# *Captation de données et vie privée en 2011*

*Par*
*Claudine Guerrier, Professeur de droit à*
*Institut Telecom, TEM Research, ETOS*
***Claudine.Guerrier@it-sudparis.eu***

**Introduction**

A une époque où la vie privée est mise à l'épreuve des technologies de la communication, les Etats contrôlent de plus en plus le corps social à travers la vidéoprotection, la biométrie, les interceptions. Dès 2005[1], Howard Rheingold, déclare au *Monde* : « *Le pouvoir des Etats et des multinationales va s'accroître car les nouvelles technologies vont leur permettre de connaître plus finement nos comportements et nos croyances »* et « *Dans dix ans, la notion de vie privée telle que nous la définissons n'existera plus* ». Le prospectiviste américain n'est pas très éloigné du français Alex Türk, président de l'autorité administrative indépendante qu'est la CNIL. En 2008[2], M.Türk déclare à propos des nouvelles technologies « … *ce ne sont pas en soi, les technologies qui sont menaçantes. C'est l'usage qu'on en fait…. Au fond, on a deux formes de traçage qui posent problème : le traçage dans l'espace et le traçage dans le temps. Le traçage dans le temps… c'est toute la problématique d'Internet, des moteurs de recherche et des réseaux sociaux* ». Et ce traçage met en cause la protection de la vie privée et le secret des correspondances.

Les interceptions légales de télécommunications ont connu un essor technologique à la fin du vingtième siècle. Actuellement, l'interception semble gagner le domaine de l'informatique et concerne l'ensemble du secteur de l'information et des communications électroniques.
Les interceptions légales sont une dérogation au secret des correspondances, reconnu par la déclaration universelle des droits de l'homme, par la Convention européenne de sauvegarde des droits de l'homme[3], par le Pacte international relatif aux droits civils et politiques de l'ONU de 1966[4], par la Charte des droits fondamentaux de l'Union européenne[5].

En France, après la condamnation par la CEDH[6] de la France et l'adoption de la loi du 10 juillet 1991[7], un nouveau régime d'interceptions judiciaires et de sécurité est mis en place. A cette époque, les interceptions judiciaires n'ont lieu qu'au stade de l'instruction et sont autorisées par le juge d'instruction.
A partir de la loi du 9 mars 2004[8], dite Perben 2, les interceptions judiciaires peuvent avoir lieu au stade de l'enquête préliminaire pour quinze crimes et délits et sont autorisées par le juge des libertés et de la détention après demande du procureur de la République[9].
Depuis l'année 2005, les paroles et les images sont prises en compte dans le cadre de l'article 706-96 du code de procédure pénale[10].

La LOPSSI deux concerne l'ensemble des secteurs concernés par la sécurité. La première mouture de la LOPPSI deux, irriguée par le livre blanc sur la défense et la sécurité nationale[11]date de 2008 et est débattue en première lecture devant l'Assemblée nationale en février 2010, devant le Sénat en septembre 2010, en deuxième lecture, en décembre 2010 devant l'Assemblée nationale et en janvier 2011 devant le Sénat. La Commission mixte paritaire[12] entérine globalement la position de l'Assemblée nationale et la loi est adoptée définitivement le 8 février 2011. Le 15 février 2011, un recours est introduit par soixante députés et sénateurs devant le Conseil constitutionnel. La décision

---

[1] *Le monde* du 27 novembre 2005, « Dans dix ans, la vie privée telle qu'on la définit n'existera plus ».
[2] « *La Provence.com* », 19 décembre 2008.
[3] Article huit.
[4] Adopté à New York le 16 décembre 1966 par l'Assemblée générale.
[5] 2000/C 364/01.
[6] CEDH, Kruslin, 24 avril 1990.
[7] Loi 91.646 du 10 juillet 1991.
[8] Loi n°2004.204 du 9 mars 2004.
[9] Alors qu'elles n'étaient autorisées par la loi du 10 juillet 1991 qu'au stade de l'instruction.
[10] Loi n°2005-1549 du 12 décembre 2005.
[11] Publiée en 2007.
[12] Comprend sept députés, sept sénateurs.

du Conseil constitutionnel intervient le 10 mars 2011 et censure treize articles (sur 140). Néanmoins, la LOPPSI 2 renforce les pouvoirs et les compétences du ministère de l'intérieur dans l'anticipation, la prévention, la protection, la lutte et l'intervention contre les menaces et les risques susceptibles de porter atteinte aux institutions de la cinquième république, et aussi à la cohésion nationale, à l'ordre public, aux personnes, aux biens, aux installations, aux ressources d'intérêt général sur le territoire de la République. La LOPPSI 2 a donc des missions de programmation et d'orientation, elle tend à encadrer juridiquement la modernisation des pratiques sécuritaires mais également à « *adapter notre arsenal juridique à l'évolution des menaces qui pèsent sur notre sécurité intérieure et qui vont de la criminalité organisée à la petite délinquance, en passant par la cybercriminalité ou par le développement anarchique des activités dites d'intelligence économique* »[13]

Avec la LOPPSI 2, est introduite notamment la captation de données informatiques à distance. La « captation » est comprise dans son sens commun (recueillir, obtenir) et non dans « le fait de s'emparer de », souvent contraire au droit (captation d'héritage). Il convient donc dans ce contexte de s'interroger sur la compatibilité de la captation de données informatiques avec le concept actuel de respect de la vie privée, tel qu'il est déterminé par la CEDH. En France, le droit pénal vise l'intimité de la vie privée, définie de façon restrictive par une partie de la doctrine[14]. L'intimité implique, pour reprendre la classification de Mme Lolies[15], l'intimité personnelle (vie conjugale, sentimentale), l'intimité relationnelle, l'intimité corporelle. Les réticences à l'égard de la LOPPSI 2, ses principes ou ses modalités, prennent en compte l'adhésion supposée des Français à l'égard du respect de la vie privée et de la protection des données à caractère personnel : « *L'attachement des Français aux institutions de protection des données personnelles et à la possibilité de sauvegarder leur vie privée est bien réel, comme le prouve la récente mobilisation contre la mise en place des fichiers EDVIGE. S'ils n'expriment pas les mêmes craintes à l'égard des nouvelles technologies de surveillance, c'est parce qu'ils n'en mesurent pas l'impact, notamment en termes d'atteinte à la vie privée* »[16]. La LOPPSI 2 serait susceptible de porter atteinte aux libertés individuelles : *« Ce texte… témoigne d'un projet de société dans laquelle le contrôle social porte en germe une surveillance généralisée des citoyens* »[17] La problématique s'applique à la captation déjà effective, celle des sons et des images, et à la captation des données informatiques, créée par la LOPPSI 2.

## I)-La captation des images et des sons compatible avec la protection de la vie privée

Cette problématique est prise en compte au niveau du Conseil de l'Europe, par la CEDH, et, au niveau français, par le code de procédure pénale et par la jurisprudence de la Cour de cassation.

### A)-La captation des images et des sons introduite dans le code de procédure pénale

#### 1)-La procédure

#### 1.1)-Le principe[18]

Quand les nécessités de l'information relative à un crime ou un délit entrant dans le champ d'application de l'article 706-73[19]l'exigent, le juge d'instruction, peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique qui a pour finalité, sans le consentement des intéressés, 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 ou véhicules privés ou publics, ou de l'image d'une ou plusieurs personnes se trouvant dans un lieu privé. Les crimes et délits sont ceux prévus dans la loi Perben deux.

