

***La protection de la vie privée à l'épreuve de l'extension des
pouvoirs d'enquête dans l'environnement numérique***

***Protection of privacy tested by expanding investigative powers
in the digital environment***

*MOSTEFAOUI Abdelkader

Doctorant

Faculté de droit/ Université d'Alger I

abdmosteafaoui285@gmail.com

<i>Date d'envoi : 21/12/2020</i>	<i>Date d'acceptation : 14/02/2021</i>	<i>Date de publication: 25/01/2022</i>
----------------------------------	--	--

Résumé :

L'émergence de la cybercriminalité n'a pu laisser indifférent le droit pénal processuel, dès lors que cette nouvelle forme de délinquance requiert l'adoption de règles de procédures adéquates, permettant d'étendre les investigations dans l'environnement numérique. A ce titre, notre dispositif juridique a adopté la surveillance des communications électroniques et la perquisition de systèmes informatiques, lesquelles techniques ciblent les contenus à caractère privé, que véhiculent les systèmes et réseaux informatiques. Les garanties entourant ces techniques, n'étant pas suffisamment mises en évidence, méritent une analyse discursive afin de révéler leur effectivité sur la protection de la vie privée.

Mots clés : *surveillance, interception, communications électroniques, perquisition, systèmes informatiques, garanties, vie privée.*

Abstract:

The emergence of cybercrime has not left the procedural criminal law indifferent, since this new form of delinquency requires the adoption of adequate procedural rules, making it possible to extend the investigations into the digital environment. As such, our legal system has adopted the surveillance of electronic communications and the search of computer systems, which techniques target private content, carried by computer systems and networks. The guarantees surrounding these techniques, not being sufficiently highlighted, deserve a discursive analysis in order to reveal their effectiveness on the protection of privacy.

Keywords: *surveillance, interception, electronic communications, search, computer systems, guarantees, privacy*

*MOSTEFAOUI Abdelkader

Introduction

L'avènement des sociétés de l'information, pur produit des technologies de l'information et de la communication a permis aux peuples d'améliorer considérablement la communication et le partage des informations en temps réel. L'accès facile à l'information et l'adhésion au débat mondial, encouragent la participation démocratique. Ces technologies puissantes laissent augurer un meilleur exercice des droits et libertés.

En même temps, l'introduction des technologies de l'information et de la communication dans la sphère du crime a offert aux délinquants une longueur d'avance qui a mis à nu les procédures de recherche et de constatation de la criminalité classique, et mis en défi, les autorités de justice et de police dans le monde, pour mener une lutte efficace contre de nouvelles formes de délinquance commises dans le cyberspace. Ce défi a été à l'origine d'initiatives juridiques cherchant à adapter les procédures de répression de la délinquance aux exigences de l'ère numérique.

Aussi, l'instrumentalisation politique de la peur a été d'une grande influence sur les politiques criminelles, qui ont introduit aisément le concept de sécurité nationale dans les textes de loi, suffisant alors pour justifier la redéfinition des contours de l'Etat de droit.

Il est clair aujourd'hui que ces nouvelles technologies risquent d'être utilisées pour la surveillance et l'interception électroniques. De récentes découvertes ont révélé que de nouvelles technologies sont développées secrètement, souvent pour faciliter ces pratiques. Ce type de surveillance représente une menace pour les droits individuels – y compris les droits à la protection de la vie privée et à la liberté d'expression et nuit au libre fonctionnement d'une société civile dynamique.

Les révélations d'Edward SNOWDEN en 2013 ont permis au monde entier de découvrir les pratiques auxquelles se livraient les services de renseignement américains « NSA : National Security Agency » consistant en des interceptions de masse, à travers l'accès direct dans les serveurs de neuf géants de l'internet, afin de surveiller et intercepter courrier électronique, partage de fichier, chat, ... aux fins de renseignement.

En décembre 2013, l'Assemblée générale des Nations Unies a adopté la résolution 68/167, dans laquelle elle a exprimé sa profonde inquiétude quant à l'impact négatif que pourrait avoir la surveillance et l'interception des communications sur les droits de l'homme. L'Assemblée générale a affirmé que les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne, et a invité tous les États à respecter et à protéger le droit à la vie privée dans le contexte de la communication numérique. Elle a également demandé à tous les États Membres de revoir leurs procédures, leurs pratiques et leur législation relatives à la surveillance et l'interception des communications, ainsi qu'à la collecte de données personnelles, et elle a souligné la nécessité pour les États de respecter pleinement toutes leurs obligations au regard du droit international des droits de l'homme.

Entre défenseurs de la cause sécuritaire et défenseurs des valeurs sociales du droit humanitaire, vient s'interposé en principe le droit qui définit le juste équilibre à même de permettre aux pouvoirs publics de disposer d'instruments juridiques à la hauteur de la menace, tout en préservant la vie privée, combien devenue vulnérable à l'ère du numérique.

A l'instar des autres pays du monde, notre société a subi de plein fouet la révolution des nouvelles technologies et ses répercussions sur l'évolution de la criminalité, non sans inciter le législateur à adopter de nouvelles dispositions juridiques à même de conforter les autorités de justice et de police dans l'accomplissement de la lutte contre la cybercriminalité. C'est ainsi qu'en 2009, fut promulguée la loi 09-04 portant règles particulières de prévention et de lutte contre la délinquance liée aux technologies de l'information et de la communication, adoptant deux techniques principales de recherche et de constatation des cyber-infractions, à savoir la surveillance des communications électroniques et la perquisition des systèmes informatiques.

Face à cette extension des techniques d'enquête dans l'environnement numérique, viendra se posée avec acuité, la question de la vie privée, dès lors que l'être humain a fait basculer des pans entiers de sa confidentialité vers les espaces numériques.

Les dispositions de la loi 09-04 dont sont issues les deux techniques sus évoquées, posent une dualité entre un cadre informel d'enquête prophylactique et le cadre des enquêtes et informations judiciaires prévues dans le code de procédure pénale, non sans laisser apparaître le sillage d'une norme juridique imprudente voire téméraire, ainsi que des zones d'ombre quant aux règles devant jalonner l'exécution de ces techniques.

En matière de surveillance des communications électroniques ladite loi reconnaît l'enquête prophylactique justifiant l'exécution de la surveillance des communications pour des impératifs liés à l'ordre public. L'approche anticipative que renferme cette technique, bien qu'elle accepte une justification par souci d'efficacité, révèle les prémices d'une modification profonde dans notre dispositif juridique.

Les autres cadres permettant le recours à la surveillance des communications, ainsi qu'à la perquisition des systèmes informatiques posent quant à eux des ambiguïtés induites d'une conciliation indisponible, avec les dispositions du code de procédure pénale, afin de garantir une protection des droits liés à la vie privée.

Dans cet article, il sera question de savoir si le législateur a prévu un régime spécial des garanties de protection de la vie privée face à l'extension des pouvoirs d'enquête dans l'environnement numérique ou bien s'est-il contenté de celles déjà prévues dans le code de procédure pénale. Le terme enquête est usité dans un sens large, comprenant l'enquête au sens du code de procédure pénale et l'enquête prophylactique. La réponse à ces questionnements se fera selon une approche analytique, à travers deux chapitres, concernant respectivement ; la protection de la vie privée face à la surveillance des communications électronique I et la protection de la vie privée face à la perquisition des systèmes informatiques.

