

## RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

### **La prise de connaissance d'e-mails « en cours de transmission », un parcours sans fin ?**

Lecroart, Elodie

*Published in:*  
Revue du Droit des Technologies de l'information

*Publication date:*  
2014

*Document Version*  
le PDF de l'éditeur

[Link to publication](#)

*Citation for published version (HARVARD):*  
Lecroart, E 2014, 'La prise de connaissance d'e-mails « en cours de transmission », un parcours sans fin ?', *Revue du Droit des Technologies de l'information*, numéro 57, pp. 19-41.

#### **General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

#### **Take down policy**

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

# La prise de connaissance d'e-mails « en cours de transmission », un parcours sans fin ?

Elodie Lecroart<sup>1</sup>

*L'essor d'Internet et des nouvelles technologies a bouleversé le secteur des communications et télécommunications. SMS, MMS, e-mail, Voice over IP et autres services ou applications témoignent du fait qu'il n'a jamais existé autant de moyens diversifiés de communiquer à distance et partout à travers le monde.*

*Or, force est de constater que ces modes de communication variés constituent également des outils privilégiés pour la mise en œuvre de pratiques illégales, d'usages détournés et d'actes criminels.*

*Afin de lutter efficacement contre ces formes de criminalités relativement récentes, le législateur se voit contraint d'adapter les dispositions pénales applicables, notamment afin de permettre la collecte de preuves relatives aux faits transitant par ces nouveaux modes de communication.*

*La présente contribution a pour objet principal d'analyser dans quelle mesure l'interception de courriers électroniques au cours d'une enquête judiciaire est rendue possible par le cadre légal belge actuel.*



*The Internet and new technologies' rise has revolutionized the communications and telecommunications sector. SMS, MMS, e-mail, Voice over IP and other services or applications testify the fact that it has never existed as many diverse ways of distant communication throughout the world as we have now.*

*However, it is clear that these various modes of communication can also be used as key tools to implement illegal practices, misuses and criminal acts.*

*To fight efficiently against these forms of quite recent criminality, the legislator is forced to adapt the applicable criminal provisions, in particular to allow the evidence gathering regarding facts transiting through these new ways of communication.*

*This paper's main purpose is to analyze how the interception of e-mails during a judicial procedure is made possible by the current Belgian legal framework.*

---

<sup>1</sup> Avocat au barreau de Namur.

## I. INTRODUCTION<sup>2</sup>

1. Si les nouveaux moyens de communication constituent un canal idéal pour l'organisation et la réalisation de crimes et délits, ils ouvrent également la possibilité de recours à des méthodes pointues de recherche qui ont vu le jour pour lutter contre la criminalité organisée<sup>3</sup>. Ainsi, il est désormais possible d'identifier l'utilisateur d'un téléphone mobile ou d'une adresse de courrier électronique, de localiser un appareil à distance, d'écouter et d'enregistrer des communications téléphoniques,...

2. Or, ces méthodes, dès lors qu'elles concernent des (télé)communications à caractère privé, qui sont un lieu d'expression privilégié de la vie privée<sup>4</sup>, doivent impérativement être entourées de garanties suffisantes, afin d'éviter les travers d'une société dite « de surveillance »<sup>5</sup>.

Ainsi, bien que les États disposent, face à la nécessité de prévenir les menaces liées au terrorisme et aux formes modernes de criminalité organisée, de la légitimité nécessaire pour s'ingérer dans la vie privée des personnes

soupçonnées de représenter un risque pour la collectivité, ils ne peuvent toutefois recourir à des mesures qui risqueraient « de saper, voire de détruire, la démocratie au motif de la défendre »<sup>6</sup>. La nécessité de trouver un équilibre entre la prévention des crimes et la sauvegarde des droits et libertés individuels est donc indispensable.

3. En Belgique, le Code d'instruction criminelle a été modifié à plusieurs reprises afin de permettre aux autorités judiciaires de procéder à des mesures de surveillance à l'égard des (télé)communications. En particulier, la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées<sup>7</sup>, bien qu'elle ait posé le principe de l'interdiction de pratiquer des écoutes, a surtout organisé les exceptions au principe et décrit d'une manière détaillée les conditions et les règles applicables à la mise en œuvre de ce type de mesures<sup>8</sup>.

À l'origine, la loi visait essentiellement l'écoute de conversations téléphoniques. Très vite, son champ d'application est apparu trop limité par rapport aux nouveaux modes de communication et à l'évolution de la criminalité de grande envergure. Malgré les tentatives d'adaptation de l'écoute téléphonique aux réalités nouvelles d'Internet et des réseaux de communication, il faut reconnaître que le texte de la loi laisse, aujourd'hui encore, une large place à l'interprétation<sup>9</sup>.

<sup>2</sup> La présente contribution est basée sur le mémoire présenté par l'auteur dans le cadre du Master complémentaire en droit des nouvelles technologies de l'information et de la communication en août 2014 à l'Université de Namur. L'auteur tient à remercier chaleureusement son promoteur, M. Olivier Leroux, juge d'instruction au tribunal de première instance francophone de Bruxelles, pour ses conseils avisés lors de la préparation de ce mémoire ainsi que ses remarques précieuses lors de sa défense.

<sup>3</sup> L. KENNES, *Manuel de la preuve en matière pénale*, Waterloo, Kluwer, 2009, p. 225.

<sup>4</sup> C. DE VALKENEER, « Les infractions en matière d'écoutes, de prise de connaissance et d'enregistrement de communications et de télécommunications », in *Les infractions – Volume 5: les infractions contre l'ordre public* (sous la dir. de H.-D. BOSLY et C. DE VALKENEER), Bruxelles, Larcier, 2013, p. 395.

<sup>5</sup> E. LABBÉ, « L'interception légale de communications électroniques privées: approche comparée d'un moyen d'enquête plus ou moins 'branché' », *R.D.T.I.*, 2008, p. 174.

<sup>6</sup> Cour eur. D.H., 6 septembre 1978, arrêt *Klass et autres c. Allemagne*, § 49.

<sup>7</sup> Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, *M.B.*, 24 janvier 1995, p. 1542.

<sup>8</sup> A. SADZOT, « Les écoutes, la prise de connaissance et l'enregistrement des (télé)communications privées après la loi du 10 juin 1998 », in *Le point sur les procédures*, Liège, CUP, 2000, p. 228.

<sup>9</sup> E. LABBÉ, *op. cit.*, p. 160.

4. Actuellement, l'utilisation du courrier électronique est considérée comme un des services les plus utilisés sur Internet, tant à des fins privées que professionnelles. Dans le cadre d'enquêtes judiciaires, la prise de connaissance du contenu d'un message transmis par courrier électronique peut naturellement s'avérer intéressante. Dès lors, la question se pose de savoir si la mesure prévue pour les écoutes téléphoniques peut être transposée aux e-mails afin que le juge d'instruction soit en mesure d'en ordonner l'interception.

5. Selon le dernier rapport publié du Service de la Politique criminelle, pas moins de 6.712 mesures d'écoute ont été exécutées en 2012, et ce chiffre est en évolution constante<sup>10</sup>. Parmi ces mesures d'écoute, la majorité (68%) vise un numéro de GSM. Par contre, aucune mesure d'écoute n'a été répertoriée jusqu'à présent pour les e-mails, selon le même rapport<sup>11</sup>.

6. Après avoir rappelé le cadre légal consacrant le principe du secret de la correspondance et des communications en Belgique (II), nous examinerons les dispositions du Code d'instruction criminelle autorisant l'écoute, la prise de connaissance et l'enregistrement de communications et télécommunications à caractère privé (III). Nous nous intéresserons aux difficultés posées par l'application de ces dispositions aux e-mails et tenterons de démontrer la nécessité d'une intervention législative clarificatrice en la matière.

## II. LA PROTECTION DU SECRET DES COMMUNICATIONS

7. Avant d'évoquer les circonstances exceptionnelles dans lesquelles il peut être, légalement, procédé à l'interception de (télé) communications, il est important de rappeler que les communications, de quelque type qu'elles soient, sont en principe couvertes par la garantie du secret.

### A. Le secret de la correspondance

8. Le secret de la correspondance, en tant qu'application particulière du droit au respect de la vie privée, est garanti par l'article 8.1 de la Convention européenne de sauvegarde des droits de l'homme (ci-après C.E.D.H) qui dispose que: «Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance», ainsi que par l'article 17.1 du Pacte international relatif aux droits civils et politiques<sup>12</sup>.

9. Au niveau belge, le droit au respect de la vie privée consacré à l'article 22, alinéa 1<sup>er</sup>, de la Constitution<sup>13</sup> ne mentionne pas expressément le droit au respect de la correspondance. Cela s'explique par le fait que dès 1831, le constituant belge a prévu une protection spécifique de celle-ci à l'article 29 de la Constitution: «Le secret des lettres est inviolable. La loi détermine quels sont les agents responsables de la violation du secret des lettres confiées à la poste».

Le secret des lettres est, en Belgique, assorti d'une incrimination pénale énoncée à l'article 460 du Code pénal qui sanctionne d'une

<sup>10</sup> Rapport 2013 en application de l'article 90*decies* du Code d'instruction criminelle (2012), Service de la Politique criminelle, disponible sur <http://www.dsb-spc.be> (2 juillet 2014), p. 9.

<sup>11</sup> Rapport 2013 en application de l'article 90*decies* du Code d'instruction criminelle (2012), *op. cit.*, pp. 9-10.

<sup>12</sup> Article 17 du Pacte international relatif aux droits civils et politiques: «Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation».

<sup>13</sup> Article 22 de la Constitution: «Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi».

peine d'emprisonnement allant de huit jours à un mois et/ou d'une amende comprise entre vingt-six et deux cents euros « quiconque sera convaincu d'avoir supprimé une lettre confiée (à un opérateur postal), ou de l'avoir ouverte pour en violer le secret » et ce, « sans préjudice des peines plus fortes, si le coupable est un fonctionnaire ou un agent du gouvernement ou (un membre du personnel d'un opérateur postal ou toute personne agissant pour son compte) ».