#### 1.2)-Les modalités

Certaines exceptions sont apportées aux modalités :

---

[13] Jean-Christophe Lagarde, Assemblée nationale, troisième séance du 9 février 2010.
[14] Ecrits de MM. Levasseur, Lindon, Bécourt.
[15] Isabelle Lolies, « *La protection pénale de la vie privée* », Presses universitaires d'Aix-Marseille, 1999.
[16] Patrick Braouzec, Assemblée nationale, troisième séance du 9 février 2010.
[17] Nicole Borvo Cohen-Seat, Sénat, séance du 18 janvier 2011.
[18] Article 706-96 du code de procédure pénale.
[19] Loi n°2004-204 du 9 mars 2004.

-Les captations d'images et de sons peuvent se faire en dehors des périodes prévues par l'article 59 du code de procédure pénale[20]
-L'installation et la captation peuvent se faire à l'insu ou sans le consentement du propriétaire ou du possesseur du véhicule ou de l'occupant des lieux[21]

**2)-La mise en place du dispositif technique**
Elle ne concerne pas les lieux où travaillent certaines personnalités

**2.1)-Les personnalités protégées**

-Les avocats : la mise en œuvre de dispositifs techniques ne peut avoir lieu dans les locaux visés à l'article 56-1 du code de procédure pénale
- Les entreprises de presse ou de communication audiovisuelle : la mise en œuvre de dispositifs techniques de captation de son ou d'image ne peut avoir lieu dans les locaux visés à l'article 56-2 du code de procédure pénale[22]
- Les médecins, les notaires, les avoués, les huissiers : la mise en œuvre de dispositifs techniques de captation de son ou d'image ne peut avoir lieu dans les locaux visés à l'article 56-3 du code de procédure pénale[23]
- Les députés et les sénateurs : la mise en œuvre de dispositifs techniques de captation de son et d'images ne peut avoir lieu au domicile des personnes visées à l'article 100-7 du code de procédure pénale[24]

**2.2)-Importance du rôle du juge d'instruction et du juge des libertés et de la détention**

- Le juge d'instruction : s'il s'agit d'un véhicule ou d'un lieu privé, l'introduction du dispositif technique de captation de paroles ou d'images est autorisée par le juge d'instruction. C'est le cas le plus fréquent.
-Le juge des libertés et de la détention : s'il s'agit d'un lieu d'habitation et que l'opération intervienne avant six heures ou après vingt-et-une heures, c'est le juge des libertés et de la détention qui délivre l'autorisation de mise en place d'un dispositif de captations de paroles ou d'images, après saisine par le juge d'instruction.

**3)-La désinstallation**

Elle implique la même intervention du juge d'instruction et du juge des libertés et de la détention que lors de l'installation.
Les exceptions aux horaires de droit commun, au consentement des personnes physiques relèvent de l'ordre public.
Certaines personnalités sont « protégées » pour des raisons tenant au respect des droits de la défense (les avocats), à la liberté d'expression (entreprises de presse ou de communication audiovisuelle), au secret professionnel (médecins, avoués, notaires)

**B)-La jurisprudence protectrice de la vie privée de la CEDH et de la Cour de cassation**

**1)-La jurisprudence de la CEDH**
Elle a été initiatrice d'une législation pour les interceptions de communications électroniques et la captation d'images et de sons

**1.1)-Les interceptions de communications électroniques**

---

[20] L'article 59 du code de procédure pénale stipule que les perquisitions ne peuvent avoir lieu avant six heures du matin ou après vingt-et-une heure.
[21] « ou de toute personne titulaire d'un droit sur ceux-ci », article 706-96 du code de procédure pénale.
[22] « *Les perquisitions dans les locaux d'une entreprise de presse ou de communication audiovisuelle ne peuvent être effectuées que par un magistrat qui veille à ce que les investigations conduites ne portent pas atteinte au libre exercice de la profession de journaliste…* ».
[23] « *Les perquisitions dans le cabinet d'un médecin, d'un notaire, d'un avoué ou d'un huissier sont effectuées par un magistrat…* ».
[24] « *Aucune interception ne peut avoir lieu sur la ligne d'un député ou d'un sénateur…* ».

C'est la jurisprudence de la CEDH qui a été à l'origine, en matière d'interceptions de télécommunications, d'une nouvelle législation au Royaume-Uni et en France, avec, notamment, les arrêts Malone et Kruslin.

**L'arrêt Malone**[25] : l'affaire a été déférée à la CEDH par la commission européenne des droits de l'homme le 16 mai 1983. James Malone a saisi la commission le 19 juillet 1978 en vertu de l'article 25. La requête individuelle est dirigée contre le Royaume-Uni. James Malone fut, le 22 mars 1977, inculpé de recel de biens volés. Son procès aboutit à une relaxe sur plusieurs points ; lors d'un procès suivant, il est acquitté pour insuffisance de preuves. Lors du premier procès, l'avocat de l'accusation reconnaît que James Malone avait fait l'objet d'interceptions téléphoniques en vertu d'un mandat délivré par le ministre de l'Intérieur. James Malone, après son acquittement, engage une action civile contre le préfet de police du Grand Londres, devant la Chancery Division de la High Court car il considère que l'interception, la surveillance et l'enregistrement de ses conversations téléphoniques étaient illicites, même s'ils se fondaient sur un mandat du ministre de l'Intérieur. Malone est débouté. Devant la CEDH, la question posée est de déterminer si le droit interne du Royaume-Uni présente des « *normes juridiques accessibles* » et des garanties suffisantes. La CEDH considère que le droit anglais et gallois en matière d'interceptions est obscur, peu accessible. Le risque d'abus existe. La CEDH applique un raisonnement identique à l'interception téléphonique et au procédé de comptage. Elle condamne le Royaume-Uni pour violation de l'article huit de la convention européenne de sauvegarde des droits de l'homme[26]. Dès 1985, le législateur tire les leçons de cette condamnation avec « The Interception of Communication Act ».

**Les arrêts Kruslin et Huvig**[27] : ont joué un rôle éminent dans la législation des interceptions judiciaires françaises, après, en France, l'arrêt Tournet[28]. Jean Kruslin avait fait l'objet d'interceptions téléphoniques alors qu'il se trouvait chez un ami qui était l'objet d'interceptions légales. Il a demandé l'annulation de l'enregistrement de la communication litigieuse, qui a été réalisée dans le cadre d'une procédure qui ne le concernait pas. La chambre d'accusation a débouté Jean Kruslin puisque le droit français n'interdit pas d'annexer à une procédure pénale les éléments d'une autre procédure à condition que la jonction ait un caractère contradictoire. Kruslin a introduit une requête individuelle devant la CEDH. La CEDH relève les lacunes du droit français. Ce dernier, écrit ou non écrit « *n'indique pas avec assez de clarté, l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré de sorte que les requérants n'ont pas joui du degré minimal de protection prévu par la prééminence du droit dans une société démocratique* ».