I-Protection de la vie privée face à la surveillance des communications électroniques

Les correspondances privées, sont protégées par la constitution, qui affirme garantir aux citoyens la confidentialité des correspondances dans le chapitre des droits et libertés, en vertu de son article 46 alinéa 1 (article 47-2

du projet de constitution de 2020). Toute atteinte à ce principe constitutionnel se trouve réprimée par l'article 303 du code pénal.

Néanmoins, ce principe est soumis au régime dérogatoire¹, tenant aux nécessités de la lutte contre la criminalité dite grave, que le droit processuel y consacre le régime particulier lié aux techniques spéciales d'enquête. En ce sens, l'article 65 bis⁵ alinéa 1, confère aux officiers de police judiciaire le recours, sur autorisation du magistrat compétent, si les nécessités de l'enquête l'exigent², à l'interception des correspondances émises par voie de télécommunication.

Après l'avènement de la révolution des technologies de l'information et de la communication, les réseaux ont offert d'importantes capacités de diffusion d'informations sous forme numérique, tels que textes, images et vidéo, opportunités que les criminels saisissent pour commettre leurs forfaits. Dans ce contexte, il est apparu nécessaire pour les services d'application de la loi de s'orienter vers l'espace virtuel pour suivre les traces des criminels et apporter la preuve la plus adaptée à la nature de la criminalité contemporaine.

En adoptant la surveillance des communications électroniques, la loi 09-04 définit celles-ci comme étant « toute transmissions, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature, par tout moyen électronique ».

Elles comprennent les données circulant d'un système informatique vers un autre sous diverses formes compréhensibles par l'être humain tels que ; écrits, sons, images, signaux....etc. ou toute forme de communication³, que l'on désigne aussi de données de contenu par opposition aux données du trafic. Au sens de la convention de Budapest sur la cybercriminalité, on entend par données relatives au contenu ; « le contenu informatif de la communication, c'est-à-dire, le sens de la communication, ou l'information véhiculée par la communication, tout ce qui est transmis dans le cadre de la communication en dehors des données relatives au trafic »⁴. Les données du trafic, quant à elles, sont des données de connexion au réseau qui permettent d'identifier l'auteur du message.

Cette définition inclut aussi, les communications téléphoniques dès lors que celles-ci sont constituées de communications sonores transmises par des systèmes électroniques, après avoir basculé du mode analogique au mode numérique⁵.

Le procédé de surveillance des communications consiste à la mise en place de dispositif technique permettant la collecte et l'enregistrement en temps réel du contenu des communications électroniques (article 3 de la loi 09-04). Si la loi ne différencie pas entre communication privée et communication publique, il demeure entendu que c'est le caractère privé de celle-ci, étant protégée par la loi, qui a motivé l'instauration du régime dérogatoire autorisant la violation de ce droit, or, un tel dispositif juridique serait inutile pour la surveillance de communications publiques.

Ne constitue donc pas une interception des communications le fait de se connecter au réseau de communication et sans modification préalable de l'installation, pour lire ce que n'importe quel utilisateur peut lire⁶. Il s'agit de collecter les données échangées dans un cadre privé, entre deux ou plusieurs personnes. Le caractère privé de la communication est déduit de deux éléments, à savoir ; l'aspect personnel du contenu de la communication et la volonté de l'expéditeur de n'en divulguer son contenu qu'aux destinataires exclusivement déterminés⁷.

Il convient d'aborder ci-après, le champ d'application de la surveillance des communications électroniques pour ensuite analyser les garanties entourant cette procédure.

1- Délimitation du champ d'application de la surveillance des communications électronique :

La surveillance des communications électroniques telles que régie par la loi 09-04 du 05/08/2009, consiste à intercepter des communications émises sur un réseau de communication électronique, dans un but préventif ou répressif à l'encontre de la délinquance liée aux technologies de l'information et de la communication.

Dans son article 3, la loi susvisée délimite le champ d'application des mesures instaurées par ce texte législatif, aux impératifs de protection de

l'ordre public (a) ou pour les besoins des enquêtes et informations judiciaires (b), ce qui nous amène à aborder ces domaines à travers les titres suivants.

a-Usage préventif justifié par l'Impératif de protection de l'ordre public

Selon le paragraphe (a) de l'article 4 de la loi 09-04, il peut être recouru à la surveillance des communications électroniques pour prévenir les infractions qualifiées d'actes terroristes ou subversifs et les infractions contre la sûreté de l'Etat.

Il s'agit donc de mettre en place un dispositif technique pour intercepter les communications échangées entre des personnes dans un cadre privé, pour « ...prévenir les infractions... » autrement dit pour empêcher la commission d'infractions qualifiées d'actes terroristes ou subversifs et les infractions contre la sûreté de l'Etat et non pour constater des infractions consommées, en collecter les preuves et rechercher les auteurs présumés.

Le paragraphe (b) de l'article 4 de la loi 09-04 prévoit également un recours à la surveillance des communications électroniques lorsqu'il existe des informations sur une atteinte probable à un système informatique représentant une menace pour l'ordre public, la défense nationale, les institutions de l'Etat ou l'économie nationale.

Ce cas s'inscrit également dans le cadre informel relatif à la prévention, dès lors qu'il s'agit de recourir à la surveillance des communications pour empêcher une infraction dont la commission est probable, en l'occurrence une atteinte à un système informatique représentant une menace pour l'ordre public, la défense nationale, les institutions de l'Etat ou l'économie nationale, et non un acte d'enquête visant une infraction consommée.

Il appert clairement que le cadre dans lequel s'effectue la surveillance préventive des communications électroniques est un cadre méconnu du dispositif classique de procédure pénale, soit une première exceptionnalité du genre dans notre droit processuel où l'on admet le recours à une telle technique, combien portant atteinte à la vie privée par la violation du secret des correspondances, en dehors du cadre des enquêtes et informations judiciaires consécutives à la commission d'infraction, mais antérieurement à l'infraction.

Cette mesure allant au-delà des normes classiques du droit, signifie elle une tendance vers l'acceptation d'un droit pénal de l'ennemi ou alors une stricte application du principe d'efficacité du droit pénal ?

Selon la théorie du droit pénal de l'ennemi, dont le fondement est posé par le professeur de droit pénal à l'université de Bonn/Allemagne GUNTHER Jakobs, la lutte contre le terrorisme justifie le recours aux règles dérogatoires de droit, conférant aux services de l'Etat des prérogatives « déchainées » allant au-delà des limites du respect des droits. Dans un tel régime l'auteur d'actes terroristes perd son statut de personne, dès lors que son acte constitue une grave violation de son rôle social⁸. Il s'agit comme son nom « ennemi » l'indique de règles de droit orientées sur la personne du coupable et non sur le fait criminel. C'est donc la négation du statut de personne pour le criminel auteur de certaines catégories graves de criminalité, dont le terrorisme, qui constitue le fondement du droit pénal de l'ennemi, combien même allant à l'encontre de nombreux principes constitutionnels.

Depuis la seconde guerre mondiale, les questions de terrorisme sont traitées dans les sociétés démocrates selon les normes de procédures du droit pénales, faisant du terrorisme un criminel, nonobstant le caractère dérogatoire des procédures législatives de l'antiterrorisme. Or, l'on constate qu'une rupture serait intervenue depuis les dernières décennies, manifestement depuis les attentats du 11 septembre 2001, où l'on a commencé à considérer le terroriste comme un ennemi et non un criminel, et partant accepter d'introduire dans le régime juridique des changements profonds, en contradiction avec l'Etat de droit⁹.