**10.** Bien qu'il s'agisse d'un droit fondamental, le secret des lettres n'est pas un droit absolu et peut souffrir certaines exceptions<sup>14</sup>. Cela a été confirmé par la Cour constitutionnelle dans un arrêt du 21 décembre 2004 où elle précise que « si le secret des lettres a pu être conçu comme absolu, lors de l'adoption de la Constitution, il ne peut être fait abstraction aujourd'hui, pour en déterminer la portée, d'autres dispositions constitutionnelles ainsi que de conventions internationales »<sup>15</sup>. Selon la Cour, même si l'article 29 de la Constitution ne prévoit pas explicitement de restriction au secret des lettres, le législateur doit, afin de prévenir les atteintes à d'autres droits fondamentaux tels que la liberté individuelle, le droit à la vie, ou encore le droit de propriété, être en mesure d'organiser une répression efficace des atteintes portées à ces droits par des activités criminelles, pour autant que les restrictions soient proportionnées au but légitime poursuivi. La Cour ajoute que « la prise de connaissance de la correspondance d'une personne soupçonnée de commettre des infractions par les autorités judiciaires fait

partie des mesures qui peuvent être utilisées en vue de lutter de manière efficace contre certaines formes de criminalité ».

Actuellement, l'interception et la saisie de courrier d'une part, et la prise de connaissance de son contenu d'autre part, sont organisées respectivement par les articles 46ter, § 1<sup>er</sup> et 88sexies, § 1<sup>er</sup>, du Code d'instruction criminelle<sup>16</sup>.

**11.** Le champ d'application de la protection dont fait l'objet la correspondance en vertu de l'article 29 de la Constitution et de l'article 460 du Code pénal mérite d'être précisé à plusieurs égards.

Ainsi, en ce qui concerne l'objet de la protection, les lettres doivent être entendues comme visant tout « échange épistolaire confié à la poste ou un organisme chargé de la distribution du courrier »<sup>17</sup>. Il ressort des travaux préparatoires de la loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête que ne sont visés, au sens de la Constitution, que les « lettres et petits paquets postaux » traditionnels, à savoir les « courriers ouverts et fermés, cartes postales, imprimés, circulaires, paquets postaux, avis, télégrammes, envois recommandés, courriers transfrontaliers, etc. »<sup>18</sup>.

De plus, en ce qui concerne la détermination de la durée de la protection, celle-ci donne lieu à des divergences d'interprétation. Pour

<sup>14</sup> R. ROBERT, « Correspondance et vie privée sur les lieux de travail: une cohabitation difficile », *Orientations*, 2008, p. 17; Projet de loi relatif à la loi concernant les méthodes particulières de recherche et autres méthodes d'investigation, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2001-2002, n° 50-1688/1, p. 53.

<sup>15</sup> C. const., 21 décembre 2004, n° 202/2004, disponible sur [www.const-court.be](http://www.const-court.be), B.12.2.

<sup>16</sup> Insérés par la loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête, *M.B.*, 12 mai 2003, p. 25351. La saisie et l'interception du courrier peuvent être autorisées par le procureur du Roi tandis que l'ouverture du courrier requiert l'intervention du juge d'instruction, hormis le cas du flagrant délit.

<sup>17</sup> C. trav. Liège, 25 avril 2002, *Rev. rég. dr.*, 2002, p. 271, note F. LAGASSE; R. ROBERT, *op. cit.*, p. 20.

<sup>18</sup> Projet de loi relatif à la loi concernant les méthodes particulières de recherche et autres méthodes d'investigation, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2001-2002, n° 50-1688/1, p. 55-56.

certain, il faut considérer que la protection s'applique aux lettres depuis « leur remise à un agent de la poste ou dans une boîte postale jusqu'à leur remise en mains propres ou dans la boîte du destinataire »<sup>19</sup> et ce, peu importe le mode de transport<sup>20</sup>. Ainsi, les courriers qui ne sont pas encore ou qui ne sont plus confiés à la poste ne bénéficient pas du secret<sup>21</sup>. Pour d'autres, cette interprétation va à l'encontre de la protection offerte par l'article 8 de la C.E.D.H. qui paraît s'étendre également aux lettres non encore envoyées ou, au contraire, arrivées depuis un certain temps déjà à destination<sup>22</sup>.

## 12. Qu'en est-il du courrier électronique ?

En France, le Tribunal de Grande Instance de Paris a dû se prononcer sur la nature juridique du courrier électronique dans une affaire relative à l'altération et à la disparition des e-mails d'un chercheur au sein d'un laboratoire. Le tribunal, après avoir considéré que « la messagerie électronique permet de transmettre un message écrit d'une personne à une autre, de

manière analogue au courrier. Il en résulte que l'envoi de message électronique de personne à personne constitue de la correspondance privée », a conclu à la violation des dispositions pénales en matière de secret des correspondances<sup>23</sup>.

Une telle assimilation pourrait-elle être réalisée en Belgique ? Rappelons que prévaut chez nous un grand principe qu'est celui de l'interprétation stricte du droit pénal. Il est donc peu probable que l'e-mail soit considéré, au sens du droit pénal, comme l'équivalent du courrier postal. L'article 460 du Code pénal est, en effet, rédigé de façon assez stricte et emploie les termes précis de « lettres » et d'« opérateur postal » qui peuvent difficilement s'appliquer aux courriers électroniques.

Les travaux préparatoires relatifs à la loi du 6 janvier 2003 ayant introduit les mesures de saisie et d'ouverture du courrier, tendent également à confirmer cette affirmation. En effet, alors que le Conseil d'État avait, durant les débats, soulevé la question de savoir ce que recouvrait exactement la notion de « courrier » au sens des dispositions en projet<sup>24</sup>, le Gouvernement avait répondu que seul pouvait être intercepté sur base de ces dispositions le courrier classique<sup>25</sup> et non pas les envois électroniques (e-mails).

<sup>19</sup> D. FESLER, « Confidentialité, sécurité et électronique au quotidien – L'expérience du barreau », in *Le droit des affaires en évolution – Le contrat sans papier*, Bruxelles-Anvers, Bruylant-Kluwer, 2003, p. 166.

<sup>20</sup> Projet de loi relatif à la loi concernant les méthodes particulières de recherche et autres méthodes d'investigation, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2001-2002, n° 50-1688/1, pp. 55-56.

<sup>21</sup> En ce sens, voy. Anvers, 25 janvier 2001, *Limb. Rechtsl.*, 2001, p. 156 (où la Cour a considéré qu'une lettre n'était plus protégée lorsqu'une fois délivrée, elle n'est plus confiée au service postal); R. ROBERT, *op. cit.*, p. 20.

<sup>22</sup> Projet de loi relatif à la loi concernant les méthodes particulières de recherche et autres méthodes d'investigation, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2001-2002, n° 50-1688/1, pp. 55-56. En ce sens, voy. Mons, 16 février 2004, *J.T.*, 2005, p. 582 (jugant que le secret était garanti non seulement « avant leur ouverture, pendant leur acheminement, par l'obligation imposée de respecter toute la correspondance, sans distinction, puisqu'il s'agit d'assurer à tous la faculté de communiquer sans contrainte » mais aussi « après leur ouverture, par l'obligation de ne pas divulguer les renseignements relatifs à la vie privée qui pourraient y être consignés »); R. ROBERT, *op. cit.*, p. 20.

<sup>23</sup> T.G.I. Paris (17<sup>e</sup> ch.), 2 novembre 2000, disponible sur [www.legalis.net](http://www.legalis.net). Pour un commentaire de cette décision, voy. A. BLOCMAN, « Le courrier électronique protégé par le secret des correspondances », *Iris*, 2000-10/17, p. 17, disponible sur <http://merlin.obs.coe.int>.

<sup>24</sup> Projet de loi concernant les méthodes particulières de recherche et autres méthodes d'investigation, Rapport fait au nom de la Commission, *Doc. parl.*, Ch. repr., sess. ord. 2001-2002, n° 50-1688/13, pp. 55-56 et 103; Projet de loi relatif à la loi concernant les méthodes particulières de recherche et autres méthodes d'investigation, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2001-2002, n° 50-1688/1, p. 103.

<sup>25</sup> Il est fait renvoi, pour la notion de « courrier », à l'article 131, 4<sup>e</sup>, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques:

13. Si, au regard du droit pénal, l'e-mail semble clairement exclu du bénéfice de la protection de l'article 460 précité, la question demeure davantage controversée en doctrine et en jurisprudence concernant le bénéfice de la protection accordée par l'article 29 de la Constitution<sup>26</sup>.

En effet, alors que certaines juridictions font expressément référence à la protection de l'article 29 de la Constitution à l'occasion de litiges relatifs à la surveillance des e-mails d'un travailleur par son employeur<sup>27</sup>, d'autres tiennent le

raisonnement opposé et excluent l'e-mail du bénéfice de la garantie constitutionnelle du secret des lettres<sup>28</sup>.

## B. Le secret des communications électroniques

14. Même à considérer que la garantie du secret des lettres consacrée par l'article 29 de la Constitution ne s'appliquerait pas aux courriers électroniques, cela ne signifierait pas pour autant que les e-mails seraient dénués de toute protection. Il existe, en effet, d'autres dispositions pouvant protéger, au même titre que le secret des lettres pour le courrier papier, le secret des communications électroniques pour le courrier électronique<sup>29</sup>.

15. Ainsi, l'article 8 de la C.E.D.H. et ses corollaires en droit belge que sont l'article 22 de la Constitution et la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel<sup>30</sup> couvrent également le secret des communications électroniques<sup>31</sup>. Cela a été rappelé par la

« toute correspondance ou envoi, personnel ou impersonnel, écrit ou imprimé obtenu par un quelconque procédé de reproduction, clos ou non clos, sous bande ou à découvert, affranchi ou non, périodique ou non, déposé à titre onéreux ou gratuit par une personne physique ou morale en vue de sa distribution à un ou des tiers, en ce compris les correspondances dont le dépôt ou l'acheminement s'effectue, à la demande et aux frais du déposant, dans des conditions spécifiques, telles notamment la recommandation, la déclaration de valeur, l'accusé de réception, le traitement express ou accéléré, acheminé par toutes voies ».