C'est ainsi que fut conçue, discutée, adoptée la loi[29]du 10 juillet 1991 sur les interceptions en France. Le principe de base est le suivant : le secret des correspondances émises par la voie des communications électroniques est garanti par la loi. La loi du 10 juillet 1991 s'inspire de l'arrêt Kruslin et des travaux, menés en France, par la Commission Schmelck[30]. La loi s'efforce de se montrer fidèle à la jurisprudence de la CEDH. Cependant, alors que pour la CEDH, les interceptions devaient rester un moyen exceptionnel de parvenir à la manifestation de la vérité, le législateur français abandonne, après débats, cette mention à ce caractère exceptionnel. Le projet de loi précisait que le juge d'instruction ne pourra recourir aux interceptions judiciaires que lorsque les nécessités de l'information l'exigent. De nombreux parlementaires constatent que cette formulation peut se prêter à

---

[25] CEDH, Malone, 16 mai 1983.

[26] A l'occasion de l'arrêt Malone, est jointe l'opinion concordante du juge Perretti, qui pose la problématique de la société démocratique et de ses exigences sécuritaires, face aux innovations technologiques : il est difficile de maintenir l'équilibre entre les nécessités de l'ordre public et la protection des libertés individuelles. La plupart des Etats qui ont ratifié la Convention européenne de sauvegarde des droits de l'homme comprennent la nécessité de légiférer pour mettre un terme aux abus. Même lorsqu'il s'agit d'interceptions afférentes au contre-espionnage, à la sûreté de l'Etat, la plupart des législations prévoient des modalités de contrôle. Selon M.Perretti, des contre-mesures apparaissent justifiées : droit à l'effacement, droit à la restitution des bandes. L'individu, selon M.Perretti, est menacé par le développement des technologies nouvelles, par la société de l'information : « *La mission du Conseil de l'Europe et de ses organes est d'empêcher l'instauration de régimes et de méthodes qui feraient des « Big Brother » les maîtres de la vie privée des citoyens* ». Arrêt Malone, opinion concordante du juge Perretti.

[27] CEDH, Kruslin, 24 avril 1990, Dalloz, 1990, 353. Notes Pradel ; CEDH, Epoux Huvig, CEDH, 24 avril 1990 ; P.Estamp, « La convention européenne des droits de l'homme et le juge français », *Gaz.Pal*., 1990, 1 doct 110 ; Michel Albarède, « Le régime juridique des écoutes téléphoniques », *Gazette du Palais*, 4 janvier 1991.

[28] Cour de cassation, Cour crim. 9 octobre 1980, Bull.n° 255, *Dalloz*, 1981, p 332, note Pradel, JCP, 191 II 19578, note Di Marino.

[29] 91.946.

[30] CNCIS, Rapport de 1991-1992.

de multiples interprétations. Il convient de prévoir des garde-fous, des précisions sur les « *nécessités de l'information* »[31]. Un texte est finalement adopté sous la forme suivante : les autres moyens d'investigation ne permettent pas de cerner la vérité ; les interceptions ne constituent pas un artifice déloyal ni une violation des droits de la défense ; la décision d'interception est écrite. Devant le Sénat, d'autres amendements sont proposés lors de la séance du 25 juin 1991. Ils ne sont pas adoptés. Et l'amendement de l'Assemblée nationale n'est pas repris dans le texte final.
Par ailleurs, la CEDH avait demandé que l'opposition apparaisse dans l'organisme qui devait être la CNCIS.[32]Cela ne fut pas retenu dans le texte de loi. Certes, l'opposition a toujours été représentée jusqu'à présent au sein de la CNCIS, mais il n'existe aucune obligation légale.
Ainsi la loi de 1991 est-elle plutôt fidèle aux exigences de la CEDH, mais pas dans sa totalité.

**1.2)-Les arrêts Peck et Van Hannover**

**Arrêt Peck c Royaume-Uni**[33] : M.Peck avait porté plainte contre la divulgation d'un film issu d'un circuit de télévision fermé. Des images représentant Peck sans son accord avaient été exploitées, diffusées à grande échelle. Un flou de masquage n'avait pas empêché les voisins et les collègues de le reconnaître. Pourtant, les autorités judiciaires britanniques avaient estimé que l'article huit de la Convention européenne de sauvegarde des droits de l'homme n'avait pas été violé. La CEDH, saisie par Peck par voie de requête individuelle a abouti à des conclusions contraires. Certes, le requérant se trouvait sur une voie publique mais il n'entendait pas participer à un évènement public et la divulgation des images ne relevait pas de la liberté de la presse ; elle « *n'était pas nécessaire dans une société démocratique* ». Certes, les circuits de télévision peuvent jouer un rôle dans la prévention de la délinquance, mais le Council devait obtenir l'accord préalable de M.Peck et procéder à un véritable masquage. M.Peck avait déclaré en outre que, dans son pays, le droit à la vie privée n'était pas protégé. La CEDH estime à cet égard que les pouvoirs confiés à la BSC et à l'ITC sont trop insuffisants pour que l'on puisse considérer les recours auprès de ces organismes comme des recours efficaces, dans la mesure où ils ne sont pas qualifiés pour ordonner des compensations financières dissuasives. Cet arrêt rappelle que « *des facteurs tels que l'identification sexuelle, le nom, l'orientation sexuelle et la vie sexuelle (constituent) des éléments très importants de la sphère personnelle protégée par l'article huit (…). Cette disposition protège également le droit à l'identité et au développement personnel ainsi que le droit pour tout individu de nouer et de développer des relations avec ses semblables et le monde extérieur. Il peut s'étendre à des activités professionnelles ou commerciales. Il existe donc une zone d'interaction entre l'individu et autrui, qui, même dans un contexte public, peut relever de la vie privée* ».

Cette interaction apparaît aussi dans **l'arrêt Van Hannover c.Allemagne**[34]
Le 24 juin 2004, la CEDH a rendu un arrêt de principe dans l'affaire Van Hannover c.Allemagne. Les juges, à l'unanimité, ont estimé que la presse ne pouvait, au nom du droit à l'information du public, violer le droit au respect de la vie privée d'une personnalité publique, quand bien même il s'agit d'une personnalité publique notoire.
Caroline Van Hannover avait saisi la CEDH le 6 juin 2000. Elle alléguait que les décisions des juridictions allemandes qui autorisaient la publication de photographies relevant de sa vie quotidienne avaient porté atteinte à son droit au respect de sa vie privée. La Cour constitutionnelle fédérale a considéré que la requérante, personnalité notoire, bénéficiait d'une protection de sa vie privée même en dehors de son domicile, mais uniquement dans un endroit isolé, à l'abri du public, *« dans lequel la personne concernée se retire dans le but objectivement reconnaissable d'être seule, et dans lequel, se fiant à son isolement, elle se comporte de manière différente de celle qu'elle adopterait en*

[31] A l'Assemblée nationale, des amendements sont discutés lors de la deuxième séance du 3 juin 1991 :
-Amendement n° 34, présenté par Jacques Toubon et François Massot. « *L'article 100 du code de procédure pénale sera ainsi rédigé :* « *Les dispositions de l'alinéa précédent ne peuvent être mises en œuvre que si : l'interception de la communication présente un intérêt pour la manifestation de la vérité ; les autres moyens d'investigation sont inopérants ou insuffisants ; elles ne constituent pas un artifice déloyal* », JOAN, 2ème séance du 13 juin 1991, p 3145, 1ère colonne.
-Amendement n° 56, présenté par François d'Aubert et Paul-Louis Tenaillon. « *Insérer les alinéas suivants : « L'interception ne peut être mise en place que si : l'interception de communications à distance présente un intérêt pour la manifestation de la vérité ; les autres moyens d'investigation sont inopérants ou insuffisants ; elle ne constitue pas un artifice déloyal ni une violation des droits de la défense* », JOAN, 2ème séance du 13 juin 1991, p 3145, 1ère colonne.
[32] Entretien de l'auteur avec Paul Bouchet en 1999.
[33] CEDH, 4ème chambre, n° 44647 du 28 janvier 2003.
[34] CEDH, req.n° 59320/00, 24 juin 2004.