Après l'Allemagne, les contours d'un droit pénal de l'ennemi ont été remarqués dans le droit espagnol, dans sa partie consacrée à la lutte contre le terrorisme de l'ETA, et le droit colombien faisant face aux cartels de la drogue, caractérisant un accroissement des mesures proactives et la suppression d'une partie des garanties procédurales, alors qualifiées d'intrusion du politique dans le juridique. Vient ensuite les USA, à partir de 2001, où l'on a adopté l'approche de guerre contre le terroriste « ennemi » dans les procédures policières et judiciaires, ensuite l'Europe à partir de la moitié de la décennie 2000-2010, avec les mesures de lutte contre le

terrorisme notamment la rétention de sûreté, le gel des avoirs et les nouvelles pratiques de surveillance.

Sur un autre registre, il importe de rappeler que l'une des marques caractéristiques du droit pénal est la menace de sanction ultérieure, par opposition au droit de la police qui se caractérise par la prévention a priori, or, il existe des normes de sanction pénale d'actes dépourvus de résultat criminel, tel que la sanction de l'entente de constituer une entreprise criminelle. Il est en effet question d'efficacité, l'un des principes caractérisant le droit pénal, selon lequel « ...un droit pénal qui ne pourrait agir que lorsque une infraction à la loi a déjà eu lieu perdrait toute crédibilité¹⁰ » et c'est selon ce principe d'efficacité qu'il est admis que l'Etat doit avoir, en cas de menace d'une grave violation du droit, la possibilité d'agir pour éviter la réalisation de cette menace. C'est aussi sous ce principe d'efficacité qu'est admise la sanction de la tentative, par crainte d'une perte de maîtrise de la situation à partir du point où il devient impossible de contrôler la suite des événements.

Dans notre droit pénal, il est totalement admis, en vertu du principe d'efficacité du droit pénal, l'incrimination de la création d'un groupe dont le but revêt un caractère terroriste (article 87bis3 du code pénal, le voyage à l'étranger dans le but de participer à des activités terroristes (article 87bis11 du CP) l'association de malfaiteurs (article 176 du code pénal), la mise en danger de la vie d'autrui (article 290 bis du CP). Il s'agit d'infractions « obstacles » ou infractions de prévention, consistant à sanctionner un comportement dangereux, sans dommage, pour éviter la commission d'infractions éventuelles¹¹.

A ce titre, l'anticipation de la culpabilité, tel que voulue par souci d'efficacité du droit, ne saurait justifier l'existence d'un droit pénal de l'ennemi.

En outre, l'apparition de menaces et dangers ont justifié les modifications structurelles dans la procédure pénale, donnant lieu à des mesures telles que les interceptions de communications, la vidéo surveillance, l'écoute de domiciles et lieux privés, la conservation des traces de connexion

en ligne et la perquisition d'ordinateurs, laissant apparaître une fusion de la prévention avec la répression dans un même système de poursuite.

Il demeure entendu que de telles mesures relèvent du droit procédural qui s'intéresse à l'infraction et non à l'auteur, principal objectif du droit pénal de l'ennemi, et donc ne sauraient justifier l'existence d'un droit pénal de l'ennemi, auquel s'ajoute le fait que notre dispositif judiciaire ouvre la porte aux délinquants pour un retour à la société, contrairement à un droit pénal de l'ennemi qui écarte totalement cette hypothèse, car considérant le criminel de « non personne », à exclure de la société¹².

Si l'hypothèse du droit pénal de l'ennemi ne semble pas tenir pour les raisons sus évoquées, la crainte de voir le sécuritaire se substituer à l'Etat de droit, est totalement légitime, d'où il appartient aux juristes et aux universitaires de démasquer toute dérive dans notre législation, allant à l'encontre des fondements de l'Etat de droit.

Il demeure entendu que la surveillance préventive des communications électroniques doit demeurer difficilement admissible dans notre dispositif juridique, s'agissant d'une technique attentatoire à la vie privée, autorisée à titre anticipatif, en dehors des cadres d'enquête reconnus en droit pénal processuel.

b-Usage pour le besoin des enquêtes et informations judiciaires

Le droit de procédure pénale est réputé droit des libertés, car composé de règles limitant l'action des autorités investies de pouvoirs d'enquête et de poursuite, contre les atteintes aux droits et libertés, en définissant les cas et modalités permettant de restreindre ces libertés, afin de maintenir un juste équilibre, justifié par l'intérêt de dévoiler la vérité liée à un trouble social, là où il devait tolérer des mesures restrictives, telles que mise en garde à vue, perquisition de domicile, détention provisoire...etc¹³.

Dans ce sillage, les techniques d'enquête extraordinaires constituant des atteintes sévères aux droits et libertés et qui dérogent aux règles communes, sont tolérées dans un souci de réprimer efficacement la criminalité organisée, elle-même considérée extraordinaire eu égard à sa gravité et la complicité de ses modes opératoires.

Ainsi, avant la promulgation de la loi 06-22 du 20/12/2006, le code de procédure pénale contenait des dispositions réparties dans différents titres concernant les délais de garde à vue en matière de terrorisme et d'atteinte à la sûreté de l'Etat (art 51-5CPP), ainsi que pour les heures légales de perquisition des lieux de débauche, et en matière de trafic de drogues (art 47-2) et de terrorisme.

Après la promulgation de la loi 06-22 du 20/12/2006 le législateur devait étendre le champs du régime dérogatoire à d'autres formes de criminalité, dans un souci de donner plus de cohérence en matière d'investigation, tout en limitant ce régime à certaines infractions, considérées graves et/ou organisées, et ce à titre exclusif¹⁴.

Le législateur n'a pas défini la criminalité dite « grave » objet du régime dérogatoire en fonction de ses caractéristiques¹⁵, alors qu'il a opté pour la définition objective consistant à énumérer limitativement les infractions auxquelles s'applique ce régime.

L'interception des correspondances dans le cadre des enquêtes et informations judiciaires a été adoptée dans notre droit en vertu de la loi 06-22 du 20/12/2006 modifiant et complétant le code de procédure pénale, qui stipule dans l'article 65bis 5 que les officiers de police judiciaire peuvent sur autorisation du procureur de la République, dans le cadre des enquêtes préliminaires et de flagrance, ou du juge d'instruction dans le cadre des informations judiciaires, recourir à l'interception des correspondances émises par voie de télécommunications, où mettre en place un dispositif technique ayant pour objet la captation la fixation la transmission et l'enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel dans des lieux privés ou publics, ou de l'image d'une ou plusieurs personnes se trouvant dans un lieu privé.

Ces techniques sont réservées exclusivement à la recherche d'infractions déterminées, à savoir celles relatives au trafic de drogues, de crime transnational organisé, d'atteinte aux systèmes de traitement automatisé de données, de blanchiment d'argent, de terrorisme, d'infractions relatives à la législation des changes, aux infractions de corruption et de contrebande

(articles 33 et 34 de l'ordonnance 05-06 relative à la lutte contre la contrebande).

De l'avis de certains auteurs¹⁶, cette technique constitue une mesure déchainée, du fait de son admissibilité durant l'enquête préliminaire basée elle-même sur le soupçon, qui ne saurait justifier de telles atteintes à la vie privée. A titre comparatif, la législation française confère aux seuls magistrats de l'instruction, l'autorisation d'une interception de communication, ce qui exclut son usage lors des enquêtes préliminaire et de flagrance¹⁷.

Il importe de rappeler que la promulgation de la loi 06-22 du 20/12/2006 modifiant et complétant le code de procédure pénale dont sont issues les dispositions supra évoquées, est venue exprimer la transposition des dispositions de la convention des nations unies pour la lutte contre le crime organisé transnational, adoptée le 15/11/2000, que l'Algérie a ratifiée en vertu du décret présidentiel n° 02-55 du 05/02/2002, incitant dans son article 20, les Etats parties à adopter dans leur droit interne, des dispositions permettant le recours aux techniques spéciales d'investigation.