<sup>26</sup> À ce propos, voy. J.-T. DEBRY, « Le droit constitutionnel à l'épreuve de la société de l'information », *Act. dr.*, 2002, p. 22, n° 14 et note 35, qui considère que la garantie de l'article 29 de la Constitution peut être étendue aux e-mails. D'autres auteurs défendent eux la thèse selon laquelle ni l'article 29 de la Constitution, ni l'article 460 du Code pénal ne s'appliquent aux e-mails. En ce sens, voy. F. DELPÈRE, *Le droit constitutionnel de la Belgique*, Bruxelles, Bruylant, Paris, p. 218; T. CLAEYS et D. DEJONGHE, « Gebruik van e-mail en internet op de werkplaats en controle door de werkgever », *J.T.T.*, 2001, p. 129; D. FESLER, *op. cit.*, p. 166; R. ROBERT, *op. cit.*, p. 19.

<sup>27</sup> En ce sens, voy. Trib. trav. Liège (3<sup>e</sup> ch.), 3 septembre 2008, p. 8, disponible sur [www.cass.be](http://www.cass.be) et Trib. trav. Liège (3<sup>e</sup> ch.), 19 mars 2008, p. 18, disponible sur [www.cass.be](http://www.cass.be), qui énoncent à propos d'un e-mail que « le caractère mixte de l'échange de correspondance lui enlève son caractère strictement professionnel, de sorte que les principes constitutionnels du secret des lettres et de respect de la vie privée doivent s'appliquer dans toute leur rigueur »; Trib. trav. Verviers (1<sup>re</sup> ch.), 20 mars 2002, *J.T.T.*, 2002, p. 183, qui considère que le comportement de l'employeur ayant consulté et copié les e-mails d'un employé préalablement au licenciement de celui-ci pour motif grave constitue une violation de l'article 29 de la Constitution et de l'article 8 C.E.D.H.

<sup>28</sup> En ce sens, voy. C. trav. Liège, 25 avril 2002, *Rev. rég. dr.*, 2002, p. 272, note F. LAGASSE et C. trav. Liège, 23 mars 2004, *Rev. rég. dr.*, 2004, p. 73 (somm.). Dans ces affaires, la Cour considère que les envois par courrier électronique doivent plutôt être assimilés à des communications téléphoniques compte tenu de leur mode de transmission.

<sup>29</sup> K. ROSIER, « Droit social : contrôle de l'usage des technologies de l'information et de la communication dans les relations de travail », *R.D.T.I.*, 2009, n° 35, p. 128.

<sup>30</sup> Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5801.

<sup>31</sup> Dans l'arrêt *Klass et autres c. Allemagne* précité, la Cour dit expressément que : « Quoique le paragraphe 1 de l'article 8 ne mentionne pas les conversations téléphoniques, elles se retrouvent comprises dans les notions de "vie privée" et de "correspondance" visées par ce texte », § 41. En ce sens, voy. également l'arrêt précité de la Cour du travail de Liège du 25 avril 2002 où la juridiction, après avoir exclu les courriers électroniques de la protection du secret de la correspondance, estime toutefois que les articles 22 de la Constitution et 8 de la C.E.D.H. leur sont applicables

Cour européenne des droits de l'homme dans un arrêt *Kennedy c. Royaume-Uni* du 18 mai 2010: «Il n'est pas contesté que la correspondance et les communications téléphoniques et électroniques, y compris celles qui concernent le domaine professionnel, sont couvertes par les notions de «vie privée» et de «correspondance» au sens de l'article 8.1»<sup>32</sup>.

**16.** À cette protection générale des communications électroniques s'ajoute une protection plus spécifique garantie par deux lois. D'une part, la loi du 13 juin 2005 relative aux communications électroniques<sup>33</sup> dont l'article 124 interdit à toute personne qui n'y est pas autorisée de prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique<sup>34</sup>.

D'autre part, la loi du 30 juin 1994<sup>35</sup> a introduit les articles 259bis et 314bis dans le Code pénal en vue de sanctionner toute interception du contenu d'un courrier électronique pendant sa transmission.

**17.** Il est important de noter qu'avant 1994, le droit pénal belge ne disposait d'aucune disposition générale ayant pour objet la protec-

tion pénale des communications et des télécommunications privées<sup>36</sup>. Même si l'écoute téléphonique était, d'une certaine manière, déjà interdite par une série de dispositions éparses, ces dispositions n'étaient pas adaptées à la technologie des communications modernes et avaient une portée trop limitée<sup>37</sup>. Les articles 259bis et 314bis du Code pénal ont ainsi consacré l'élargissement du champ de protection accordée jusque-là aux conversations téléphoniques en l'étendant aux communications et télécommunications<sup>38</sup>.

**18.** L'article 314bis du Code pénal, en son paragraphe 1<sup>er</sup>, punit d'un emprisonnement allant de six mois à un an et/ou d'une amende comprise entre deux cents euros et dix mille euros toute personne qui «soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications; soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque»<sup>39</sup>.

étant donné que le respect de la vie privée englobe non seulement le secret des lettres mais également «tout écrit confidentiel même s'il ne peut être qualifié de correspondance au sens où l'entendent les articles 29 de la Constitution et 460 du Code pénal».

<sup>32</sup> Cour eur. D.H., 18 mai 2010, arrêt *Kennedy c. Royaume-Uni*, § 118.

<sup>33</sup> Loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005, p. 28070.

<sup>34</sup> Cet article remplace l'article 109terD de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (*M.B.*, 27 mars 1991, p. 6155), dite «Loi Belgacom», qui proscrivait la prise de connaissance frauduleuse, et sans l'accord de toutes les personnes directement ou indirectement concernées, de communications électroniques.

<sup>35</sup> Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, *M.B.*, 24 janvier 1995, p. 1542.

<sup>36</sup> C. DE VALKENEER, «Les infractions en matière d'écoutes, de prise de connaissance et d'enregistrement de communications et de télécommunications», *op. cit.*, p. 394; T. FREYNE, «De bewaking van privécommunicatie en -telecommunicatie in strafonderzoeken: een stand van zaken», *T. Strafr.*, 2008/3, p. 166.

<sup>37</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Sén., sess. ord. 1992-1993, n° 843-2, pp. 7-8.

<sup>38</sup> C. DE VALKENEER, «Les infractions en matière d'écoutes, de prise de connaissance et d'enregistrement de communications et de télécommunications», *op. cit.*, p. 394.

<sup>39</sup> La disposition, en ses paragraphes 3 et 4, sanctionne également la tentative de perpétrer une telle infraction et le cas de récidive spécifique.

L'article 259bis du Code pénal réprime quant à lui plus lourdement ces mêmes faits lorsqu'ils sont commis par des officiers ou des fonctionnaires publics dans le cadre de l'exercice de leurs fonctions.

**19.** Ces dispositions s'appliquent, de manière générale, aux communications et télécommunications, à savoir «les conversations ou déclarations directes et les conversations téléphoniques mais également, au sens large, toutes les formes modernes de la télématique»<sup>40</sup>, en ce compris les télécopies et les courriers électroniques<sup>41</sup>.

Pour être punissable, l'infraction doit remplir les conditions suivantes: viser une communication ou télécommunication à caractère privé et avoir lieu pendant sa transmission<sup>42</sup>. Enfin, la loi précise qu'il doit avoir été fait usage d'un matériel d'assistance technique<sup>43</sup>.

En ce qui concerne l'élément moral de l'infraction, l'article requiert une intention de la part de l'auteur. Comme l'expliquent les travaux préparatoires, une simple indiscretion ou une pure coïncidence ne sera pas punie. Quant

aux personnes chargées de l'entretien ou de la surveillance du réseau téléphonique public ou privé, elles ne se rendent pas coupables d'une telle infraction lorsque, dans le cadre de leur fonction, elles interceptent certaines bribes de conversation pour s'assurer du bon fonctionnement de la liaison<sup>44</sup>.

**20.** En vertu de ces dispositions, toute personne qui prendrait intentionnellement connaissance d'un e-mail qui ne lui est pas destiné, au cours de sa transmission et à l'insu de son destinataire pourrait être poursuivie sur base des articles 314bis ou 259bis du Code pénal, à moins, comme exposé ci-après, de remplir les conditions énoncées aux articles 90ter et suivants du Code d'instruction criminelle<sup>45</sup>.

### III. L'ÉCOUTE, LA PRISE DE CONNAISSANCE ET L'ENREGISTREMENT DE (TÉLÉ) COMMUNICATIONS PRIVÉES

**21.** Malgré l'interdiction de principe énoncée aux articles 314bis et 259bis du Code pénal, les articles 90ter et suivants du C.i.cr. permettent, à certaines conditions, d'écouter, de prendre connaissance ou d'enregistrer des (télé) communications à caractère privé si cela s'avère nécessaire dans le cadre d'une enquête judiciaire.

#### A. Le champ d'application des articles 90ter et suivants du C.i.cr.

##### 1. *Ratio legis et balance avec le droit au respect de la vie privée*

**22.** Outre la volonté de consacrer dans une seule disposition générale le principe de l'inter-

<sup>40</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Exposé des motifs, *Doc. parl., Sén., sess. ord. 1992-1993*, n° 843-1, p. 3.

<sup>41</sup> J. MASSON, «Le secret des communications», in *Les droits de la personnalité – Actes du X<sup>e</sup> Colloque de l'Association «Famille et Droit» du 30 novembre 2007*, Bruxelles, Bruylant, 2007, p. 250.

<sup>42</sup> Nous reviendrons plus amplement sur la portée de ces notions dans le chapitre suivant.