*public ».* Elle a approuvé le jugement de la Cour fédérale de justice, en date du 19 décembre 1995, qui insiste sur la liberté de la presse. Il s'agit de répartir, dans le contexte, le poids respectif de l'article huit (vie privée) et de l'article dix (liberté de la presse) dans la convention européenne de sauvegarde des droits de l'homme. La CEDH note que les photos publiées montrent la requérante dans sa vie quotidienne. Caroline Van Hannover joue parfois un rôle de représentation pour l'Etat monégasque mais n'exerce aucune fonction officielle pour Monaco. Or, la CEDH opère une distinction entre un reportage afférent à des personnalités politiques, dans l'exercice de leurs fonctions officielles où la presse peut intervenir[35] et le reportage consacré à la requérante qui satisfait la curiosité d'un public ciblé mais ne participe à aucun débat d'intérêt général pour la société, et où l'article dix ne trouve pas sa place. Les critères retenus par les juridictions internes ne permettent pas d'assurer une protection effective de la vie privée de Caroline Van Hannover.
Les deux arrêts sont amenés à analyser le rapport entre sphère publique et sphère privée au regard de la convention européenne de sauvegarde des droits de l'homme.

**2)-Les arrêts français de la Cour de cassation**

Ils sont pris en conformité avec les arrêts de la CEDH : l'arrêt du 21 mars 2007 de la Cour de cassation[36] et l'arrêt de la Cour de Cassation du 13 novembre 2008 appliquent le droit national et le droit du Conseil de l'Europe.

**2.1)-L'arrêt du 21 mars 2007 :**

Les faits
Des officiers de police judiciaire installés sur la voie publique ont photographié au téléobjectif une propriété à usage d'habitation d'une personne suspectée de participation à un trafic de véhicules.
Les policiers ont photographié plusieurs véhicules, leurs plaques d'immatriculation et les personnes qui entraient et sortaient de la propriété privée.
L'une des personnes mises en examen a contesté devant la Chambre de l'Instruction la régularité de l'opération de surveillance qui a abouti à son interpellation.
Elle a soutenu que les photographies étaient nulles dans la mesure où elles constituaient une violation de l'article 706-96 du Code de procédure pénale au niveau national et une violation de l'article huit de la Convention européenne de sauvegarde des droits de l'homme au niveau du conseil de l'Europe.
La chambre de l'Instruction considère que la procédure relative aux photographies de personnes se trouvant à l'intérieur de la propriété est irrégulière.

Le droit
Un pourvoi a été formé par le Parquet et la Cour de cassation a pris position.
- La question de la régularité en enquête préliminaire de la surveillance photographique d'une personne se trouvant à son domicile à partir de dispositifs techniques placés sur la voie publique :
La Cour de cassation observe que « *la captation, la fixation, l'enregistrement ou la transmission par les enquêteurs de l'image d'une personne se trouvant dans un lieu privé, ne sont autorisés que dans les cas et conditions prévus par l'article 706-96 du Code de procédure pénale* »
C'est pourquoi, en l'absence du contrôle d'un juge d'instruction, les policiers ne devaient pas photographier des personnes situées à l'intérieur d'une propriété privée, même si les photographies ont été prises à partir de la voie publique. Constitue, en effet, une ingérence au sens de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme, dans l'exercice du droit au respect de la vie privée et du domicile, le fait pour les policiers de photographier clandestinement, au moyen d'un téléobjectif, une personne se trouvant à son domicile.

- La question de la régularité en enquête préliminaire de photographies prises à partir de la voie publique de véhicules circulant ou stationnant à l'intérieur d'une propriété privée :
La Cour de cassation déclare que « *constitue une ingérence dans l'exercice du droit au respect de la vie privée et du domicile le fait, pour les enquêteurs, de photographier clandestinement, au moyen d'un téléobjectif, les plaques d'immatriculation des véhicules se trouvant à l'intérieur d'une propriété privée non visible de la voie publique, aux fins d'identification des titulaires des cartes grises et alors que cette immixtion, opérée en enquête préliminaire, n'est prévue par aucune disposition de procédure pénale* ».

[35] « *chien de garde du public* », CEDH, Sunday Times c.Royaume-Uni, 26 avril 1979.
[36] Cour de cassation, chambre criminelle ; n°06-89.444.

Ainsi, le procédé utilisé par les policiers viole l'article huit de la Convention européenne de sauvegarde des droits de l'homme, relatif au respect de la vie privée.

Selon Pierre Belloir[37], si le relevé des plaques d'immatriculation avait été effectué à l'extérieur du domicile des prévenus dans le cadre d'une opération de surveillance de la voie publique, la solution de la Cour de cassation aurait été différente. Il appartenait aux policiers d'effectuer le relevé des numéros de véhicules à partir de clichés pris sur la voie publique et montrant les véhicules pénétrant dans la résidence, et non à partir de clichés représentant les véhicules à l'intérieur du domicile. La jurisprudence de la CEDH n'est pas respectée : la Cour de Cassation le relève.

**2.2)-L'arrêt de la Cour de cassation du 13 novembre 2008[38]-**

Les faits

Dans l'information poursuivie pour vols, blanchiment et escroquerie en bande organisée, le juge d'instruction a, par ordonnance du 6 avril 2007, autorisé la mise en place d'un dispositif technique de sonorisation et de captation d'images dans un immeuble à usage d'habitation.
Le 10 avril 2007, le juge des libertés et de la détention a autorisé les enquêteurs à s'introduire dans ces lieux, en dehors des heures légales, afin d'y installer le dispositif.
Le 16 avril 2007, le juge d'instruction a donné commission rogatoire au commandant de la section recherche de la gendarmerie de Paris afin d'installer le dispositif technique pour une période de deux mois.
Plusieurs personnes ont été mises en examen le 30 novembre 2007. Elles ont saisi la chambre de l'instruction de requêtes tendant, notamment, à l'annulation de la procédure de sonorisation et de captation d'images au domicile de S A. Ce dernier ( S A) a été débouté

Le droit

Les moyens :
Le premier moyen est pris de la violation des articles 706-96, 706-97, 802 du code de procédure pénale, de l'article huit de la convention européenne des droits de l'homme.
Le deuxième moyen est pris de la violation des articles 706-96, 706-97, 706-101 du code de procédure pénale, de l'article huit de la convention européenne des droits de l'homme
L'arrêt de la Cour de cassation refuse de constater la nullité des opérations de sonorisation, de leur retranscription et de la procédure subséquente ; selon la Cour de cassation, l'article 706-96 du code de procédure pénale exige que les opérations de sonorisation dans un lieu privé[39] et notamment dans un domicile privé soient effectuées sous le contrôle et l'autorité d'un juge d'instruction ; le point de départ de la durée de l'autorisation délivrée par le juge ne peut être reporté au jour de la mise en place effective, par les officiers et agents de police judiciaire du système d'enregistrement sans qu'il soit porté atteinte à l'autorité et au contrôle effectif du juge d'instruction : ces dispositions n'ont pas été respectées

