engagés au niveau européen doivent être amplifiés pour mieux appréhender les équilibres raisonnables entre les enjeux différents et contradictoires.

En outre, un inventaire des partenariats possibles avec les associations d'usagers et les institutions chargées des actions déontologiques publiques et privées doit conduire à mieux déterminer ce que devrait être une réparation effective et pertinente quand de telles infractions peuvent être sanctionnées.

4.2 Les acteurs répressifs

Ils sont en première ligne pour définir et réprimer les aspects pénaux en la matière.

L'adaptation du droit classique aux dérives pénales de l'Internet qui a été la première réaction des pénalistes, a montré ses limites et a conduit à l'élaboration d'un nouveau droit pénal, mais aussi d'une nouvelle procédure pénale.

L'ampleur des modifications législatives ne doit pas faire sous-estimer celle des comportements de ces acteurs, confrontés à la nouveauté de la compréhension, de la définition et de la détection de cette nouvelle délinquance.

Sur la base des efforts déjà entrepris, les orientations des mesures à prendre et à développer à l'égard de ces acteurs particuliers peuvent être résumées en quelques lignes directrices :

- poursuivre l'harmonisation des lois pénales spécifiques aux nouvelles technologies, notamment en s'assurant de la transposition effective des textes européens déjà adoptés,
- définir un cadre commun de principes directeurs sur les questions de compétence territoriale, de régime de prescription,
- généraliser l'adoption de circonstances aggravantes des infractions traditionnelles en cas de recours à ces technologies,
- développer les actions communes de formation et de spécialisation,
- constituer une base de données juridique des jurisprudences en la matière,
- donner aux organes de coordination pénale européens (EUROJUST, EUROPOL) des compétences spécifiques,
- favoriser les systèmes de lanceurs d'alerte et les procédures de signalement.

4.3 Les acteurs technologiques et le champ pénal

Le développement des nouvelles technologies a considérablement impacté les comportements publics et privés, mais il a également conduit à l'apparition de nouveaux métiers dont la culture juridique n'est pas la caractéristique la plus marquante.

Toutes ces nouvelles catégories d'acteurs technologiques sont cependant naturellement soumises à l'État de droit, quand bien même celui-ci peut sensiblement varier en fonction des territoires où ils sont nés et où ils sont basés.

Que ce soit les **opérateurs** qui gèrent les réseaux de communication, les **fournisseurs d'accès** qui proposent des informations et les acheminent, **les fournisseurs d'hébergement** qui détiennent et stockent ces données, les **éditeurs de contenu** qui mettent en ligne les données**, les éditeurs de logiciels** qui permettent l'usage de ces données, mais aussi les auteurs de blogs, les services spécialisés dans les réseaux sociaux ou les gestionnaires de plateformes de vente, tous doivent pouvoir s'appuyer sur des règles harmonisées, au moins à l'échelle européenne, qui définissent davantage leur rôle, leur statut et leur régime de responsabilité pénale.

Cet effort considérable qui est en cours est essentiel au regard de l'impératif de précision de la loi pénale comme le montrent les fluctuations actuelles des jurisprudences nationales ou transnationales en la matière.

Les exemples de la lutte contre le terrorisme ou la cyber-pédophilie montrent l'intérêt de conforter cette logique à deux vitesses, où les opérateurs sont partenaires pour lutter contre les formes les moins graves du détournement pénal des nouvelles technologies, mais sont tenus pour les formes les plus graves, à filtrer eux-mêmes les données suspectes, voire à être assujettis à une déclaration de soupçon dans les cas prévus par la loi.

La nécessité d'harmoniser le droit applicable aux prestataires techniques et de définir des protocoles de coopération avec les prestataires extracommunautaires s'en déduit en rappelant, comme une évidence, que ces négociations souvent déséquilibrées au regard de la nationalité et du poids économique de ces prestataires, ont tout intérêt à être conduites de manière unie et cohérente par les États européens.

La nécessité d'inciter à des partenariats cohérents entre les institutions publiques et les principaux opérateurs privés est perceptible partout, comme un prérequis à toute réponse pénale efficace, c'est-à-dire capable d'influer positivement sur les comportements illicites.