<sup>43</sup> Voy. Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Exposé des motifs, *Doc. parl., Sén., sess. ord. 1992-1993*, n° 843-1, p. 6: «L'expression "à l'aide d'un appareil quelconque" a, il est vrai, un sens étendu mais cependant suffisamment précis. D'ailleurs on ne voit pas comment on pourrait définir ces moyens techniques sans courir le risque de voir les définitions très rapidement dépassées par l'évolution technologique».

<sup>44</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Exposé des motifs, *Doc. parl., Sén., sess. ord. 1992-1993*, n° 843-1, p. 6.

<sup>45</sup> Ci-après C.i.cr.

diction de pratiquer des écoutes, les auteurs de la loi du 30 juin 1994 poursuivaient le principal objectif de renforcer la protection de la société contre le terrorisme et la grande criminalité en autorisant, à certaines conditions, l'interception de (télé)communications privées<sup>1</sup>. Une telle mesure a été introduite par la loi aux articles 90ter et suivants du C.i.cr.

**23.** Étant donné le caractère particulièrement intrusif d'une telle mesure dans le droit au respect de la vie privée des citoyens, le recours à celle-ci doit être limité à des circonstances exceptionnelles et est soumis à des conditions très strictes<sup>2</sup>.

**24.** En effet, bien que l'article 8 de la C.E.D.H. protège le secret des (télé)communications au nom du droit au respect de la vie privée, la Cour de Strasbourg admet, en application du paragraphe 2 du même article, que des mesures secrètes de surveillance de la correspondance, des envois postaux et des télécommunications soient prévues par les législateurs nationaux et ce, afin de lutter efficacement contre le terrorisme et la criminalité organisée<sup>3</sup>.

La Cour européenne des droits de l'homme n'a toutefois cessé, au fil de sa jurisprudence, d'affermir les critères de légalité, de légitimité

et de proportionnalité requis pour qu'une loi puisse valablement déroger à l'article 8.1 de la C.E.D.H. Ainsi, dans l'arrêt *Malone*, la Cour a clairement établi que le critère de légalité comprenait également une exigence de qualité de la loi<sup>4</sup>. Dans les arrêts *Huvig* et *Kruslin*<sup>5</sup>, la Cour a rappelé cette obligation qu'a la loi interne d'être accessible et prévisible pour le justiciable<sup>6</sup>.

**25.** En Belgique, la Cour de cassation a été amenée à examiner la conformité de l'article 90ter du C.i.cr. aux exigences imposées par l'article 8.2 de la C.E.D.H. Dans un arrêt du 26 mars 2003, elle a déclaré que la disposition permettant à l'autorité publique d'exercer une ingérence dans l'exercice du droit au respect de la vie privée des citoyens était « une norme accessible aux personnes concernées et énoncée de manière précise »<sup>7</sup>.

En effet, comme nous le verrons, l'article 90ter, § 1<sup>er</sup>, 1<sup>er</sup> alinéa du C.i.cr. prévoit que le juge d'instruction peut uniquement ordonner une

<sup>1</sup> H.-D. BOSLY et D. VANDERMEERSCH, « La loi belge du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement des communications et télécommunications privées », *Rev. dr. pén.*, 1995, p. 301.

<sup>2</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Exposé des motifs, *Doc. parl.*, Sén., sess. ord. 1992-1993, n° 843-1, pp. 1, 5, 11-12; H.-D. BOSLY et D. VANDERMEERSCH, *op. cit.*, p. 301.

<sup>3</sup> Cour eur. D.H., 6 septembre 1978, arrêt *Klass et autres c. Allemagne*, <http://hudoc.echr.coe.int>, § 48; Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Avis du Conseil d'État, *Doc. parl.*, Sén., sess. ord. 1992-1993, n° 843-1, pp. 37-38.

<sup>4</sup> Cour eur. D.H., 2 août 1984, arrêt *Malone c. Royaume-Uni*. Voy. § 67 de l'arrêt où la Cour affirme qu'une telle loi doit « user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à opérer pareille atteinte secrète, et virtuellement dangereuse, au droit au respect de la vie privée et de la correspondance ».

<sup>5</sup> Cour eur. D.H., 24 avril 1990, arrêt *Huvig c. France*, § 32 et Cour eur. D.H., 24 avril 1990, arrêt *Kruslin c. France*, § 33. Dans ces deux arrêts, la Cour dit : « Les écoutes et autres formes d'interception des entretiens téléphoniques représentent une atteinte grave au respect de la vie privée et de la correspondance. Partant, elles doivent se fonder sur une "loi" d'une précision particulière. L'existence de règles claires et détaillées en la matière apparaît indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner ».

<sup>6</sup> Pour un examen plus détaillé de la jurisprudence de la Cour européenne des droits de l'homme à propos du respect de l'article 8 de la C.E.D.H. dans le cadre des écoutes téléphoniques, voy. T. HENRION, « Écoutes téléphoniques », *Postal Memorialis*, 2009, pp. 7-18.

<sup>7</sup> Cass. (2<sup>e</sup> ch.), 26 mars 2003, *J.T.*, 2003, p. 626.

telle mesure « s'il existe des indices sérieux que le fait dont il est saisi constitue une infraction visée par l'une des dispositions énumérées au § 2, et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité ». L'exception ne concerne donc qu'une liste limitative de faits et est soumise aux principes de proportionnalité et de subsidiarité afin d'assurer son caractère exceptionnel<sup>8</sup>.

## 2. Notions

**26.** Si les auteurs de la loi du 30 juin 1994 avaient essentiellement à l'esprit, lors de sa rédaction, la mesure de l'écoute téléphonique<sup>9</sup>, son champ d'application est toutefois plus étendu et vise en réalité l'écoute, la prise de connaissance et l'enregistrement de tout type de (télé)communications privées en cours de transmission<sup>10</sup>. La loi ne se prononce cependant pas sur la portée de ces différents termes.

**27.** Par écoute, il y a lieu d'entendre « une mesure de surveillance secrète d'une communication téléphonique ou d'une communication verbale directe entre personnes »<sup>11</sup>. L'expression « prise de connaissance » est quant à elle plus large et comprend des formes plus techniques de communication comme le transfert de données entre des systèmes informatiques<sup>12</sup>. Quant à la notion d'enregistrement,

elle fait référence à la fixation des données sur un support<sup>13</sup>.

**28.** Concernant les notions de télécommunications et de communications, celles-ci doivent être, selon les travaux préparatoires de la loi, utilisées dans leur sens usuel et bénéficient d'une portée étendue<sup>14</sup>. Ainsi, pour la notion de « télécommunications », il est fait référence à la définition donnée par l'article 68, 4°, de la loi Belgacom du 21 mars 1991, à savoir: « Toute transmission, émission ou réception de signes, de signaux, d'écrit, d'images, de sons ou de données de toute nature, par fil, radioélectricité, signalisation optique ou autre système électromagnétique »<sup>15</sup>.

**29.** Les communications sont, elles, définies comme « tout énoncé oral ou non, directement ou à distance, quel que soit le nombre de personnes concernées »<sup>16</sup>. Dans un arrêt du 26 mars 2003 déjà mentionné, la Cour de cassation a, en partie, repris cette définition, de sorte que sont visés les monologues, l'enregistrement et l'écoute d'un texte sur dictaphone, de même que les télégrammes, les télex, les télécopies et la transmission électronique de

<sup>8</sup> H.-D. BOSLY et D. VANDERMEERSCH, *op. cit.*, p. 340.

<sup>9</sup> La loi est d'ailleurs souvent évoquée dans la pratique par les termes de « loi sur les écoutes téléphoniques ».

<sup>10</sup> D. VANDERMEERSCH, *Les recherches en matière de téléphonie et de (télé)communications*, Bruxelles, Éditions du Jeune Barreau, 2006, p. 49.

<sup>11</sup> T. HENRION, « Écoutes téléphoniques », *Postal Mémoires*, 2009, p. 25; L. KENNES, *op. cit.*, p. 205.

<sup>12</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Rapport fait au nom de la Commission de la Justice, *Doc. parl., Sén., sess. ord. 1992-1993*, n° 843-2, p. 11.

<sup>13</sup> T. HENRION, *op. cit.*, p. 25; L. KENNES, *op. cit.*, p. 205.

<sup>14</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Exposé des motifs, *Doc. parl., Sén., sess. ord. 1992-1993*, n° 843-1, p. 7.

<sup>15</sup> C. DE VALKENEER, « Les infractions en matière d'écoutes, de prise de connaissance et d'enregistrement de communications et de télécommunications », *op. cit.*, p. 396; T. CLAEYS et D. DEJONGHE, *op. cit.*, p. 126; L. ARNOU, « Afluisteren tijdens het gerechtelijk onderzoek », in *Commentaar Strafrecht en Strafvoeding*, Mechelen, Kluwer, 2008, p. 25.

<sup>16</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Exposé des motifs, *Doc. parl., Sén., sess. ord. 1992-1993*, n° 843-1, p. 7; M. PREUMONT, « Les informations bancaires et l'interception des communications », in *L'enquête, les poursuites et les sanctions*, coll. O.B.F.G., Limal, Anthemis, 2011, p. 125.

données dans des ordinateurs ou des réseaux d'ordinateurs<sup>17</sup>.

**30.** Certains critiquent toutefois cette définition pour un double motif. D'une part, la définition serait trop vaste et laisserait également entrer dans le champ d'application de la loi toute correspondance écrite étant donné qu'il s'agit d'un énoncé non verbal émis à distance. Il en irait de même d'un geste provocateur ou insultant<sup>18</sup>.

D'autre part, elle serait trop étroite lorsqu'elle requiert un « énoncé » car elle ne prendrait dès lors pas en compte les photos et dessins qui seraient faxés ou envoyés par Internet et qui peuvent également être interceptés par le juge d'instruction<sup>19</sup>.