Aux termes de l'article 706-96 du Code de procédure pénale l'autorisation donnée par le juge d'instruction porte sur la mise en place d'un dispositif technique d'enregistrement dans un lieu privé[40] de sorte que la durée mentionnée obligatoirement est[41] celle du maintien en place de ce dispositif. En

---

[37] « *La surveillance photographique en matière d'enquête préliminaire* », *Lamy Droit de l'immatériel*, juillet 2007, Pierre Belloir.
[38] Arrêt n° 5605 du 13 novembre 2008 (08-85.456), Chambre criminelle de la cour de Cassation.
[39] Le lieu privé a été défini par Hervé Pelletier ( JCl Pénal Code Art 226-1 à 226-3, fasc.20 ) comme « *celui où personne ne peut pénétrer sans le consentement de l'occupant* » ; Jean.Ravanas considérait que le lieu privé était le lieu dont « *l'accès dépend du consentement de celui qui l'occupe » (* « *La protection des personnes contre la réalisation et la publication de leur image* », collection *Solus, LGDJ*, 1978, p 514 ). Un jugement du 6 juillet 1995 ( TGI Paris, 17ème chambre, 6 juillet 1995, P : 94 167 200029), inspiré par plusieurs décisions antérieures ( Cf, notamment, CA Besançon, 5 janvier 1978, D.1978, p 357, note Lindon) indique, à propos de la piscine du centre de thalassothérapie de l'hôtel Royal à La Baule : « *Le lieu privé est défini comme un endroit qui n'est ouvert à personne, sauf autorisation de celui qui l'occupe d'une manière permanente ou temporaire, alors que le lieu public est celui qui est accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent ou inconditionnel ou subordonné à certaines conditions …* » « *Il importe peu que la piscine ait été fréquentée, lors de la prise de vue par d'autres personnes que la demanderesse, rien n'empêchant que l'intimité de la vie privée d'un individu soit partagée par des tiers dont la présence est admise par celui-ci. »* L'accès à ladite piscine étant ainsi très limité par des considérations *intuitu personae*, le caractère privé de ce lieu ne peut être raisonnablement contesté.
[40] Cf : note 35.
[41] Cf : article 706-97 du code de procédure pénale.

conséquence, à l'expiration de la durée fixée par le juge, en l'absence de renouvellement, le dispositif technique doit être retiré. En décidant que le dispositif pouvait être maintenu en place après l'expiration de la durée de deux mois fixée par le juge d'instruction, l'arrêt a méconnu le sens et la portée des textes précités.

Selon l'article 706-101 du Code de procédure pénale, seules peuvent être versées au dossier les conversations enregistrées qui sont utiles à la manifestation de la vérité. Or, les dates et lieu de vacances de S A et de sa famille avaient été connus des enquêteurs. Cette connaissance provenait de l'exploitation des sonorisations[42]. Cette exploitation n'était manifestement pas utile à la manifestation de la vérité. En conséquence, ces informations ne pouvaient ni apparaître dans la procédure ni être exploitées pour décider du maintien en place du dispositif de surveillance inactif.
La chambre de l'instruction a raisonné à bon escient en arguant que le point de départ des mesures de sonorisation devait être fixé au jour de leur mise en place effective.
Par contre, la chambre de l'instruction, en déclarant régulière l'ordonnance de renouvellement intervenue le 5 juillet 2007 alors que l'autorisation précédente avait pris fin le 23 juin 2007, a méconnu les textes mentionnés ci-dessus du Code de procédure pénale.
La Cour de cassation, pour ces raisons, annule l'arrêt de la chambre d'instruction. Elle fait respecter l'article huit de la Convention européenne de sauvegarde des droits de l'homme.

La jurisprudence, en la matière, n'est pas créatrice de droit mais elle interprète au plus près les dispositions légales du code de procédure pénale et empêche des dérives qui auraient pu être considérées comme liberticides et suit l'article huit de la Convention européenne des droits de l'homme.
La Cour de cassation a joué son rôle de gardienne des principes fondamentaux du droit, en se référant au droit du Conseil de l'Europe .La doctrine, quant à elle, ne s'est pas penchée sur la conformité de la captation des sons et des images à la Convention européenne de sauvegarde des droits de l'homme.

**II)-La captation des données informatiques :**

Posent également question, du point de vue du respect de la vie privée, dans le contexte de la LOPPSI II, les nouvelles possibilités de captation des données informatiques prévues dans les articles 706-102-3, 706-102-7, 706-102-9 du Code de procédure pénale.
La LOPPSI 2 permet, dans le cadre de la lutte contre la criminalité organisée, la captation de données informatiques. L'accès aux données stockées dans les systèmes informatiques, prévu par plusieurs dispositions du Code de procédure pénale, n'est plus adapté en effet à l'utilisation croissante de certains périphériques. Ainsi, le système proposé permettrait-il à un enquêteur d'accéder sans le consentement de l'intéressé à des données informatiques « *telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères* »[43]. Il est possible à la police, dans le respect des procédures, d'installer des mouchards[44] dans les ordinateurs des personnes suspectées d'avoir commis certains crimes ou délits en bande organisée prévus dans la loi du 9 mars 2004 ou, s'il est impossible d'accéder physiquement à l'ordinateur, de mettre en place des mouchards, des logiciels qui doivent récupérer le contenu de certains fichiers et transmettre ce contenu à un destinataire prédéfini par Internet, ou des « keyloggers », logiciels dont la finalité est de capturer les touches du clavier pressées par l'utilisateur, de les enregistrer dans un fichier et d'envoyer ce fichier à un destinataire prédéfini par Internet.[45]

Jusqu'alors, il fallait, pour accéder aux données informatiques, demander une autorisation à des fournisseurs d'accès à Internet et les enquêteurs n'étaient pas en mesure de capter les conversations cryptées ; au demeurant, certains périphériques ne laissaient pas de trace des données dans les unités centrales. Ce dispositif est nouveau, puisque l'accès aux données informatiques ne pouvait s'effectuer jusqu'à présent que lors de perquisitions. La grande majorité des sociétés commerciales ne sont pas concernées par la captation des données informatiques : la LOPPSI 2 autorise le recours à ce procédé quand il y a échanges informatiques entre membres d'une organisation délinquante ou criminelle ; cela se produit rarement. Toutefois, si un salarié est soupçonné de se livrer à une telle

[42] PV D 121.
[43] Article 706-102-1 du nouveau code de procédure pénale.
[44] Ou spywares.
[45] L'exposé des motifs de l'article 23 explique que « *la captation de données informatiques s'avère indispensable pour démanteler des réseaux et trafics qui recourent à des techniques sophistiquées* ».

activité en utilisant les moyens informatiques de son employeur, le système informatique de la société se verrait alors l'objet d'une surveillance ; dans cette hypothèse, les enquêteurs agiraient en concertation avec l'employeur. Si une discrétion totale devait s'imposer, la LOPPSI 2 dote les enquêteurs de la possibilité de placer les dispositifs de captation sur le réseau de l'entreprise sans informer les responsables.