Mais si les trois grandes catégories d'acteurs concernés ont logiquement des regards différents sur les enjeux, il est possible d'envisager des réponses cohérentes entre elles qui reposent essentiellement sur une meilleure sensibilisation aux risques potentiels, une capacité de détection des menaces réelles, une mise en réseau des compétences aptes à les combattre et le choix de sanctions effectives.

4.4. Les auteurs d'infractions

Une quatrième catégorie d'acteurs, celle des **auteurs d'infractions** peut nous offrir un exemple paradoxal des objectifs à assigner aux lois pénales en matière de nouvelles technologies, si l'on considère la remarquable adaptabilité des auteurs traditionnels aux potentialités nouvelles, mais aussi l'émergence de nouvelles catégories d'auteurs, bien au-delà des « hackers » ou des « geeks » auxquels la cybercriminalité paraissait initialement réservée.

Enfin, le sentiment d'impunité qui est largement partagé parmi ces nouveaux criminels doit contribuer à motiver les partisans de l'État de droit à ne pas se résigner à l'insignifiance ou à la stérilité répressive dans un domaine certes complexe, mais dont les conséquences justifient qu'on les combatte sans relâche.

Il suffit de rappeler la considération selon laquelle la cyber criminalité, c'est avant tout de la criminalité, pour se convaincre de mobiliser les efforts utiles à la mise en œuvre d'une véritable politique criminelle européenne.

Celle-ci ne peut à l'évidence se contenter de renvoyer aux seuls principes du droit pénal, ni à la seule responsabilisation des opérateurs techniques.

C'est donc bien une politique spécifique à part entière qu'il convient d'encourager pour espérer un impact durable sur les phénomènes d'augmentation du nombre des cybercriminels, de diversification des domaines concernés et des victimes touchées.

5. Des réponses à réinventer

Le défi pour l'Europe est d'imaginer une réponse pénale aux nouvelles technologies qui conjugue réduction des pouvoirs étatiques et maintien d'un corpus juris commun minimal garanti par un pouvoir judiciaire compétent.

Le choix de mesures spécifiques, adaptées et proportionnées pour tenir compte de l'ambivalence du numérique implique un recensement des réponses éprouvées et une incitation à généraliser les bonnes pratiques labellisées.

L'intérêt de mesures évolutives et négociées est évident, compte tenu de la grande évolutivité des techniques et des comportements concernés.

L'expérience acquise depuis la mise en œuvre de la Convention de Budapest implique que soit repensé le rôle des acteurs publics et que le partenariat public/ privé et juriste/ technicien soit encouragé de manière volontariste.

En termes de stratégie européenne, les pistes à privilégier pour une adaptation réussie des règles de droit au risque pénal des nouvelles technologies invitent à définir une approche globale.

Celle-ci doit se faire autour d'idées complémentaires conjuguant et renforçant la sensibilisation du grand public, la prévention des principaux risques, la détection des infractions, l'investigation spécialisée, la détermination des responsabilités pénales, la répression dissuasive des faits avérés et la mise en place de réseaux de coopération judiciaire ad hoc.

Pour l'essentiel, ce recentrage pourra se faire à partir des institutions, des instruments et des expériences déjà en place dans l'espace européen dont l'évaluation globale pourrait être la première étape.

Un des exemples positifs qui peut être encouragé est la constitution par Europol d'une J-CAT (force d'intervention spécialisée pluridisciplinaire) qui favorise, sur le territoire européen et au-delà des concertations, des coordinations et des actions plus en rapport avec la complexité des cyber infractions transnationales.

De même, le renforcement du rôle des structures européennes d'entraide répressive pourra largement appuyer sur les initiatives en cours, au premier rang desquelles les structures pénales européennes Europol et Eurojust occupent une place déterminante en termes de recueil d'informations et de coordination des enquêtes transnationales.

En matière de cybercriminalité, les deux structures ont commencé à s'investir notamment dans les affaires complexes mettant en cause les nouvelles technologies.

Leur volonté de se doter de mécanismes protecteurs de leur propres données personnelles doit servir de modèle à tous les dispositifs chargés de « garder le gardien » afin de se prémunir de toutes les dérives que pourrait entraîner soit l'usage excessif de données personnelles, soit une transparence excessive dangereuse pour la sécurité des enquêtes.