**31.** Quoi qu'il en soit, doctrine et jurisprudence s'accordent pour dire que les courriers électroniques et les messages textuels (« SMS ») entrent dans le champ d'application de la loi<sup>20</sup>, alors que le surf sur Internet semble lui être exclu étant donné qu'il ne s'agit pas d'une communication entre deux personnes<sup>21</sup>.

**32.** En outre, rappelons que seules les communications à caractère privé tombent sous le champ d'application de la loi. Elles peuvent se prévaloir de ce caractère à partir du moment où elles ne sont pas destinées à être entendues par tout un chacun<sup>22</sup>. Dès lors, le lieu où

cette communication est émise ou est reçue ne revêt aucune importance<sup>23</sup>. Le caractère privé de la communication dépendra seulement et uniquement de l'intention des participants et du contexte dans lequel elle prendra place<sup>24</sup>.

**33.** Enfin, la loi ne s'applique qu'aux interceptions qui ont lieu « pendant la transmission, c'est-à-dire sur le trajet entre l'émetteur et le récepteur »<sup>25</sup>. Nous reviendrons sur cette notion, à l'apparence simple mais dont l'application en pratique se révèle complexe.

### 3. Régime

**34.** L'intérêt de cette contribution n'étant pas de revenir en détail sur le régime légal des articles 90ter et suivants du C.i.cr., nous nous contenterons de rappeler brièvement les principales conditions de fond et de formes auxquelles doit répondre une mesure d'écoute pour être légale.

**35.** Tout d'abord, il revient à la compétence exclusive du juge d'instruction de faire procéder, dans le cadre d'une instruction, à des interceptions et enregistrements de (télé)communications privées<sup>26</sup>. Pour autoriser une

---

gistrement de communications et de télécommunications privées, Exposé des motifs, *Doc. parl., Sén., sess. ord. 1992-1993*, n° 843-1, p. 7.

<sup>23</sup> H.-D. BOSLY et D. VANDERMEERSCH, *op. cit.*, p. 305.

<sup>24</sup> L. ARNOU, *op. cit.*, p. 28. Pour une application de ce principe aux communications tenues dans le cadre professionnel, voy. T. CLAEYS et D. DEJONGHE, *op. cit.*, p. 126, qui considèrent qu'une communication professionnelle qui n'est pas destinée à être entendue par d'autres personnes que celles concernées par les propos tenus, est une communication privée au sens de la loi; voy. également T. HENRION, *op. cit.*, p. 26 qui soutient que l'on peut aboutir à la même conclusion en ce qui concerne les e-mails.

<sup>25</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Exposé des motifs, *Doc. parl., Sén., sess. ord. 1992-1993*, n° 843-1, p. 6.

<sup>26</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enre-

---

<sup>17</sup> La définition exacte reprise par la Cour est la suivante: « tout énoncé, oral ou non oral, fait directement ou à distance et, notamment, les déclarations et conversations directes ou téléphoniques de même que toutes les formes modernes de la télématique ».

<sup>18</sup> L. ARNOU, *op. cit.*, p. 24.

<sup>19</sup> L. ARNOU, *op. cit.*, p. 25.

<sup>20</sup> H.-D. BOSLY et D. VANDERMEERSCH, *op. cit.*, p. 305; L. ARNOU, *op. cit.*, p. 26; D. VANDERMEERSCH, *Les recherches en matière de téléphonie et de (télé)communications*, *op. cit.*, p. 49.

<sup>21</sup> T. CLAEYS et D. DEJONGHE, *op. cit.*, p. 126; P. DE HERT, « C.A.O. nr. 81 en advies nr. 10/2000 over controle van internet en e-mail », *R.W.*, 2003, p. 1284.

<sup>22</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enre-

telle mesure, le juge d'instruction doit prendre une ordonnance motivée qui, à peine de nullité, doit comporter les mentions prévues à l'article 90<sup>quater</sup>, § 1<sup>er</sup><sup>27</sup>. Le procureur du Roi est cependant également compétent en cas de flagrant délit d'infractions de prise d'otage et d'extorsion à l'aide de violences ou menaces<sup>28</sup>.

**36.** Ensuite, il est requis qu'il existe des indices sérieux que le fait dont le juge d'instruction est saisi constitue une infraction visée par l'une des dispositions énumérées au § 2 de l'article 90<sup>ter</sup> du C.i.cr.<sup>29</sup>. En 1994, la volonté du législateur était de limiter strictement cette mesure à des formes de criminalité graves telles que le terrorisme, le grand banditisme ou la criminalité organisée<sup>30</sup>. C'est pour cette raison que les infractions susceptibles de faire l'objet d'une telle mesure font l'objet d'une énumération exhaustive. Cette condition est

une application du principe de proportionnalité et vise à empêcher l'utilisation d'une telle mesure à des fins de prévention ou dans le cadre d'une enquête proactive. De même, les écoutes exploratoires ne sont pas autorisées<sup>31</sup>. Afin de tenir compte de l'essor des nouvelles technologies sur le plan des (télé)communications et des nouvelles formes de criminalité en lien avec celle-ci, plusieurs lois sont venues compléter cette liste<sup>32</sup>.

**37.** Par ailleurs, la mesure d'interception doit être nécessaire à la manifestation de la vérité et doit rencontrer le principe de subsidiarité. Cela signifie que le juge d'instruction ne pourra recourir à une telle mesure que si les autres moyens d'investigation semblent être insuffisants, sans qu'il soit nécessaire que ces autres moyens aient effectivement été mis en œuvre<sup>33</sup>.

**38.** En outre, la mesure ne peut être ordonnée qu'à l'égard des personnes soupçonnées d'avoir commis une des infractions visées par la loi, de leurs moyens de communication ou de télécommunication ou des lieux présumés fréquentés par ceux-ci. Elle peut l'être également à l'égard des personnes présumées être en communication régulière avec des suspects<sup>34</sup>.

gistrement de communications et de télécommunications privées, Exposé des motifs, *Doc. parl.*, Sén., sess. ord. 1992-1993, n° 843-1, p. 12; D. VANDERMEERSCH, «Le droit pénal et la procédure pénale confrontés à Internet (les apprentis surfeurs)», in *Internet sous le regard du droit* (sous prés. C. DOUTRELEPONT et P. MANDOUX), Bruxelles, Éditions du Jeune Barreau, 1997, p. 256.

<sup>27</sup> À savoir: les indices ainsi que les faits concrets et propres à la cause qui justifient la mesure conformément à l'article 90<sup>ter</sup>; les motifs pour lesquels la mesure est indispensable à la manifestation de la vérité; la personne, le moyen de communication ou de télécommunication ou le lieu soumis à la surveillance; la période pendant laquelle la surveillance peut être pratiquée et qui ne peut excéder un mois à compter de la décision ordonnant la mesure et les nom et qualité de l'officier de police judiciaire commis pour l'exécution de la mesure.

<sup>28</sup> Article 90<sup>ter</sup>, § 5, du C.i.cr. Dans ce cas, la mesure doit être confirmée dans les vingt-quatre heures par le juge d'instruction.

<sup>29</sup> D. VANDERMEERSCH, «Le droit pénal et la procédure pénale confrontés à Internet (les apprentis surfeurs)», *op. cit.*, p. 257.

<sup>30</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Exposé des motifs, *Doc. parl.*, Sén., sess. ord. 1992-1993, n° 843-1, p. 12.

<sup>31</sup> T. HENRIEN, *op. cit.*, p. 36.

<sup>32</sup> Notamment la loi du 10 juin 1998 modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, *M.B.*, 22 septembre 1998, p. 3059 et la loi du 20 novembre 2000 relative à la criminalité informatique, *M.B.*, 3 février 2001, p. 2909.

<sup>33</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Exposé des motifs, *Doc. parl.*, Sén., sess. ord. 1992-1993, n° 843-1, p. 14; C. DE VALKENEER, *Manuel de l'enquête pénale*, Bruxelles, Larcier, 2011, p. 370.

<sup>34</sup> Il n'est pas requis que ces dernières personnes soient soupçonnées d'être complices ou coauteurs des faits litigieux mais la présomption suivant laquelle ces personnes sont en contact régulier avec le suspect

**39.** Concernant la durée d'une mesure d'écoute, celle-ci ne peut dépasser un mois mais peut être prolongée de mois en mois jusqu'à atteindre un maximum de six mois<sup>35</sup>.

**40.** Enfin, en vertu de l'article 90*quater*, § 2, l'opérateur d'un réseau de communication est tenu de prêter son concours technique à l'exécution de la mesure<sup>36</sup>.

**41.** Signalons encore que le ministre de la Justice est tenu, conformément à l'article 90*decies* du C.i.cr., de présenter annuellement un rapport au Parlement sur l'application des mesures d'écoute et reprenant le nombre d'instructions ayant nécessité une telle mesure, la durée de cette mesure, le nombre de personnes impliquées et le résultat final de l'enquête<sup>37</sup>.

## B. L'application des articles 90*ter* et suivants du C.i.cr. aux e-mails

**42.** Si l'on sait désormais que les articles 90*ter* et suivants du C.i.cr. ont vocation, en théorie, à s'appliquer aux courriers électroniques, encore faut-il déterminer dans quelle mesure ces dispositions rédigées dans une ère pré-Internet et qui visaient à l'origine essentiellement les écoutes téléphoniques vont, en

pratique, pouvoir s'appliquer à ce type de communications.

**43.** Une des conditions énoncées pour que le juge d'instruction ordonne valablement l'interception de télécommunications est que cette interception ait lieu au cours du processus de transmission de la conversation ou du message. La période de transmission paraît simple à définir lorsque la communication entre les personnes emprunte une forme classique telle une conversation téléphonique. Une autre chose est de l'interpréter lorsque la (télé) communication prend une forme moderne tel un message vocal, un SMS, un courrier électronique ou autre<sup>38</sup>.

**44.** S'agissant de l'e-mail, cette difficulté d'interprétation apparaît encore plus clairement dès l'instant où l'on décompose le trajet parcouru par celui-ci sur le réseau Internet depuis son envoi jusqu'à sa réception.