En 2009, et dans une démarche d'adaptation de notre arsenal procédural avec les exigences de la lutte contre la cybercriminalité, le législateur algérien a adopté la surveillance des communications électroniques comme nouveau mode d'obtention de preuves, dans le cadre des enquêtes et informations judiciaires.

Selon le paragraphe (C) de l'article 4 de la loi 09-04, le recours à la surveillance des communications électroniques est envisagé pour les besoins des enquêtes et des informations judiciaires, sans pour autant définir les modalités d'exécution de cette technique. S'agissant de cadre d'enquête régi par le code de procédure pénale, il est admis que les dispositions dudit code s'appliquent pour ce cas, à travers une transposition des procédures relatives à l'interception des correspondances prévenues à l'article 65 bis 5, s'agissant de procédés similaires.

Néanmoins, une ambiguïté de taille apparaît, lorsqu'il s'agit de concilier le code de procédure pénale et la loi 09-04 en matière de champ d'application de l'interception des communications électroniques. En effet,

l'article 65bis 5 du CPP limite la technique d'interception aux infractions relatives au trafic de drogues, de crime transnational organisé, d'atteinte aux systèmes de traitement automatisé de données, de blanchiment d'argent, de terrorisme, d'infractions relatives à la législation des changes, aux infractions de corruption et de contrebande.

Or, à la lecture de l'article 3 de la loi 09-04, définissant le champ d'application de ladite loi, il appert que la surveillance des communications électroniques s'applique aux infractions liées aux TIC, elles-mêmes définies comme étant les atteintes aux systèmes de traitement automatisé de données, prévues dans le code pénal et toute autre infraction commise ou dont la commission est facilitée par un système informatique ou un système de communication électronique.

Cette disposition est de nature à élargir, sans limite, le champ d'application de la surveillance des communications électroniques, y compris celle de moindre gravité, telle que la diffamation via les réseaux sociaux, l'une des infractions les plus répondues sur la toile. Une telle disposition serait alors contraire au principe appliqué au régime dérogatoire selon lequel les actes d'enquête revêtant un caractère dérogatoire de par l'atteinte qu'elles constituent sur les droits, sont limitativement appliquées à un éventail rétréci d'infractions graves, de manière à trouver un compromis entre la préservation des droits et libertés proportionnellement avec la nécessité de trouver les moyens adéquat à la lutte contre la criminalité grave menaçant les intérêts de la société, principe constituant une des garanties devant entourer le régime dérogatoire¹⁸.

La surveillance des communications électroniques peut être également exercée dans le cadre de l'exécution des demandes d'entraide judiciaire internationale, tel que stipulé au paragraphe (d) de l'article 4 de la loi 09-04. Ainsi il est envisageable de recevoir des commissions rogatoires internationales, prescrivant l'enregistrement en temps réel de communications électroniques, ou alors des demandes d'entraide judiciaire en application d'éventuels accords ou conventions avec le pays demandeur.

A ce titre, en adhérant à la convention Arabe de lutte contre la cybercriminalité, les autorités algériennes sont tenues de fournir et demander

aux autres pays ayant ratifié la convention, l'entraide en matière de collecte en temps réel de données transmises par voie électronique, tel que stipulé dans l'article 42 de ladite convention. La même obligation est applicable en faveur de notre pays.

2-Garanties entourant l'utilisation de la surveillance électronique

Comme toute procédure dérogatoire constituant une atteinte aux droits et libertés, la surveillance des communications électroniques est entourée de garanties issues principalement d'un contrôle renforcé par l'autorité judiciaire et des règles qui jalonnent son exécution.

a- Une procédure soumise à autorisation judiciaire

Dans un souci de trouver un équilibre entre la nécessité du recours au régime dérogatoire, renfermant des mesures contraignantes qui s'opposent à certains droits, dont certains font l'objet d'une protection constitutionnelle, tel que le secret des correspondances, le législateur a imposé des mesures renforcées du contrôle que doit exercer l'autorité judiciaire lors de l'exécution du régime dérogatoire.

Il convient de rappeler dans ce contexte que le conseil constitutionnel Français, a imposé à l'autorité judiciaire d'exercer ce contrôle sur l'exécution du régime dérogatoire en statuant ainsi « Considérant qu'il résulte de l'ensemble de ces dispositions que, si le législateur peut prévoir des mesures d'investigations spéciales en vue de constater des crimes et délits d'une gravité et d'une complexité particulières, d'en rassembler les preuves et d'en rechercher les auteurs, c'est sous réserve que ces mesures soient conduites dans le respect des prérogatives de l'autorité judiciaire gardienne de la liberté individuelle et que les restrictions qu'elles apportent aux droits constitutionnellement garantis soient nécessaires à la manifestation de la vérité, proportionnées à la gravité et à la complexité des infractions commises et n'introduisent de discriminations injustifiées ; qu'il appartient à l'autorité judiciaire de veiller au respect de ces principes, rappelés à l'article préliminaire du code de procédure pénale, dans l'application des règles de procédure spéciales instituées par la loi. »¹⁹

C'est ainsi que toutes les mesures prises dans le cadre exceptionnel du régime dérogatoire doivent emporter l'accord de l'autorité judiciaire

compétente. S'agissant de la perquisition en dehors des heures légales et la prolongation des délais de garde à vue au-delà des périodes initiales, une autorisation du Procureur de la République ou du juge d'instruction est obligatoirement sollicitée, conformément aux principes généraux.

Ainsi, le recours aux techniques spéciales d'investigation telles que l'interception des correspondances, il est impérativement exigé une autorisation préalable du Procureur de la République ou du magistrat instructeur, sous peine de nullité de la procédure y afférente.

En France, en application de la décision du Conseil constitutionnel susvisée, l'OPJ doit soumettre en outre au Procureur de la République la qualification dérogatoire qu'il envisage, suffisamment argumentée des éléments de faits et de droit, afin d'être validée, avant de mettre en œuvre les articles d'enquête propre à ce régime²⁰.

a.1-autorisation judiciaire de la surveillance préventive :

S'agissant de la surveillance préventive des communications électroniques, le législateur a conféré au seul procureur général près la cour d'Alger le pouvoir d'autoriser la mise en œuvre de la surveillance prévue au paragraphe (a) de l'article 4 de la loi 09-04, pour une durée de 6 mois renouvelable. Ce procédé qui déroge à la règle, à savoir le transfert de ce pouvoir d'autorisation, du procureur de la république et du juge d'instruction au procureur général près la Cour d'Alger trouve justificatif dans le fait que les OPJ relevant de l'organe national de prévention et de lutte contre la criminalité liée aux TIC, exclusivement habilités à exécuter ce type de surveillance élisent résidence à Alger, auquel s'ajoute le caractère informel du cadre dans lequel est opérée l'opération, ne donnant compétence à aucune juridiction selon les formes classiques.

A la différence du cas prévu au paragraphe (a) de l'article 4, le cas visé dans le paragraphe (b) soulève des questionnements quant à l'autorité judiciaire habilitée à autoriser le recours à la surveillance, dès lors que les règles de compétence ordinaire ne sont pas réunies.