**A)-Les modalités de captation de données informatiques**

Elles s'inspirent souvent de la captation des images et des sons

**1)-Le principe et la durée**

**1.1)-Le principe** : L'opération de captation de données informatiques est possible si les nécessités de l'instruction l'exigent. La captation de données informatiques n'est envisagée qu'au stade de l'instruction, et non au stade de l'enquête préliminaire. Le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données.[46]

**1.2)-La durée**

Les décisions sont prises pour une durée maximale de quatre mois[47]. Si les nécessités de l'instruction l'exigent, une renouvelabilité de quatre mois est possible, à titre exceptionnel et dans des conditions de forme identiques. Cette unique renouvelabilité se distingue de la renouvelabilité « à l'infini » des interceptions judiciaires de communications électroniques au stade de l'instruction. Elle s'inscrit dans la continuité de la durée prévue pour la captation des images et des sons. Par ailleurs, le juge d'instruction peut ordonner, à tout moment, l'interruption de l'opération.

**2)-Le procès-verbal et la destruction des données informatiques**

**2.1)-Le procès-verbal**

Le juge d'instruction ou l'officier de police judiciaire commis par lui dresse un procès-verbal de chacune des opérations de mise en place du dispositif technique et des opérations de captation des données informatiques. Ce procès-verbal mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée[48].

Les enregistrements des données informatiques sont placés sous scellés fermés.[49] Le juge d'instruction ou l'officier de police judiciaire commis par lui décrit, dans un procès-verbal qui est versé au dossier, les données qui sont utiles à la manifestation de la vérité. Le ministère de l'intérieur a indiqué, dans un courrier du 27 mars 2009, que l'ensemble des enregistrements opérés seraient placés sous scellés.

A cet égard, dans sa décision du 2 mars 2004 relative à la loi portant adaptation de la justice aux évolutions de la criminalité, le Conseil constitutionnel a précisé, s'agissant des dispositions du Code de procédure pénale autorisant les sonorisations et fixations d'images de certains lieux et véhicules que l'article 706-101 *« limite aux seuls enregistrements utiles à la manifestation de la vérité le contenu du procès-verbal* » et « *que dès lors, le législateur a nécessairement entendu que les séquences de la vie privée étrangères aux infractions en cause ne puissent en aucun cas être conservées dans le dossier de la procédure* ». La CNIL rappelle cette décision du Conseil constitutionnel et incite au strict respect de ces principes dans l'hypothèse comparable de la captation des données informatiques.

En matière de procès-verbal, c'est le droit commun, s'appliquant aussi dans le secteur des interceptions judiciaires au stade de l'instruction, qui prévaut. On constate un souci d'équilibre entre l'ordre public et les libertés individuelles dans le cadre de cette procédure qui déroge à la protection de la vie privée.

---

[46] Article 706-102-1 du code de procédure pénale.
[47] Article 706-102-3 du code de procédure pénale.
[48] Article 706-102-7 du code de procédure pénale.
[49] Article 706-102-8 du code de procédure pénale.

**2.2)-La destruction des données informatiques**

-La difficulté de détruire les données : il est bien difficile, techniquement, de détruire complètement des données, sans qu'il reste des traces. L'effacement partiel, la non-accessibilité aux données informatiques est plus simple à réaliser. Cependant, la destruction des données informatiques est prévue par la loi.
-La prescription de l'action publique :
Comme pour les interceptions judiciaires au stade de l'instruction, la date de la destruction des données informatiques prête à discussion[50]. Une personne mise en examen peut être relaxée ; il peut y avoir non-lieu. Les enregistrements des données informatiques sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de l'action publique. Le non-lieu n'induit donc pas de destruction de l'enregistrement.

**2.3)-Les opérations incidentes**

Les opérations ne peuvent avoir un autre objet que la recherche et la constatation des infractions visées dans les décisions du juge d'instruction. Le fait que ces opérations révèlent des infractions autres que celles créées dans ces décisions ne constitue pas une cause de nullité des procédures incidentes.[51]

**B)-Des questions restent pendantes en matière de captation des données informatiques**

**1) La CNIL a émis des réserves le 16 avril 2009 :**
Avant le vote de la LOPPSI 2, la CNIL a fait apparaître des réserves sur la captation des données informatiques à distance. Le ministère de l'intérieur ne lui avait soumis en janvier 2009 que sept articles de l'avant-projet de loi. Pour la première fois, et à la demande de Jean-Luc Warsmann[52] , la CNIL a rendu public son avis[53]. Elle savait que le projet de texte sur lequel elle s'est prononcée le 16 avril 2009 est quelque peu différent de celui qui a été déposé à l'Assemblée nationale. Cet avis, désormais connu des députés et des sénateurs pouvait servir à amender le texte de façon à suivre les recommandations de la CNIL

1.1)-**L'usage des captations pour certaines professions dites « protégées »**

La CNIL a émis des critiques sur l'adverbe *« habituellement »* dans l'article qui interdit l'usage des captations de données informatiques à certaines professions[54]. Elle y a vu un risque « *d'aléa et un risque d'insécurité juridique disproportionnés au regard des finalités poursuivies* ». La rédaction permettrait de collecter des données transitant sur des systèmes utilisés par des personnes protégées par le législateur en raison de secrets particuliers liés à l'exercice de leur profession ou de les collecter dans les lieux de travail ou domiciles de ces dernières.
Les associations de défense de droits de l'homme se sont particulièrement inquiétées pour les journalistes. Elles redoutent notamment la captation de données par des logiciels espions et l'utilisation excessive de ce système d'espionnage par la police, qui pourrait mettre en danger la protection des sources journalistiques. Ces associations ont été entendues et la captation des données informatiques à distance à l'endroit des journalistes est juridiquement impossible

**1.2)-La captation des données informatiques à distance et les points d'accès public à Internet**

La CNIL déplorait que le projet de loi prévoie la possibilité de mettre en œuvre un dispositif de captation dans tout type de point d'accès public à Internet.[55].
La CNIL mettait l'accent sur cette disposition, qui aurait pu permettre pendant une durée de huit mois, la captation de tous les caractères saisis au clavier et de toutes « *les images affichées sur l'écran de tous les ordinateurs d'un point d'accès public à Internet, et ce, à l'insu des utilisateurs ».*

---

[50] Article 706-102-9 du code de procédure pénale.
[51] Article 706-102-4 du code de procédure pénale.
[52] Président de la Commission des lois de l'Assemblée nationale.
[53] Délibération n° 2009-200 du 16 avril 2009 portant avis sur sept articles du projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure.
[54] Médecin, avocat, notaire, parlementaire, entreprise de presse.
[55] Cybercafés ou bornes d'accès publiques.

Il existerait une menace pour les droits et libertés des internautes : « *La Commission relève que si l'installation de dispositifs de captation de données informatiques demeure une mesure d'investigation exceptionnelle, sa mise en œuvre dans des points publics d'accès au réseau Internet présente un caractère particulièrement sensible ».*La CNIL rappelle que le Conseil constitutionnel a considéré[56], concernant la loi pour la sécurité intérieure[57], qu'il appartenait au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent le respect de la vie privée, ainsi que la liberté individuelle , que l'article 66 de la Constitution place sous la surveillance de l'autorité judiciaire.