**45.** Avant d'étudier les différentes interprétations auxquelles la notion d'interception « en cours de transmission » donne lieu en pratique s'agissant du courrier électronique, abordons les aspects techniques caractérisant la période de transmission d'un e-mail.

### 1. La description technique de la notion « en cours de transmission »

**46.** Lorsque l'on analyse le parcours effectué par un courrier électronique, l'on constate que celui-ci se décompose en différentes étapes depuis l'émetteur jusqu'au destinataire via un ou plusieurs intermédiaires. Examinons ce parcours ainsi que les alternatives dont disposent l'émetteur et le destinataire du message électronique.

---

doit reposer sur des faits précis. Notez également qu'un régime plus restrictif est prévu pour les (télé) communications couvertes par le secret professionnel aux articles 90*sexies*, alinéa 3 et 90*octies* du C.i.cr.; D. VANDERMEERSCH, «Le droit pénal et la procédure pénale confrontés à Internet (les apprentis surfeurs)», *op. cit.*, p. 257; H.-D. BOSLY et D. VANDERMEERSCH, *op. cit.*, p. 314; Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Exposé des motifs, *Doc. parl.*, Sén., sess. ord. 1992-1993, n° 843-1, p. 15.

<sup>35</sup> Article 90*quater*, § 1<sup>er</sup>, 4<sup>e</sup> et article 90*quinquies* du C.i.cr.

<sup>36</sup> D. VANDERMEERSCH, «Le droit pénal et la procédure pénale confrontés à Internet (les apprentis surfeurs)», *op. cit.*, p. 258.

<sup>37</sup> A. SADZOT, *op. cit.*, p. 253.

<sup>38</sup> C. DE VALKENEER, «Les infractions en matière d'écoutes, de prise de connaissance et d'enregistrement de communications et de télécommunications», *op. cit.*, p. 399.

**47.** Lors de l'envoi d'un e-mail, l'émetteur a, en réalité, deux possibilités. La première possibilité consiste à utiliser un client de messagerie, c'est-à-dire un logiciel installé et configuré sur son ordinateur personnel (par exemple Microsoft Outlook, Mozilla Thunderbird,...). Ce client de messagerie, appelé aussi *Mail User Agent* (MUA), transfère alors l'e-mail à un serveur mail (dans bien des cas, il s'agira du serveur mail du fournisseur d'accès à Internet) via le protocole SMTP.

La seconde possibilité repose sur l'utilisation d'un service de messagerie *webmail*, c'est-à-dire que l'émetteur se connecte, depuis son navigateur, à une application web. Depuis cette application web, une requête contenant l'e-mail est envoyée à un serveur web via le protocole HTTP. Ce serveur web va alors entrer en contact avec un serveur mail pour poursuivre l'expédition de l'e-mail.

**48.** Après la phase d'envoi, l'e-mail pénètre ensuite dans le nuage Internet où il est découpé en séquences acheminées de routeurs en routeurs, les *Mail Transfer Agents* (MTA). Au cours de ce voyage, qui ne dure que quelques secondes, l'e-mail est en grande partie intraversable. Finalement, l'e-mail parvient à la boîte finale où il est reconstitué en un message complet, il s'agit du *Mail Delivery Agent* (MDA).

**49.** Pour réceptionner un e-mail, le destinataire du message a également deux options. La première revient à utiliser un client de messagerie (MUA) afin de récupérer les courriers électroniques sur son ordinateur depuis le serveur mail. La réception peut alors se faire via deux protocoles: soit le protocole POP3 grâce auquel les e-mails sont téléchargés sur l'ordinateur personnel du destinataire et sont effacés du serveur mail, soit le protocole IMAP où les e-mails restent stockés sur le serveur mail (ce qui permet de les consulter depuis différents clients de messagerie voire via un service de messagerie *webmail*).

La seconde option dont dispose le destinataire pour prendre connaissance de ses e-mails est d'utiliser un service de messagerie *webmail* par le biais de son navigateur. Une fois connecté à la page web du service, une requête sera envoyée au serveur web qui lui-même entrera en contact avec le serveur mail sur lequel est stocké l'e-mail. La réponse du serveur web, à savoir le résultat visible par le destinataire, prendra alors la forme d'une page HTML contenant le message.

## **2. La portée de la notion « en cours de transmission »**

**50.** Vu la complexité du parcours d'un e-mail, il est parfois très difficile, tant sur le plan technique que juridique, d'affirmer avec exactitude l'endroit où commence et, surtout, où s'achève sa transmission. La question, loin d'être anodine, mérite d'être examinée avec attention puisqu'elle permet de savoir jusqu'à quel moment un e-mail peut être intercepté par les autorités judiciaires sur base de l'article 90ter du C.i.cr.

### *a. Les contours de la notion « en cours de transmission »*

**51.** Selon les travaux préparatoires de la loi du 30 juin 1994, l'interception d'une communication ou d'une télécommunication sera considérée comme légale, et donc comme intervenant « en cours de transmission », si elle se réalise « sur le trajet entre l'émetteur et le récepteur »<sup>39</sup>.

**52.** Sont donc exclues du champ d'application de la loi, les situations dans lesquelles aucune communication n'a encore été effectuée malgré le fait qu'un message soit apprêté

<sup>39</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Exposé des motifs, *Doc. parl., Sén., sess. ord. 1992-1993, n° 843-1, p. 6.*

pour l'envoi. Il en va ainsi des e-mails en cours de rédaction ou qui sont enregistrés dans les « brouillons »<sup>40</sup>.

**53.** Est également exclue du champ d'application de la loi, la prise de connaissance du résultat concret d'une transmission de données. Cela comprend notamment le texte imprimé d'un message télécopié, des données (telles que des images ou des e-mails) reçues et mises en mémoire dans l'ordinateur du destinataire, des paroles enregistrées sur un répondeur téléphonique ou sur un dictaphone, ou encore des SMS arrivés et stockés dans la mémoire d'un GSM<sup>41</sup>. Dans toutes ces hypothèses, les données se trouvent en effet dans une situation statique de sorte que la prise de connaissance de celles-ci pourra s'effectuer par une saisie dans le cadre d'une perquisition ou dans le cadre d'une recherche informatique basée sur l'article 88ter du C.i.cr.<sup>42</sup>

La Cour de cassation a validé cette interprétation dans un arrêt du 31 mars 2010<sup>43</sup>. Dans cette affaire, le requérant invoquait la violation des articles 90ter à 90decies du C.i.cr. par des enquêteurs qui, sans ordonnance motivée,

avaient écouté les messages contenus dans la boîte vocale de son GSM. La Cour a confirmé que les dispositions invoquées ne trouvaient à s'appliquer qu'aux écoutes, prises de connaissance et enregistrements de communications et télécommunications privées pendant leur transmission. Par conséquent, la prise de connaissance d'un message vocal après que celui-ci soit arrivé à destination ne rentrait pas, selon elle, dans le champ d'application de ces articles<sup>44</sup>.

*b. Les interprétations restrictive et extensive de la notion « en cours de transmission »*

**54.** Si, toujours selon les travaux préparatoires de la loi du 30 juin 1994, le message « electronic-mail » mis en mémoire chez le destinataire entérine la fin de la phase de transmission des données, plusieurs interprétations ont cependant vu le jour en doctrine quant à la manière d'interpréter cette expression.

**55.** Une partie de la doctrine a adopté une interprétation que l'on peut qualifier de *restrictive* dans la mesure où elle soutient que lorsque les e-mails sont stockés dans la boîte aux lettres sur le serveur mail du fournisseur d'accès à Internet, ces e-mails ne doivent pas être perçus comme « en cours de transmission ». Cela implique d'une part, qu'ils ne bénéficient pas de la protection générale du secret des (télé)communications et, d'autre part, qu'ils ne peuvent être interceptés sur base

<sup>40</sup> J. DE WILDE D'ESTMAEL, « Surveillance des courriels et de l'internet », in *Discipline et surveillance dans la relation de travail*, Limal, Anthemis, 2013, p. 361; L. ARNOU, *op. cit.*, p. 30.

<sup>41</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Exposé des motifs, *Doc. parl.*, Sén., sess. ord. 1992-1993, n° 843-1, p. 6; H.-D. BOSLY et D. VANDERMEERSCH, *op. cit.*, p. 306; A. SADZOT, *op. cit.*, p. 240.

<sup>42</sup> D. VANDERMEERSCH, *Les recherches en matière de téléphonie et de (télé)communications*, *op. cit.*, p. 53; L. ARNOU, *op. cit.*, p. 30; D. VANDERMEERSCH, « Les modifications en matière de repérage et d'écoute de (télé)communications introduites par la loi du 10 juin 1998 », *Rev. dr. pén.*, 1998, p. 1066; D. VANDERMEERSCH, « Le droit pénal et la procédure pénale confrontés à Internet (les apprentis surfeurs) », *op. cit.*, pp. 252-253; T. FREYNE, *op. cit.*, p. 170.

<sup>43</sup> Cass., 31 mars 2010, disponible sur <http://jure.juridat.just.fgov.be>.

<sup>44</sup> Dans le même ordre d'idées, voy. la Recommandation d'initiative n° 8/2012 du 2 mai 2012 de la Commission de la Protection de la vie Privée relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail, p. 12, disponible sur [www.privacycommission.be](http://www.privacycommission.be). Dans cette Recommandation, la Commission estime que le fait pour un employeur de consulter des données relatives à des e-mails stockés sur le disque dur du travailleur doit être considéré comme intervenant après la transmission de ces données.

d'une ordonnance fondée sur l'article 90ter du C.i.cr.<sup>45</sup>

**56.** Une autre partie de la doctrine considère que le législateur de 1994 envisageait d'abord une interprétation *extensive* de la notion « en cours de transmission ». La transmission s'entend alors comme couvrant l'entièreté du trajet entre émetteur et récepteur et ne s'achevant qu'une fois l'e-mail sauvegardé sur l'ordinateur personnel du destinataire après que ce dernier ait activé sa boîte de réception<sup>46</sup>.