Un raisonnement par analogie²¹ est entièrement admis dans pareil cas, en ce sens que le Parquet général d'Alger demeure seul compétent en la matière, étant donné qu'il s'agit de procédé similaire « cadre préventif ». Ce

raisonnement est d'autant onforté du fait que les OPJ relevant de l'organe susvisé demeurent exclusivement habilités à opérer la surveillance préventive visée aussi bien au paragraphe (a) (pour des impératifs liés au terrorisme et atteintes à la sûreté de l'Etat) que le paragraphe (b) (impératifs de l'ordre public), en vertu d'une disposition de « ratrapage » contenue dans le décret présidentiel n°15-261 du 08/10/2015 portant composition, organisation et fonctionnement de l'organe national de prévention et de lutte contre la criminalité liée aux TIC.

a.2-autorisation judiciaire de la surveillance dans le cadre des enquêtes et informations judiciaires

Dans le cadre des enquêtes et informations judiciaires, les OPJ peuvent recourir à la surveillance des communications électroniques, après avoir dument obtenu l'autorisation soit du procureur de la République pour le cas d'enquête soit du juge d'instruction pour le cas de l'information judiciaire, reste à s'interroger sur la période fixée dans cette autorisation. Celle de 04 mois fixée dans l'article 65bis 5 du CPP semble la plus plausible, en écartant la période de 6 mois fixée pour la surveillance préventive (article 4, paragraphes A et B de la loi 09-04), car se rapportant à un cadre totalement différent de celui prévu dans le CPP.

Il importe de souligner que l'autorisation de l'autorité judiciaire d'une durée de validité de 6 mois pour la surveillance préventive et 4 mois pour la surveillance consécutive aux enquêtes et aux procédures d'entraide judiciaire peut être renouvelée sans limite, d'où il appartient au magistrat autorisant cette technique d'apprécier l'opportunité de son renouvellement. En droit français, l'autorisation d'interception est renouvelable une seule fois. Un tel plafonnement est de nature à renforcer les garanties entourant la mesure de surveillance des communications.

Par ailleurs, il convient de souligner que le formalisme lié à l'autorisation de l'autorité judiciaire n'est nullement indiquée, s'agissant de surcroit de cause de nullité. Il est ainsi admis de transposer les mêmes conditions de forme prévues pour l'autorisation judiciaire relative à l'opération d'infiltration régies en vertu de l'article 65bis 15, à savoir une autorisation écrite et motivée, mentionnant l'infraction ayant justifié le

recours à la surveillance et l'identité de l'OPJ devant exécuter la surveillance²².

b-Des garanties liées à l'exécution de la surveillance électronique

b.1-Les garanties tirées de la qualité des personnes habilitées à exécuter la surveillance

Dans le contexte de la surveillance préventive prévue au paragraphe A de l'article 4 de la loi 09-04, seuls les OPJ relevant de l'organe national de prévention et de lutte contre les infractions liées aux TIC²³ sont habilités à procéder à la surveillance sus-évoquée.

Or, la surveillance préventive opérée dans le but de prévenir des atteintes probables à un système informatique représentant une menace pour l'ordre public, la défense nationale ou l'économie nationale semble être épargnée de cette mesure imposée à la surveillance prévue au paragraphe A de l'article 4 de la loi 09-04.

En ce sens, la loi 09-04 est silencieuse en ce qui concerne les OPJ habilités à exécuter cette surveillance. Cette inadvertance semble être rattrapée au terme du décret présidentiel 15/261 du 08/10/2015 fixant la composition, l'organisation et les modalités de fonctionnement de l'organe national de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication. En effet, il est stipulé dans l'article 11 dudit décret présidentiel que la direction de la surveillance préventive relevant de cet organe est chargée entre autres de l'exécution des opérations de surveillance préventive des communications électroniques en vue de relever les infractions liées aux technologies de l'information et de la communication sur autorisation écrite de l'autorité judiciaire et sous son contrôle conformément à la législation en vigueur.

Pour les deux autres cas de surveillance, la compétence en matière d'exécution de cette technique revient aux OPJ territorialement compétents selon les formes prévues dans le code de procédure pénal

b.2-Les garanties tirées des dispositions explicites du code de procédure pénale

Les opérations de surveillance sont dirigées exclusivement pour la prévention et la lutte contre le terrorisme et les atteintes à la sûreté de l'Etat,

sous peine de sanctions pénale en matière d'atteinte à la vie privée. Il s'agit là de faire appel à l'article 303bis du code pénal.

Aussi, à la différence de la surveillance prévue au paragraphe (a), celle prévue au paragraphe (b) semble être écartée des dispositions de mise en garde quant à l'usage des données y obtenues, en dehors du cadre pour lequel l'opération de surveillance a été réalisée. Cette inadvertance peut être résorbée à travers un raisonnement par analogie, appelant à l'application de la même disposition de mise en garde, soit le recours aux sanctions relatives à l'atteinte à la vie privée.

Quant aux deux autres cas de surveillance, il demeure entendu que les sanctions prévues pour violation du secret de l'enquête ou de l'instruction s'appliquent pour tout usage des données obtenues de la surveillance en dehors de la procédure en cours.

II-La protection de la vie privée face à la perquisition des systèmes informatiques

La perquisition des systèmes informatique est l'une des principales procédures adoptée par la loi 09-04 en matière de lutte contre la cybercriminalité, laquelle est venue étendre le champ des investigations à l'environnement numérique. Il est question, ci-après d'examiner la nature de cette procédure par rapport à la perquisition déjà prévue dans le droit de procédure, pour ensuite aborder les garanties entourant son exécution.

1-La perquisition des systèmes informatiques : acte nouveau ou acte aménagé ?

La perquisition du système informatique est une procédure d'enquête insérée dans notre arsenal processuel au terme de la loi 09-04, du 05/08/2009, dans son article 05. Cette disposition a été instaurée pour faciliter les recherches et constatations des infractions liées aux Technologies de l'information et de la communication.

Néanmoins, aucune définition n'est donnée à cette technique, ce qui nous amène à rappeler des dispositions existantes dans le droit procédural. En effet, seule la perquisition du domicile est jalonnée de règles de procédure par souci de trouver un équilibre entre l'inviolabilité du domicile et la nécessité de réprimer la délinquance.

a-La perquisition au sens du code de procédure pénale :

La perquisition de latin « perquitio-onis et perquirere » signifie chercher avec soin ou chercher dans un endroit clos²⁴. En droit pénal, la perquisition consiste en un acte d'enquête visant la recherche d'indices ou de pièces à conviction utiles à la manifestation de la vérité²⁵. Cet acte qui constitue une dérogation à la règle de l'inviolabilité du domicile, est prévu par la loi, qui confère aux magistrats et sur autorisation de ceux-ci, aux officiers de police judiciaire les prérogatives d'opérer des perquisitions, comme stipulé dans les articles 44 du CPP (pour les officiers de police judiciaire) et l'article 81 du CPP, pour les magistrats instructeurs.

Le domicile est le lieu abritant l'être humain et les membres de sa famille, dans lequel il trouve refuge et où il se fie pour ses secrets et son intimité, peu importe s'il l'occupe de manière temporaire ou permanente. Selon la jurisprudence, le domicile est « le lieu où une personne a son principal établissement mais encore le lieu où, qu'elle y habite ou non, elle a le droit de se dire chez elle, quels que soient le titre juridique de son occupation et l'affectation données aux locaux »²⁶. L'accès sans autorisation du chef de maison est interdit, sauf pour les cas où la loi en dispose autrement²⁷.