**1.3)-La traçabilité**

En termes de garanties, la CNIL souhaite que des mécanismes soient mis en place afin de rendre impossible l'exploitation des matériels et logiciels de captation de données à des fins détournées. Selon la CNIL, des mesures de traçabilité devraient encadrer l'utilisation de ces outils, afin que ceux-ci ne puissent être employés que sous le contrôle d'un juge d'instruction. La CNIL souhaite notamment que soient instaurées des mises sous coffre-fort logique des outils de captation des données.

**1.4)-La captation en continu des données informatiques**

La CNIL a critiqué les articles afférents au dispositif susceptible de capter en continu des données informatiques utilisées ou saisies sur un ordinateur, que les données soient ou non destinées à être émises et qu'elles empruntent ou non un réseau de communications électroniques. Selon la CNIL *« la collecte de données par captation en continu des données utilisées ou saisies sur un ordinateur ne devrait concerner que les données utiles à la manifestation de la vérité ou les personnes susceptibles d'être impliquées dans des faits relevant de la criminalité organisée* ».

**1.5)-La jurisprudence de la Cour constitutionnelle de Karlsruhe**

Dans ses délibérations datées du 16 avril 2009, la CNIL rappelait que la Cour constitutionnelle de Karlsruhe a précisé les limites de la captation des données : « *L'introduction clandestine dans des systèmes informatiques de logiciels espions ne peut être autorisée que s'il existe réellement des éléments présentant une menace concrète sur l'intégrité corporelle, la vie, la liberté des personnes ou une atteinte aux intérêts fondamentaux de la nation* ».
Par cette référence explicite à une importante jurisprudence allemande, la CNIL attirait l'attention du gouvernement français sur la nécessité de définir clairement le cadre de mise en œuvre de la captation des données.
Le gouvernement ne donne pas suite à la plupart de ces observations.

**2)-La CNIL après l'adoption du texte par l'Assemblée nationale[58] en première lecture**
La CNIL rend un nouvel avis.
A la demande du rapporteur de la loi LOPPSI 2 au Sénat, la CNIL a formulé des observations, qui portent sur l'ensemble du texte

**2.1)-Le préambule**

La CNIL observe que sa recommandation sur les personnes protégées[59] a été prise en compte.

**2.2)-Les nouvelles recommandations**

La CNIL exprime des souhaits et renouvelle les demandes qui n'ont pas été prises en considération. Cela concerne surtout l'utilisation d'outils de captation dans les points publics d'accès à Internet.

---

[56] Décision n° 2003-467 du 13 mars 2003.
[57] Loi 2003-239 du 18 mars 2003.
[58] Le 18 février 2010.
[59] Telles que les cabinets d'avocats, de médecin, de notaire, d'avoué ou d'huissier ainsi que les locaux d'une entreprise de presse.

Or, selon la CNIL, cette disposition « *présente un caractère particulièrement sensible puisqu'elle conduit à placer sous surveillance l'ensemble des postes informatiques mis à disposition du public ».* La CNIL demande donc qu'une telle pratique ne soit possible que dans des conditions exceptionnelles et pour des motifs spécifiques ; elle souhaite également que la loi impose la traçabilité des accès aux outils de captation et de leur utilisation. En la matière, les observations ne sont pas suivies d'effet. Un amendement de suppression est présenté par les Verts au Sénat en première lecture et n'est pas adopté.

**3)-Les difficultés d'application[60]**

**3.1)-La neutralisation du « mouchard policier »**

Plusieurs juristes et notamment Etienne Papin s'interrogent sur l'éventuelle neutralisation du « mouchard policier » s'il était découvert et neutralisé.
Il convient de se demander ce qui se passera si le spyware policier est découvert et neutralisé par le RSSI, à l'instar de n'importe quel autre virus ou cheval de Troie. La question n'a pas été envisagée au cours des débats parlementaires. L'article 434.4 du code pénal punit de trois ans d'emprisonnement et de 45000 euros d'amende le fait, ce qui constitue un obstacle à la manifestation de la vérité, de détruire, soustraire, receler ou altérer un objet de nature à faciliter la découverte d'un crime ou d'un délit, la recherche des preuves ou la condamnation des coupables.
Or, la commission de cette infraction requiert l'intention délictuelle : il faut que la personne qui détruit ou neutralise le dispositif agisse avec le dessein de faire obstacle à la manifestation de la vérité. Dans une entreprise, il ne pourra en être ainsi que si la personne chargée de la sécurité du système sait que le dispositif détecté a été placé par l'autorité judiciaire et le neutralise en connaissance de cause. Néanmoins, il est évident que les mouchards policiers ne se feront pas reconnaître.

**3.2)-Le déroulement des opérations**

Les opérations seront effectuées sous l'autorité et le contrôle du juge d'instruction. A peine de nullité, la décision du juge d'instruction devra préciser l'infraction qui motive le recours à ces dispositifs, la localisation exacte ou la description détaillée du système informatique ainsi que la durée des opérations. Le texte prévoit que ces opérations peuvent révéler des infractions autres que celles visées par la décision du juge d'instruction. Il n'y pas de nullité des procédures incidentes : les infractions révélées par le « mouchard », même sans rapport avec la délinquance et la criminalité organisée, pourront faire l'objet de poursuites.
Les enquêteurs disposent déjà d'un certain nombre de prérogatives : l'actuel article 60.2 du code de procédure pénale autorise, dans le cadre d'une enquête de flagrance, les officiers de police judiciaire à requérir l'accès aux données contenues dans des systèmes informatiques ou traitements de données nominatives de certains organismes tels que les administrations ou les opérateurs de communications électroniques. De manière plus directe, les officiers de police judiciaire peuvent, au cours d'une perquisition, accéder aux données intéressant l'enquête stockées sur un système informatique[61].

**3.3)-Le matériel**

Pour ce qui concerne le matériel utilisé, une comparaison peut être établie avec le régime instauré pour les interceptions de communications électroniques. La détention de tels appareils est soumise à autorisation ministérielle. D'abord conçu pour les dispositifs matériels, ce régime a été étendu aux logiciels qui permettent de procéder à de tels enregistrements. La LOPPSI 2 prévoit aussi d'inclure dans les matériels dont la détention, l'importation, la falsification ou la commercialisation nécessitent une autorisation ministérielle les mouchards destinés à capter les données informatiques.

Par ailleurs, qu'il s'agisse de dispositifs de captation de l'image, de la voix, ou des données informatiques, leur efficacité est subordonnée au fait qu'ils ne soient pas découverts et neutralisés.
Néanmoins, des distinctions doivent être établies entre captation de sons et d'images et captation de données informatiques : distinction technique, distinction juridique. La distinction technique concerne la traçabilité des données informatiques et la très grande difficulté qu'il y a à détruire des données

[60] Cf notamment : Etienne Papin, avocat associé du cabinet Féral-Schuhl.
[61] Article 57.1 du code de procédure pénale.

informatiques. L'effacement est possible ; la destruction complète est exceptionnelle. C'est pourquoi il n'est guère pertinent, au regard du respect de la vie privée de procéder à la captation de données informatiques.
De plus, la distinction juridique pose la question du dispositif de captation dans tout type de point d'accès public à Internet. Il s'agit d'une problématique de sécurité juridique et de sécurité technique.