**57.** À l'examen des travaux préparatoires de la loi du 10 juin 1998<sup>47</sup>, il apparaît que cette dernière thèse ait été défendue – à tout le moins dans un premier temps – par le ministre de la Justice faisant fonction. Pour confirmer

le raisonnement selon lequel les autorités judiciaires sont habilitées à intercepter un e-mail lorsqu'il se trouve sur le serveur mail, le ministre invoque deux arguments *a contrario* qui peuvent être synthétisés comme suit :

Tout d'abord, le fait de considérer qu'un e-mail se trouvant sur le serveur mail du fournisseur d'accès à Internet n'est plus « en cours de transmission » signifierait que les articles 314bis et 259bis du Code pénal ne s'appliqueraient pas non plus et que la prise de connaissance illégale de cet e-mail ne serait pas pénalement punissable. En effet, l'écoute constitue une exception au principe de protection des (télé)communications. D'où, lorsqu'une communication doit être protégée, elle doit aussi pouvoir faire l'objet d'une mesure d'écoute si les nécessités de l'instruction le requièrent.

Ensuite, les travaux préparatoires de la loi de 1994 stipulent que la protection ne joue que jusqu'à ce que le message « electronic mail » soit mis en mémoire chez le destinataire. Il faut en déduire que toute la phase préalable, y compris celle où l'e-mail est stocké sur le serveur mail, fait partie du processus de transmission<sup>48</sup>.

**58.** Selon certains auteurs, cette solution extensive est conforme à l'esprit de la loi et peut également être déduite de l'explication donnée au mot « télécommunications » lors des discussions relatives au projet de loi de 1994<sup>49</sup>. À l'époque, le représentant du ministre avait déclaré que ce terme visait les communications réalisées à distance, « avec un décalage qui peut d'ailleurs aussi se situer dans le temps,

<sup>45</sup> En ce sens, voy. D. VANDERMEERSCH, « Le droit pénal et la procédure pénale confrontés à Internet (les apprentis surfeurs) », *op. cit.*, pp. 252-253 et D. VANDERMEERSCH, *Les recherches en matière de téléphonie et de (télé)communications*, *op. cit.*, pp. 53-54. L'auteur assimile le fournisseur d'accès à Internet à un mandataire du destinataire qui réceptionnerait et stockerait le message sur son disque dur pour le mettre à disposition du destinataire. Selon lui, la prise de connaissance de courriers électroniques stockés sur le serveur mail du fournisseur d'accès pourrait alors avoir lieu sur base d'une mesure prise en vertu de l'article 88ter du C.i.cr. ou à l'occasion d'une perquisition. Voy. également L. ARNOU, *op. cit.*, pp. 32-36 qui affirme qu'une nouvelle phase de transmission s'ouvre au moment où le destinataire utilise son client de messagerie pour rapatrier ses e-mails et qu'une écoute peut dès lors uniquement être réalisée pendant les étapes séparées qui caractérisent la phase de transmission.

<sup>46</sup> L. CEULEMANS, *op. cit.*, p. 230.

<sup>47</sup> Projet de loi modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées; proposition de loi complétant l'article 90ter du Code d'instruction criminelle; proposition de loi complétant l'article 90ter du Code d'instruction criminelle en vue de permettre l'application de mesures de surveillance à l'égard de personnes soupçonnées d'avoir commis des infractions à la législation sur les hormones, Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Ch. repr., sess. ord. 1996-1997, n° 1075/9, pp. 15-16.

<sup>48</sup> L. ARNOU, *op. cit.*, pp. 33-34. Selon cet auteur, aucun de ces deux arguments ne semble convaincant.

<sup>49</sup> P. VAN LINTHOUT et J. KERKHOF, « Internetrecherche: informatiecatap en netwerkzoekling, licht aan het eind van de tunnel », *T. Strafr.*, 2008/2, p. 85; P. DE HERT, « C.A.O. nr. 81 en advies nr. 10/2000 over controle van internet en e-mail », *op. cit.*, p. 1284.

puisqu'on peut imaginer que l'information soit d'abord stockée avant d'être transmise»<sup>50</sup>.

**59.** Poussant le raisonnement encore plus loin, d'autres sont d'avis que la transmission ne s'achève que lorsque le destinataire prend effectivement et entièrement connaissance du message. Il en résulte que la prise de connaissance d'une copie d'un message stockée sur un serveur durant sa transmission est à assimiler à une prise de connaissance au cours de cette transmission<sup>51</sup>.

**60.** Il se dégage donc de ces deux tendances le constat selon lequel la notion de transmission est loin de faire l'unanimité en doctrine.

**61.** Il semble d'ailleurs que lors des discussions préparatoires à la loi du 10 juin 1998 déjà évoquées, le ministre de la Justice lui-même, ainsi que son représentant, se soient emmêlés les pinceaux au point de se contredire. Ainsi, quelques mois après avoir défendu une interprétation extensive, le ministre paraît ensuite préconiser la première interprétation plus restrictive en affirmant que, sur le plan technique, il y a lieu de distinguer la phase de transmission du message et la phase durant laquelle ce message est stocké sur le serveur mail. Il ajoute que si l'on se trouve dans la phase de transmission, il peut être fait appel aux articles 90ter et suivants du C.i.c.r. pour intercepter l'e-mail. Au contraire, dès que le message est stocké sur le serveur mail, les données se trouvent dans une situation statique et ni le secret des télécommunica-

tions, ni les mesures d'écoute ne trouvent à s'appliquer<sup>52</sup>.

Et au représentant du ministre de la Justice, à son tour, de prétendre que dans « la logique du législateur de 1994, le secret des télécommunications s'étend aux deux phases de transmission, mais non à la phase au cours de laquelle les données sont mises en mémoire sur le serveur du fournisseur de services »<sup>53</sup>.

*c. Les limites des interprétations restrictives et extensives de la notion « en cours de transmission »*

**62.** D'après les auteurs P. Van Linthout et J. Kerkhofs, la faiblesse qui caractérise ces modèles restrictif et extensif est qu'ils ne tiennent pas compte des réalités d'Internet, et notamment du type de client-mail utilisé, ni du comportement du destinataire (pratique-t-il un usage normal ou abusif du service mail, à quel moment prend-il réellement connaissance du courrier électronique ?)<sup>54</sup>.

Ainsi, ces auteurs considèrent que l'interprétation extensive de la notion de transmission omettrait d'envisager la possibilité qu'a le destinataire du message d'en prendre connaissance au moment où l'e-mail se trouve encore sur le

<sup>50</sup> Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Sén., sess. ord. 1992-1993, n° 843-2, p. 38.

<sup>51</sup> O. RIJCKAERT et N. LAMBERT, *Le respect de la vie privée dans la relation de travail*, coll. Études pratiques de droit social, Bruxelles, Kluwer, 2012, p. 131.

<sup>52</sup> Projet de loi modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Sén., sess. ord. 1997-1998, n° 828/3, p. 15.

<sup>53</sup> Projet de loi modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, Rapport fait au nom de la Commission de la Justice *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1075/17, p. 10; C. DE VALKENBERG, « Les infractions en matière d'écoutes, de prise de connaissance et d'enregistrement de communications et de télécommunications », *op. cit.*, p. 400.

<sup>54</sup> P. VAN LINTHOUT et J. KERKHOFS, « Internetrecherche: informatie op een netwerkzoektocht, licht aan het eind van de tunnel », *op. cit.*, p. 86.

serveur mail du fournisseur d'accès Internet et n'a pas encore été rapatrié sur l'ordinateur du destinataire<sup>55</sup>.

De même, l'interprétation restrictive ainsi que l'interprétation selon laquelle le fournisseur d'accès Internet agirait en tant que mandataire du destinataire sembleraient faire l'impasse sur le fait que, si le destinataire ne prend pas connaissance du message au moment où il se trouve sur le serveur mail, la communication ne peut concrètement s'achever que lorsque le message arrive sur l'ordinateur du destinataire<sup>56</sup>.

**63.** Eu égard à ces développements, il nous paraît indispensable, pour saisir la portée de la notion de transmission au sens de l'article 90ter du C.i.cr., de mieux distinguer les différentes possibilités d'utilisation des applications et services de messagerie électronique.

### **3. Le critère du «geïndiceerd noodzakelijk eindstation» pour interpréter la notion «en cours de transmission»**

**64.** À la certitude de savoir que la période de transmission a pour point de départ l'ordre de l'émetteur d'envoyer le message s'oppose la délicate question de savoir où s'achève cette période de transmission. Comme remède au reproche formulé à l'encontre des interprétations restrictive et extensive, les auteurs précités P. Van Linthout et J. Kerkhofs proposent, pour identifier le point final de la communication, d'utiliser le critère du «geïndiceerd noodzakelijk eindstation»<sup>57</sup>. Il s'agit de l'endroit où l'on peut considérer qu'un e-mail a,

en principe, atteint sa destination finale. Nous allons voir que celui-ci dépend du type de client mail choisi par le destinataire, à savoir un client de messagerie configuré en POP ou une messagerie web.

#### *a. L'utilisation d'un client de messagerie configuré en POP*<sup>58</sup>

**65.** Le principe d'un client de messagerie utilisé avec le protocole POP est de permettre au destinataire de récupérer sur son poste de travail les e-mails acheminés vers et stockés sur un serveur mail, en général celui du fournisseur d'accès Internet. Il y a donc une transmission de données, depuis l'expéditeur jusqu'à la boîte de réception installée sur l'ordinateur du destinataire de la communication en passant par une «boîte aux lettres» du fournisseur d'accès Internet où les données seront stockées le temps que le destinataire active son client de messagerie (Microsoft Outlook, Mozilla Thunderbird,...).

**66.** Dans une telle situation, de quelle manière le juge d'instruction va-t-il pouvoir intercepter un e-mail «en cours de transmission»? *A priori*, il devrait considérer que la transmission ne se termine qu'une fois le «geïndiceerd noodzakelijk eindstation» atteint, à savoir lorsque l'e-mail est arrivé sur l'ordinateur personnel du destinataire où est installée sa boîte de réception et que le destinataire peut effectivement en prendre connaissance.