Le domicile au sens du droit algérien est défini dans l'article 355 ainsi rédigé « est réputé maison habitée tout bâtiment, logement, loge, tente, cabine même mobile qui, même sans être actuellement habité est destiné à l'habitation, et tout ce qui en dépend comme cours, basses-cours, granges, écuries, édifices qui y sont enfermés quel qu'en soit l'usage et quand même ils auraient une clôture particulière dans la clôture ou enceinte générale ». Il s'agit donc de lieux clos à usage privé.

Il est ainsi reconnu au domicile son intimité en vertu de laquelle il est protégé contre la violation. Cette inviolabilité est garantie par la loi fondamentale, dans son article 48.

b-Inviolabilité du système informatique :

Etant donné que les systèmes informatiques constituent un élément omniprésent dans les infractions liées aux TIC, ceux-ci sont devenus les espaces idoines pour sauvegarder les données numériques des utilisateurs et

se substituent de plus en plus aux espaces physiques traditionnels de stockage. Il s'agit en fait de nouveaux espaces où l'on peut retrouver les éléments d'incrimination, telles que les documents, les photos, les enregistrements vidéo, outre les données numériques relatives aux systèmes informatiques ayant servi ou facilité la commission de l'infraction.

C'est dans ce contexte, que les nécessités des investigations édictent l'exigence de recourir à la perquisition des systèmes informatiques afin de rechercher des indices nécessaires à la manifestation de la vérité, dès lors que ces indices sont majoritairement sous forme numérique, eu égard à la nature de l'infraction elle-même. Par conséquent, l'espace numérique est devenu le milieu naturel où l'on peut rechercher et trouver de tels indices.

Le droit processuel classique ne permettait pas de concevoir un accès dans des espaces virtuels, ce qui a amené le législateur dans différents pays à adapter la norme juridique aux exigences de l'évolution de la criminalité²⁸.

En Algérie, la loi 09-04, venue s'inscrire dans ce sillage, stipule dans son article 5 que les autorités judiciaires et les officiers de police judiciaire, agissant dans le cadre du code de procédure pénale, peuvent, aux fins de perquisition, accéder aux systèmes informatiques et aux systèmes de stockage informatique.

La perquisition du système informatique est donc le procédé par lequel l'on accède à un système informatique en usant du système d'exploitation du système lui-même, à savoir les instructions et commandes qui permettent de rechercher et atteindre les données recherchées. Néanmoins l'usage du système d'exploitation s'avère parfois limité, ce pourquoi il est fait appel à des outils spécifiques qui permettent une recherche ciblant soit les données produites par l'utilisateur et stockées dans le système, soit les données produites par le système tels que les données système « fichiers Logs ». Ce type d'outils est conçu spécialement pour les services d'enquête « outils forensic » permettent de réaliser ces opérations avec performance.

Quel est donc le régime juridique applicable au système informatique en matière de perquisition ?

Tout d'abord, il est utile de rappeler que la loi 09-04 définit le système informatique de « tout dispositif isolé ou ensemble de dispositif

interconnectés qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ». Ainsi, les systèmes informatiques les plus utilisés de nos jours sont les ordinateurs, les téléphones portables, les tablettes, les serveurs ainsi que tout autre appareil doté de processeurs de traitement de données. Quant aux systèmes de stockage ceux-ci se présentent en des supports de sauvegarde, tels que les clés USB, les CD, les disques durs, ...etc.

L'intégration de ce nouveau mode de perquisition dans le droit procédural n'a pas manqué de poser la question sur l'applicabilité du régime classique de la perquisition et partant accorder le droit d'inviolabilité au système informatique et l'entourer des garanties liées à l'inviolabilité du domicile.

Au regard des usages variés des systèmes informatiques notamment ceux à usage privé, tels que PC individuel à usage domestique et téléphone portable, il est aujourd'hui évident que ces appareils comportent toute sorte d'intimité telles que photos de famille, messages privés échangés entre amis et membres de la famille, ... Etc. Ces éléments constituent autant d'intimités indissociables de l'intimité quotidienne de la vie privée telle que vécue au sein du domicile²⁹.

Ce raisonnement est conforté par la protection pénale accordée au système informatique, dès lors que l'accès, sans droit, dans un système informatique est un acte constitutif d'une infraction réprimée par l'article 394 bis du code pénal, qui interdit tout accès frauduleux à un système de traitement automatisé de données.

C'est à juste titre, que le législateur a fait renvoi au code de procédure pénale, expressément invoqué dans l'article 3 de la loi 09-04, concernant le champ d'application de cette loi, et rappelé dans l'article 5 consacré à la perquisition de systèmes informatiques. Cette manière de disposer laisse entendre judicieusement, à l'applicabilité du régime consacré à la perquisition du domicile, sur la perquisition de système informatique, en considération à la nature de ses espaces virtuels, qui comportent autant d'intimité et de secrets privés, méritant une protection similaire à celle accordée au domicile.

Il convient de rappeler que la perquisition de domicile est entourée de plusieurs garde-fous constituant des garanties quant à son inviolabilité et préserver l'intimité des personnes dans les cas où la loi autorise cet acte d'enquête. Il s'agit notamment des garanties ci-après :

-Mesure exclusive aux magistrats et Officiers de police judiciaire : Outre les magistrats, la perquisition du domicile est une mesure exécutable par les seuls OPJ dument habilités à exercer les missions de police judiciaire tel que défini dans le code de procédure pénale (articles 15 et 16 du CPP). Un agent de police judiciaire ne peut exécuter une perquisition sans la présence d'un OPJ.

-Autorisation préalable de l'autorité judiciaire : Dans le cadre des enquêtes de flagrance, l'officier de police judiciaire ne peut opérer une perquisition au domicile de la personne soupçonnée d'avoir commis ou participer à la commission d'une infraction ou celle que l'on croit possédant des objets en relation avec l'infraction commise, qu'après avoir dument obtenu une autorisation écrite du procureur de la république ou du juge d'instruction.

Cette disposition procédurale prévue par l'article 44 du CPP est confortée par une disposition constitutionnelle garantissant l'inviolabilité du domicile en conditionnant toute perquisition à l'autorisation écrite de l'autorité judiciaire.

Il est également stipulé dans l'article 44 du CPP que l'autorisation de perquisition doit mentionner la qualification de l'infraction pour laquelle l'on recherche des indices, ainsi que l'adresse du domicile objet de la perquisition, sous peine de nullité. Ceci outre les conditions de forme liées au document, tel que nom et prénom du magistrat ayant autorisé l'opération et son cachet.

-Respect des heures légales : Le domicile, et en sus des garanties de protection sus évoquées, est protégé davantage durant la nuit contre toute visite ou perquisition, par souci de sauvegarder la tranquillité que doit y retrouver les occupants pendant la nuit. C'est ainsi que les perquisitions sont limitées à un créneau horaire allant de 05 h du matin à 08 du soir (Article 47-1 du CPP)³⁰, sauf exception prévue par le régime dérogatoire.

-Présence du mis en cause : La présence de la personne soupçonnée, durant à la perquisition est une condition requise par l'article 44 du CPP. En l'absence de celle-ci, c'est son représentant qui doit y assister. En cas d'indisponibilité ou d'impossibilité de désigner un représentant, l'OPJ désigne deux témoins en dehors du personnel relevant de son autorité.

Une exception à cette disposition est également prévue dans le régime dérogatoire³¹.

Il importe de rappeler que l'inobservation des dispositions contenues dans les articles 44, 45 et 47, a savoir ; 1-L'autorisation préalable de l'autorité judiciaire, qui doit comporter la qualification des infractions recherchées et l'adresse du domicile ciblé, 2-la présence de la personne soupçonnée, son représentant ou deux témoins et 3-le respect des heures légales, entraîne la nullité de la procédure.