Les impératifs qui devraient inspirer les stratégies à venir peuvent être ainsi résumés :

5.1 Légiférer

La dimension normative est intrinsèque à la matière pénale, mais doit conjuguer relecture et mise à jour des lois avec celles des recueils de bonnes pratiques.

C'est dans cet esprit que pourra être prolongée l'actualisation des dispositions de laConvention de Budapest et des textes européens subséquents.

Plus que d'une réécriture des lois de fond et de procédure, qui serait sans doute en décalage avec la rapidité et l'imprévisibilité de la technologie numérique, c'est plutôt une vérification permanente de la pertinence des principes posés il y a plus de 10 ans qui doit mobiliser les énergies juridiques européennes au regard des mutations à venir de la technologie et des délinquances qui lui sont attachées.

En matière procédurale, la feuille de route paraît clairement à rechercher par priorité à sécuriser les armes numériques mobilisées contre la cybercriminalité, à harmoniser les règles d'interception des données, d'infiltration numérique, de captation des données, de gel des données, de réquisitions numériques et de géolocalisation.

Une synthèse des législations européennes actuelles pourrait constituer, sur la base d'un questionnaire adressé aux pays membres, une source précieuse d'inspiration pour mieux définir les progrès normatifs qui restent à accomplir.

5.2 Connaître

Les observatoires européens et nationaux, publics et privés, doivent être encouragés et invités à définir en commun les définitions et les classifications des données utiles.

Il s'agit de mieux tirer parti des capacités de la nouvelle technologie :

- La traçabilité des systèmes a été un des points critiques dès le début de l'informatique.
  La mise en place de cette traçabilité a été un dilemme pour les informaticiens et les utilisateurs notamment quand il s'agit de déterminer les contraintes techniques, les temps de traitement et la capacité de stockage et contrôle.

- L'évolution des moteurs de recherche et leur vitesse de transmission, comme l'impact du Cloud sur les capacités de stockage le plan de la vitesse de transmission des données, de leur nature, de la capacité de stockage, du principe du « CLOUD ».

Cela doit conduire les Etats à mieux appréhender les questions de traçabilité, essentielles pour les investigations pénales, comme à tirer avantage de la masse accrue des données disponibles qui peuvent être autant de preuves recevables.

Cela peut se réaliser à grande échelle, dès lors que ces preuves respectent les principes nécessairement restrictifs de toute procédure pénale compatible avec les principes garantis par la Cour européenne des droits de l'homme.

À ce titre, il est indispensable d'établir un recueil des méthodes et des pratiques admissibles afin d'expliquer les processus dans la recherche de la preuve, qu'elle soit structurée, semi structurée ou non structurée.

Mieux maîtriser la technique nouvelle implique, du juge à l'expert en passant par le policier, une collaboration internationale mettant à disposition des outils pertinents, par exemple de surveillance et de capture des données.

Ces guides devraient par exemple être interactifs et en ligne afin de garantir leur évolutivité.

L'intérêt d'un **référentiel de l'expertise pénale** en matière de cybercriminalité est ici évident et doit être largement diffusé aux experts, aux enquêteurs comme aux juges ; dans le même esprit, des formulaires de mission d'expertise type favoriseraient grandement l'harmonisation et la sécurisation des enquêtes sur l'ensemble de l'espace européen.

5.3 Informer

Les actions de prévention adaptées aux différents acteurs doivent être généralisées sur la base de campagnes nationales européennes, internationales.

Le rôle spécifique du Conseil de l'Europe en la matière doit être souligné à différents niveaux :

Qu'il s'agisse de diffuser les actions et les méthodes qui ont été couronnées de succès,

Qu'il s'agisse de promouvoir des programmes d'études en lien avec les universités scientifiques pour anticiper et expliciter les avancées technologiques dans une perspective de risque pénal, mais aussi avec les universités de sciences humaines sur l'étude de l'évolution des comportements associés, et bien sûr avec les universités juridiques pour analyser les nombreuses incidences des nouvelles technologies sur les lois de fond ou de procédure.

Les institutions européennes pourraient, en outre, renforcer leur soutien, à travers des programmes spécifiques avec les écoles de formation des acteurs répressifs étatiques.