**4)-Le contrôle parlementaire**

Il est timide. L'article 23 sur la captation des données informatiques à distance n'a été examiné qu'en première lecture au Sénat et non en deuxième lecture, le texte étant inchangé en deuxième lecture. Les opinions varient en fonction des origines. Pour le législateur, la captation de données informatiques est nécessaire à l'Etat français et se situe dans le prolongement de la captation des sons et des images. La classe politique dans sa grande majorité est favorable à l'introduction de la captation des données informatiques à distance. Seuls, les Verts et le PCF manifestent une opposition tangible : déclarations, dépôt d'amendements. Au demeurant, en deuxième lecture, devant l'Assemblée nationale, le seul amendement significatif, au demeurant rejeté, n° 105[62] propose la suppression pure et simple de l'article 23 qui introduit la captation de données informatiques à distance : c'était le principe qui était visé, en vain. Ce relatif unanimisme coïncide avec l'attitude générale des députés et des sénateurs à l'égard de la LOPPSI 2.

Certes, devant l'Assemblée nationale, l'amendement n° 245[63] limite le champ d'application de la captation des données ; est mis notamment en cause « le délit de solidarité »[64], l'aide apportée aux étrangers en situation irrégulière. Devant le Sénat, les amendements 152 et 153 tendent aussi à restreindre le nombre de crimes ou de délits pour lesquels il est possible de recourir à la captation de données informatiques[65]. Ils ne sont pas adoptés. L'utilité du dispositif est discutée. Mme Labarre craint que le ministère de l'Intérieur puisse, à partir des soupçons tirés de fichiers approximatifs, espionner des courriels ou se servir d'opinions développées sur des forums de discussion[66]. Le ministre de l'Intérieur de l'époque[67]fait valoir que, dans l'état actuel du droit, il n'est pas possible de capter des données informatiques tapées sur un ordinateur avant qu'elles ne soient diffusées ou cryptées ; cela constitue un obstacle contre la lutte afférente à la délinquance et à la criminalité organisées[68]. Les Verts insistent sur les dangers encourus par les libertés individuelles du fait de la captation des données informatiques : « *Le caractère particulièrement intrusif de ce dispositif ne nous semble pas du tout conforme aux principes de proportionnalité et de respect du droit à la vie privée* »[69]. La loi ne donne aucune indication sur le type de matériel qui sera utilisé pour la captation des données. Aucune mention n'est faite d'une quelconque autorisation ministérielle. Or, la question des matériels a toujours joué un rôle éminent, en matière d'interceptions et de captations et la réglementation est souvent apparue avec retard : pour la loi du 10 juillet 1991 sur les interceptions de télécommunications et les matériels, le décret annoncé[70] ne paraît qu'un an et demi après l'adoption de la loi, en 1993, ce qui a retardé d'autant la parution des arrêtés ministériels. Se pose également la question des modalités susceptibles de garantir l'intégrité des données captées lors de leur transmission vers les agents habilités à les recevoir. Le gouvernement annonce qu'une étude spécifique sera diligentée pour garantir l'intégrité des informations, mais ne donne aucune précision. Le débat est assez formel.

---

[62] Amendement de Noël Mamère.
[63] Assemblée nationale, 11 février 2010.
[64] Expression employée par Jean-Yves Le Bouillonnec, Assemblée nationale, 11 février 2010.
[65] « *La nouvelle rédaction de l'alinéa 4 que nous proposons entend réserver ( la captation des données)… aux crimes et délits les plus graves, en excluant qu'on puisse y recourir, par exemple, s'agissant d'informations concernant des vols ou dégradations commis en bande organisée ou les délits d'aide à l'entrée, à la circulation et au séjour irréguliers d'un étranger en France commis en bande organisée, ce qui est d'ailleurs conforme à l'avis de la Commission nationale consultative des droits de l'homme* », Mme Labarre, Sénat, 9 septembre 2010.
[66] « *La reconnaissance légale de ces logiciels-espions, qui ne connaissent pas de frontières, mais qui sont, par ailleurs bien connus des pirates informatiques et de certaines officines de renseignement privées, nous paraît donc extrêmement dangereuse* », Mme Marie-Agnès Labarre, Sénat, 9 septembre 2010.
[67] Brice Hortefeux.
[68] « … *cela rend naturellement plus difficile, plus long et plus incertain le démantèlement de ces groupes criminels »,* Brice Hortefeux, Sénat, 9 septembre 2010.
[69] Alima Boumediene-Thiery, Sénat, 9 septembre 2010.
[70] Le décret n° 93 513 du 25 mars 1993 est pris en application de l'article 24 de la loi n° 91646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications

**Conclusion**

Les ONG de défense de droits de l'homme ont tendance à supputer que la captation de données informatiques peut être porteuse de dérives. C'est le point de vue également exprimé par Reporters sans frontière[71], par la Quadrature du net[72].
Par ailleurs, la captation des données informatiques à distance, comme la captation d'images et de sons, donne une place éminente au juge d'instruction. Si cette fonction est supprimée, le procureur, qui ne présente pas le même profil en tant que caution des libertés, peut être amené sur le devant de la scène. Dans ce contexte, la CEDH ferait peut-être l'objet d'une requête.

La CNIL, et cela apparaît dans tout le débat relatif à la LOPPSI 2, détient le monopole dans le domaine du conseil et du contrôle pour ce qui concerne la vie privée et les libertés individuelles. Cette référence incontournable actuellement a des avantages et des inconvénients. Certes, la CNIL bénéficie d'une légitimité rare parmi les autorités administratives indépendantes. Elle est bien armée sur le plan juridique et technique. Ses experts juristes sont reconnus. Cependant, le budget de la CNIL est insuffisant et tout organisme peut être exposé à diverses dérives. Or, aucune autre entité n'est acceptée par les juristes et la classe politique. Même la CNCDH voit ses avis traités avec une certaine commisération. Cette situation, dangereuse, induit des effets particuliers pour la captation des données informatiques qui ne présente aucune réelle garantie pour les acteurs et les utilisateurs.

Peut-être viendra le temps de la jurisprudence nationale et celui de la conformité à l'article huit de la Convention européenne des droits de l'homme. Il est trop tôt pour se prononcer en la matière.
La captation des images, des sons, des données informatiques, s'inscrit dans une société qui s'interroge sur son devenir en termes de libertés individuelles.[73] En effet, comme l'a signifié Mireille Delmas-Marty[74] : « *De ce point de vue, nous avons rencontré plusieurs exemples d'innovation pour résister au tout sécuritaire, qu'il s'agisse des cours constitutionnelles ou européennes. On pense notamment à la Cour européenne des droits de l'homme…apprenant à « raisonner la raison d'Etat » en contrôlant les limitations aux droits de l'homme. Autant d'efforts pour fortifier la justice, en utilisant non pas les forces de police ou les forces armées mais les forces imaginantes du droit* »

[71] www.rsf.org : site de Reporters sans frontière ; « Les logiciels espions inquiètent RSF », Zdnet, 29 juillet 2009.
[72] www.laquadrature.net : site de La quadrature du net ; Cf : présentation critique de la LOPPSI 2 sur le site.
[73] Cf à ce sujet, sur les exigences constitutionnelles telles que le respect de la vie privée et la prévention d'atteintes à l'ordre public, la conclusion du Conseil constitutionnel dans sa décision du 25 février 2010.
[74] Mireille Delmas-Marty, « Libertés et sûreté dans un monde dangereux », La couleur des idées, Le Seuil, 2010, p 247.