. Quelles sont donc les garanties susceptibles de préserver les droits des personnes dont le système informatique venait à faire l'objet de perquisition ?

2-Les garanties applicables à la perquisition des systèmes informatiques

a-Garanties déduites du code de procédure pénale

La transposition des règles applicables à la perquisition domiciliaire permet de mettre en évidence les mesures de garantie ci-après, lors de l'exécution de la perquisition informatique. Il s'agit de :

-Autorisation préalable de l'autorité judiciaire :

La perquisition de système informatique nous donne à s'interroger sur le contrôle que doit exercer l'autorité judiciaire, sur l'exécution de cet acte d'enquête.

A la lecture de l'article 05 de la loi 09-04, il n'est nullement fait mention de la procédure à observer en matière de perquisition de système informatique, ni encore moins, fait renvoi exprès aux dispositions du CPP relatives à la perquisition domiciliaire, à savoir les articles 44 à 48 (CPP) et 64 CPP, à l'exception d'un renvoi « muet » aux dispositions du code de procédure pénale, sans spécification aucune.

Cette manière de disposer laisse surgir une ambiguïté quant à la suspension de la régularité de la perquisition du système informatique, à

l'autorisation préalable de l'autorité judiciaire tel qu'exigé pour la perquisition du domicile, conformément à l'article 44 CPP.

Néanmoins, à la lumière de la réflexion supra citée plaidant à l'inviolabilité du système informatique au et au renvoi express aux dispositions du code de procédure pénale, il est permis de déduire que le système informatique à usage domestique doit jouir de la même protection que le domicile, et donc la perquisition de ce système doit requérir une autorisation préalable de l'autorité judiciaire, sous peine de nullité.

Il est opportun de s'interroger dans ce cadre si l'autorisation judiciaire de perquisition domiciliaire couvre la perquisition des systèmes informatiques s'y trouvant ?

A notre sens, ceci est valable uniquement en matière de recherche d'infractions liées au TIC, des lors que l'objectif est la recherche d'indices sous forme numérique, faudra il s'assurer encore que le système informatique trouvé au domicile perquisitionné est bien celui du mis en cause.

Autrement dit, une autorisation de perquisition d'un domicile pour rechercher des stupéfiants ne doit pas permettre d'opérer une perquisition des systèmes informatiques trouvés, par souci de parer au détournement de procédure³².

Quand est-il alors des systèmes informatiques à usage professionnel ?

Les systèmes informatiques à usage professionnel constituent une extension pour l'espace professionnel, et par conséquent la règle applicable aux lieux et locaux professionnels doit être étendue pour ces espaces virtuels. Ainsi, un système informatique utilisé par une personne tenue par le secret professionnel bénéficie de la protection conférée aux locaux de cette catégorie de professionnel.

-Présence de la personne soupçonnée :

La personne soupçonnée doit assister à la perquisition de son système informatique, afin d'être confrontée aux indices relevés. Cette présence est également exigée pour jeter du crédit à l'opération et éliminer toute éventuelle contestation par le mis en cause, quant aux indices trouvés en son absence.

-Exclusivité aux autorités judiciaires et OPJ :

La loi 09-04 a expressément donné compétence exclusive aux autorités judiciaire et aux OPJ pour l'exécution de l'acte en question, à l'instar d'autres actes d'enquête. Cette garantie est donc expressément prévue dans la dite loi.

Il est à souligner que la perquisition de système informatique requiert des techniques spécifiques, nécessitant le concours de techniciens, ce pourquoi en pratique cet acte est réalisé soit par des officiers de police judiciaire relevant de services spécialisés (services de lutte contre la cybercriminalité), soit par des experts dument requis par les OPJ ou les magistrats instructeurs.

-L'observation des heures légales :

Selon un raisonnement logique, l'observation des heures légales pour la perquisition des systèmes informatiques ne trouve pas de justifiant, des lors que l'objectif de cette restriction, à savoir assurer une tranquillité nocturne aux occupants, n'est pas concevable par rapport aux systèmes informatiques.

Néanmoins, Une telle garantie ne saurait être évincée étant donné que le renvoi aux dispositions du code de procédure pénale doit être pris dans son ensemble, s'agissant d'un dispositif de protection d'un droit constitutionnel. A ce titre et en l'absence d'exception expresse, cette garantie doit être observée dans le cadre de la perquisition de système informatique.

b-Garanties spécifiques à la perquisition distante :

La perquisition à distance est une perquisition informatique opérée à partir d'un système informatique étendue à travers celui-ci vers un autre système.

La loi 09-04 prévoit que cet acte d'enquête est également admis dans le cadre des enquêtes menées par les officiers de police judiciaire, après avis de l'autorité judiciaire compétente.

Le recours à l'avis préalable de l'autorité judiciaire en matière d'extension de la perquisition vient à notre avis, corroborer notre réflexion faisant état de la nécessité de l'autorisation préalable de l'autorité judiciaire pour effectuer une perquisition informatique, et qu'en cas d'extension de celle-ci d'un système vers un autre, un avis à l'autorité judiciaire ayant délivré l'autorisation initiale s'avère logiquement nécessaire.

Cette disposition constitue une exception au respect de la procédure d'extension de compétence, pour l'exécution d'actes d'enquête en dehors de la compétence territoriale de l'OPJ.

Lorsqu'il y a nécessité d'étendre la perquisition vers un autre système se trouvant en dehors du territoire national, la loi 09-04 suspend sa réalisation au concours des autorités étrangères en vertu d'accords internationaux et suivant le principe de réciprocité.

La question qui se pose dans ce contexte est de savoir quel sont les garanties qui permettent d'empêcher qu'un système informatique se trouvant en territoire national ne fasse l'objet d'une perquisition par une autorité étrangère, sans l'accord préalable des autorités nationales ?

Il s'avère ainsi que seuls des accords ou conventions garantissent cette immunité. Si l'on se réfère à la convention du Budapest « 2001 », celle-ci stipule en effet dans son article 32-b que l'accès des autorités d'un pays aux données stockées dans un autre Etat est soumis au consentement légal de la personne légalement autorisée à divulguer ces données.

Il s'agit là d'une garantie de l'inviolabilité des systèmes informatiques par accès à distance. Il va sans dire que l'Algérie, n'ayant pas ratifié cette convention, demeure exposé au risque que les autorités d'un autre Etat peuvent accéder à distance à des systèmes se trouvant dans notre territoire national, sans le consentement de la personne habilitée à autoriser cet accès.

Conclusion :

La protection des droits et libertés dont la vie privée, doit être au centre de préoccupation du législateur lors de la mise en place de la norme juridique processuelle, une tâche qui devient de moins en moins simplifiée avec le basculement de la société dans le cyberspace. La démarche adoptée en vertu de la loi 09-04 du 05/08/2009, exprimait le souci d'adapter notre dispositif juridique de répression aux évolutions de la criminalité.

Cette loi a marqué notre dispositif de procédure pénale par deux techniques nouvelles, à savoir la surveillance des communications électroniques et la perquisition des systèmes informatiques.

Concernant la surveillance des communications électroniques, il est prévu d'y recourir dans un cadre préventif justifié par les impératifs de

l'ordre public, afin d'empêcher la commission d'infractions qualifiées d'actes terroristes ou subversifs ou atteinte à la sûreté de l'Etat, ainsi que les atteintes aux systèmes informatiques susceptibles d'affecter l'ordre public, la défense nationale ou l'économie nationale. Ce cadre informel créé en marge du dispositif classique du code de procédure pénale soulève des inquiétudes quant à ses répercussions sur la vie privée, dès lors qu'il a admis le recours à la surveillance sur la base du soupçon.