5.4 Réprimer

Des avancées sur les questions typiques de la dimension pénale des nouvelles technologies, telles que l'harmonisation de la définition des lois de fond et la mise en compatibilité des lois de procédures sont nécessaires à la concrétisation d'une réponse pénale effective.

Plus que l'écriture ou la réécriture des règles actuelles sur des questions qui restent très marquées par le principe de souveraineté comme par exemple la question de la compétence territoriale ou le choix pertinent, l'ambition pourrait être centrée sur la constitution d'un véritable catalogue européen des peines encourues et un fichier des peines effectivement prononcées en lien avec les casiers judiciaires des différents États.

Il reste également à définir un mode de communication, destiné aux opérateurs techniques comme aux utilisateurs sur l'existence et la consistance des peines prononcées.

5.5 Coopérer

L'identification des partenaires privilégiés est un préalable à toute pratique réussie de coopération internationale, particulièrement en matière d'entraide répressive où la confiance mutuelle et la vérification de procédures et de principes communs sont essentielles.

Les conditions d'une réussite reposent sur des principes éprouvés au sein des États membres.

Ils s'articulent autour de la mise en place de réseaux de professionnels dédiés, à l'image du réseau judiciaire européen, et d'exercices de formations communes qui peuvent, le cas échéant, sur des thématiques précises, être élargies à d'autres interlocuteurs comme les associations d'usagers, les organisations représentatives des professionnels des nouvelles technologies ou les réseaux universitaires

Les pratiques de coopération doivent aussi conjuguer approche multilatérale et approche bilatérale en gardant à l'esprit dans ce domaine particulier le risque de la dépendance technologique extracommunautaire pour le droit européen.
Pour y parvenir, il n'y aurait que des avantages à s'appuyer sur les actions du comité de la Convention sur la cybercriminalité, chargé du suivi de la Convention sur la cybercriminalité du Conseil de l'Europe, et son rôle de mise à jour des menaces de la cybercriminalité, de suivi de la Convention.

Le recensement nécessaire des initiatives des organisations internationales et du secteur privé dans le domaine de la cybercriminalité fait aussi partie des actions à mener à bref délai.

En résumé, les mesures adéquates raisonnables qui peuvent être envisagées à court terme (dans la continuité des instruments européens déjà en place) pour une meilleure maîtrise pénale des changements de comportements induits par les nouvelles technologies peuvent s'articuler autour de 3 axes principaux :

le premier qui vise à une meilleure sensibilisation des utilisateurs européens aux risques pénaux des nouvelles technologies et des bonnes pratiques permettant d'en réduire l'ampleur, notamment à l'aide d'observatoires et de plateformes de signalements,

le deuxième qui s'intéresse à une formation spécialisée des agents répressifs européens à partir d'outils de connaissance mutualisés, et de la constitution de réseaux d'échange et coopération opérationnels infra nationaux, inter-européens et internationaux, en privilégiant la recherche de partenariats public/privé,

le troisième qui privilégie des techniques d'évaluation mutuelle susceptibles de faire évoluer et d'harmoniser les pratiques et les cadres normatifs.

Conclusion

Depuis plus de vingt ans, nos sociétés ont accueilli la « révolution numérique » en saluant avec une ferveur qui ne se dément pas les extraordinaires perspectives de progrès qu'elles offrent à l'ensemble de nos comportements.

Comme souvent, l'existence a précédé l'essence, et ce n'est que progressivement que les limites et les dangers qui caractérisent ces nouvelles frontières ont commencé à être perçus.

Les lois pénales ont également commencé à jouer leur rôle d'accompagnement, de bornage et de sanction des dérives qui se sont faites jour.

Désormais, l'objectif est d'accélérer la construction d'un véritable espace répressif judiciaire européen numérique, d'en faire un lieu inhospitalier à la cybercriminalité.

Cela suppose de reconnaître que la société numérique a créé des droits et des devoirs nouveaux, et de veiller à ce que notre patrimoine juridique commun européen continue de jouer résolument son rôle de réflexion, d'anticipation et de régulation.

« Nous façonnons nos outils, et ceux-ci, à leur tour, nous façonnent. »
Marshall Mc Luhan, *Understanding Media, 1964*
("We become what we behold. We shape our tools and then our tools shape us.")