L'autre cadre de surveillance se rapporte aux enquêtes et informations judiciaire et à l'exécution des demandes d'entraide judiciaire. Ce cadre crée des chevauchements avec l'application de l'article 65bis 5 du CPP relatif à l'interception des communications émise par voie électronique, duquel sont déduites les modalités d'exécution du premier. En ce sens, le chap d'application du cadre de surveillance prévu par la loi 09-04 paragraphe C et D, s'avère élargie à toutes les infractions liée aux Tic, combien même de simple gravité, or le cadre prévu par l'article 65bis 5 est limité aux seules infractions graves constituant l'objet du régime dérogatoire.

Il est ainsi plus judicieux de rétrécir le champ d'application de ce cadre de la surveillance aux infractions graves prévues dans l'article 65bis 5 du CPP lorsque la commission est facilitée par les TIC, afin de renforcer les garanties en lien avec cette technique, sur la vie privée.

Quant à la perquisition des systèmes informatiques, la loi 09-04 est restée silencieuses en ce qui concerne les règles d'exécution de cette technique. Une analyse des éléments de la vie privée dans le contexte numérique nous a permis de déduire l'inviolabilité des systèmes informatiques pour ensuite conclure à la transposition des garanties entourant la perquisition du domicile sur la perquisition du système informatique.

Cette transposition non encore approuvée dans la pratique judiciaire mérite une intervention du législateur afin d'entourer expressément la perquisition des systèmes informatiques des garanties consacrées à la perquisition domiciliaire et conférer aux citoyens le droit à l'inviolabilité de leurs systèmes informatiques

- ¹ محمد أبو العلا عقيدة، مراقبة المحادثات الهاتفية دراسة مقارنة، دار النهضة العربية، القاهرة، 2008، ص 75
- ² وهاب حمزة، الحماية الدستورية للحرية الشخصية خلال مرحلة الاستدلال والتحقيق في التشريع الجزائري، دار الخلدونية، الجزائر، 2011، ص 124
- ³ عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، القاهرة، بدون سنة نشر، ص 108
- ⁴ Rapport explicative de la convention sur la cybercriminalité, Conseil de l'Europe, 2001, n°209 <https://rm.coe.int/16800ccea4> 10/11/2020.
- ⁵ Réseau téléphonique commuté, encyclopédie en ligne wikipedia, https://fr.wikipedia.org/wiki/R%C3%A9seau_t%C3%A9l%C3%A9phonique_commut%C3%A9 12/11/2020
- ⁶ Myriam QUEMENER-Cybercriminalité-édit Economica Paris 2010-P174
- ⁷ Sabine HADDAD, forum juridique Légavox, violation du secret des correspondances et atteinte à la vie privée, 08/04/2014, <https://www.legavox.fr/blog/maitre-haddad-sabine/violation-secret-correspondances-atteinte-privee-14549.htm> 01/12/2020
- ⁸ Christian JAGER, Le terrorisme : Quelle personne ? A propos des théories du droit pénal de l'ennemi, les colloques de l'ISCJ, Institut de sciences criminelles et de la justice université de Bordeaux, n°2, juin 2017, P21
- ⁹ Dominique LINHARDT, Cédric Moreau DE BELLAING, la doctrine du droit pénal de l'ennemi et l'idée de l'antiterrorisme genèse et circulation d'une entreprise de dogmatique juridique, Lextenso droit et société, n°97, 2017, P617
- ¹⁰ Christian JAGER, Le terrorisme : Quelle personne ? A propos des théories du droit pénal de l'ennemi, les colloques de l'ISCJ, Institut de sciences criminelles et de la justice université de Bordeaux, n°2, juin 2017, P27
- ¹¹ Wilfrid JANDIDIER, droit pénal général, 2^{ème} édi, Montchrestien, Paris 1991, Page 265
- ¹² Christian JAGER, Le terrorisme : Quelle personne ? A propos des théories du droit pénal de l'ennemi, les colloques de l'ISCJ, Institut de sciences criminelles et de la justice université de Bordeaux, n°2, juin 2017, P21
- ¹³ عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، طبعة منقحة ومزودة، دار هومة، الجزائر، 2015، ص 15
- ¹⁴ ضياء عبد الله عبود، التنصت على المكالمات الهاتفية كإجراء من إجراءات التحقيق، مجلة رسالة الحقوق، جامعة كربلاء، العدد الثاني، 2009، ص 221
- ¹⁵ نبيلة حروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، 2006، ص 121
- ¹⁶ عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، طبعة منقحة ومزودة، دار هومة، الجزائر، 2015، ص 332
- ¹⁷ François-Bernard HUYGHE, les écoutes téléphoniques, PUF, Paris, 2009, page 44
- ¹⁸ عبد الرحيم صدقي، موسوعة صدقي الجنائية، المجلد السابع، بلا سنة طبع، دار النهضة العربية، القاهرة، ص 212
- ¹⁹ Hervé VLAMYNCK-Droit de la Police-édit Vuibert Paris--5^{ème} édition 2014-P169
- ²⁰ Hervé VLAMYNCK-Droit de la Police-édit Vuibert Paris--5^{ème} édition 2014-P169
- ²¹ عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، طبعة منقحة ومزودة، دار هومة، الجزائر، 2015، ص 16
- ²² عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، طبعة منقحة ومزودة، دار هومة، الجزائر، 2015، ص 18
- ²³ cet organe a depuis sa mise en activité en 2015, changé 3 fois de tutelle, à savoir le Ministère de la justice sous le décret présidentiel n°15-261 du 08/10/2015, en suite le Ministère de la Défense nationale sous le décret présidentiel n°19-172 du 16/06/2019, avant de passer sous la tutelle de la présidence de la République en vertu du décret présidentiel n°20-170 du 30/06/2020

²⁴ www.larousse.fr

²⁵ Serge GUINCHARD et Jacque BUISSON-procédure pénale -4^{ème} édition-Litec Pais 2008-Page 453

²⁶ Cass. Crim 13/10/1982 www.legalis.net

²⁷ عبد الله أوهابيه-شرح قانون الإجراءات الجزائية الجزائري، طبعة منقحة، دار هومة، الجزائر، 2015 ص299

²⁸ La recommandation n° R(95) du conseil de l'Europe du 11/09/1995 relative aux problèmes de procédure pénale liés aux technologies de l'information incitait les Etats à adapter leurs règles de procédure pénale afin de permettre aux autorités chargées des enquêtes, de perquisitionner dans des systèmes informatiques dans des conditions similaires à celles utilisées dans le cadre pouvoirs traditionnels de perquisition et de saisie. Aussi, la convention de Budapest sur la cybercriminalité stipule dans son article 19-1 que chaque Etat membre adopte les mesures législatives nécessaires pour habilitier ses autorités compétentes à perquisitionner ou accéder d'une façon similaire (...) à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées et à un support de stockage informatique, sur son territoire.

²⁹ C MEUNIER, la loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique, revue de droit pénale et de criminologie n°7, 2001, page 660

³⁰ عبد الله أوهابيه-مرجع سابق ص304

³¹ Bernard Bouloc, Haritini Matsopoulou –Droit pénal général et procédure pénale 15^{ème} édition-Dalloz 2004 p257

³² Bernard Bouloc, Haritini Matsopoulou –Droit pénal général et procédure pénale 15^{ème} édition-Dalloz 2004 p258