Dès lors qu'en pratique le juge d'instruction va techniquement procéder à l'interception de l'e-mail chez le fournisseur d'accès Internet, il devra donc se soumettre aux exigences des articles 90ter et suivants du C.i.cr. pour en

<sup>55</sup> P. VAN LINTHOUT et J. KERKHOFS, «Cybercriminaliteit doorgeïndiceerd», *T. Strafr.*, 2010/4, pp. 194-195.

<sup>56</sup> P. VAN LINTHOUT et J. KERKHOFS, «Internetrecherche: informatiecatap en netwerkzoekling, licht aan het eind van de tunnel», *op. cit.*, p. 86.

<sup>57</sup> P. VAN LINTHOUT et J. KERKHOFS, «Internetrecherche: informatiecatap en netwerkzoekling, licht aan het eind van de tunnel», *op. cit.*, p. 87.

<sup>58</sup> Notons que le protocole IMAP devient de plus en plus courant face au protocole POP3 (version actuelle). Contrairement à ce dernier, il consiste à laisser les messages sur le serveur mail et permet ainsi de les consulter via différents clients de messagerie ou *webmail*.

prendre connaissance puisque l'e-mail sera encore réputé être « en cours de transmission ».

**67.** Une hypothèse souvent oubliée par la doctrine risque pourtant de mettre à mal cette solution. Il s'agit du cas où le destinataire, plutôt que d'utiliser son client de messagerie pour rapatrier et lire ses e-mails, utilise une application webmail mise à disposition par son fournisseur d'accès Internet pour en prendre connaissance alors qu'ils se trouvent encore sur le serveur mail. Cela peut, par exemple, être le cas lorsque le destinataire est en déplacement et qu'il n'activera sa boîte de réception sur son ordinateur personnel qu'une fois de retour chez lui<sup>59</sup>.

Dans un tel cas de figure, le destinataire mettrait donc fin à la période de transmission dès l'instant où il prendrait connaissance de ses e-mails en se connectant à l'application *webmail* dont il dispose. Or, une telle situation étant, *a priori*, purement spéculative, le critère du « *geïndiceerd noodzakelijk eindstation* » ne doit pas, selon P. Van Linthout et J. Kerkhofs, être remis en cause. En effet, le terme « *geïndiceerd* » se réfère à ce que l'on peut, *a priori*, raisonnablement identifier comme étant le point de destination final de l'e-mail à savoir, en principe, l'ordinateur personnel du destinataire. Il demeure donc, à première vue, légitime et justifié pour le juge d'instruction d'avoir recours à l'article 90ter du C.i.cr.

**68.** Que se passerait-il cependant si, dans le cadre d'une instruction, un suspect dont les courriers électroniques auraient été interceptés sur base d'une ordonnance fondée sur l'article 90ter du C.i.cr., parvient à prouver qu'il avait déjà pris connaissance de ses e-mails avant leur interception et que, par conséquent, la transmission avait pris fin ?

Bien que la preuve d'une telle allégation ne soit pas toujours évidente à fournir, il se pourrait que le suspect apporte des éléments crédibles établissant qu'un e-mail avait déjà été lu lors de son interception par les autorités judiciaires (par exemple, le suspect pourrait avoir imprimé le texte de l'e-mail lors de sa consultation sur l'application *webmail*)<sup>60</sup>. Dans ce cas, le suspect parviendrait à démontrer que l'ordonnance du juge d'instruction n'était pas valable étant donné qu'elle aurait dû être fondée sur l'article 88ter du C.i.cr. et non pas sur l'article 90ter du C.i.cr.

**69.** Il faut déduire de cette possibilité qu'il sera, en toute hypothèse, plus prudent de la part du juge d'instruction de prendre une ordonnance basée sur l'article 90ter *juncto* 88ter afin d'écarter tout risque de voir son ordonnance déclarée nulle.

**70.** Afin d'illustrer ces propos, examinons la décision rendue par le tribunal correctionnel de Louvain le 4 décembre 2007<sup>61</sup>. Dans cette affaire, un manager IT avait pris connaissance des e-mails d'un employé haut placé de l'entreprise. Il était accusé de la violation de l'article 109terD, § 1<sup>er</sup>, de la loi Belgacom<sup>62</sup> et de l'article 314bis, § 1<sup>er</sup>, 1<sup>o</sup>, du Code pénal. Pour sa défense, le manager soutenait que l'article 314bis du Code pénal ne pouvait pas s'appliquer étant donné qu'il n'avait pris connaissance des e-mails qu'une fois ceux-ci parvenus

<sup>59</sup> P. VAN LINTHOUT et J. KERKHOFS, « Internetrecherche: informatiecatap en netwerkzoekling, licht aan het eind van de tunnel », *op. cit.*, p. 80.

<sup>60</sup> Une telle éventualité confirme, par ailleurs, le constat selon lequel la correspondance au sens classique du terme et les e-mails ne peuvent faire l'objet d'une assimilation en droit pénal. Il est en effet impossible pour le destinataire d'une lettre d'en prendre connaissance avant qu'elle ne soit déposée dans sa boîte aux lettres, sa destination finale, tandis qu'il est possible pour le destinataire d'un e-mail d'en prendre connaissance via une application *webmail* avant que le courrier électronique ne soit arrivé dans sa boîte de réception.

<sup>61</sup> Corr. Louvain, 4 décembre 2007, *T. Strafr.*, 2008/3, p. 223.

<sup>62</sup> Les faits étant antérieurs à l'entrée en vigueur de l'article 124 de la loi du 13 juin 2005.

sur le serveur de l'entreprise, ce qui selon lui, ne rentrait pas dans la phase de transmission<sup>63</sup>.

Le tribunal s'il n'a pas partagé ce raisonnement, n'a toutefois pas clairement établi ce qu'il fallait entendre par la notion « en cours de transmission ».

En effet, dans son analyse, le tribunal déclare dans un premier temps, que le fait que les e-mails se trouvent déjà sur le serveur de l'entreprise, « n'emporte pas le fait que ceux-ci n'aient pas encore été demandés et lus par la personne concernée ». Le tribunal en conclut que ces e-mails, non encore consultés, peuvent être considérés comme étant en cours de transmission<sup>64</sup>.

Or, dans un second temps, le tribunal ajoute qu'un « e-mail envoyé n'est reçu par le destinataire que lorsque ce dernier active sa boîte mail et peut ouvrir et lire son courrier ».

Concluant à la violation des dispositions invoquées, le tribunal condamne donc une interprétation restrictive de la notion de transmission où seule la phase de l'envoi serait visée ce qui rendrait la protection accordée par l'article 314bis du Code pénal peu utile. De plus, la phase de l'envoi ne durant que quelques secondes, toute interception de message en cours de transmission serait rendue techniquement impossible.

**71.** Plusieurs auteurs ont tenté d'interpréter cette décision afin d'identifier le critère pertinent pour délimiter la période de transmission. Certains se sont ainsi ralliés à la position du tribunal selon laquelle la transmission ne s'achève pas lorsque l'e-mail se trouve sur le serveur mail du fournisseur d'accès Internet mais bien au moment où il est rapatrié dans la

boîte à message du destinataire, prêt à être lu par celui-ci<sup>65</sup>. Ces auteurs ne partagent toutefois pas la suite du raisonnement soutenu par le tribunal qui est de dire que la transmission continue même lorsque l'e-mail, bien que télé-chargé, n'a pas été effectivement ouvert et lu par le destinataire<sup>66</sup>.

**72.** En conséquence, faut-il considérer que les e-mails doivent seulement être demandés par le destinataire ou que celui-ci doit également les avoir lu? Et que penser de ce qu'affirme le tribunal dans un second temps, à savoir que la réception s'effectue une fois que le destinataire active sa boîte de réception et a la *possibilité*<sup>67</sup> d'ouvrir et de lire son courrier électronique? Il s'agit là d'un nouveau critère, distinct des précédents, avancé par le tribunal et qui ne fait qu'ajouter de l'incertitude à l'interprétation de la décision.

**73.** Selon une partie de la doctrine, c'est bien le critère de la « demande d'e-mails » par l'activation de la boîte de réception qu'il faut retenir. C'est à ce moment que les e-mails sont transférés sur l'ordinateur personnel du destinataire

<sup>65</sup> En faveur de cette interprétation, voy. F. DE VILLENFAGNE, « Criminalité informatique », in *Chronique de jurisprudence en droit des technologies de l'information (2002-2008) (2<sup>e</sup> partie)*, R.D.T.I., n° 39, p. 22.

<sup>66</sup> *Ibid.*; C. DE VALKENEER, « Les infractions en matière d'écoutes, de prise de connaissance et d'enregistrement de communications et de télécommunications », *op. cit.*, p. 399, pour qui ce critère de l'ouverture paraît être une interprétation qui donne une protection trop étendue à ce mode de télécommunication. Selon lui, une fois l'e-mail reçu par le destinataire et stocké sur son ordinateur ou sur le serveur du gestionnaire de courrier électronique, la protection prend fin et ce même si l'ouverture et la prise de connaissance n'ont pas encore eu lieu. L'auteur ajoute que la prise de connaissance de ce message pourra alors tomber sous le coup d'autres dispositions pénales telles que la pénétration irrégulière dans un système informatique (article 550bis du Code pénal).

<sup>67</sup> Nous soulignons.

<sup>63</sup> L. CEULEMANS, *op. cit.*, p. 230.

<sup>64</sup> Dans son argumentation, le tribunal fait référence à P. DE HERT et à la décision du T.G.I. de Paris (17<sup>e</sup> ch.) du 2 novembre 2000.

et que la phase de transmission et la protection de l'article 314bis du Code pénal prennent fin<sup>68</sup>.

**74.** En évoquant d'autres critères tels que la lecture effective du courrier électronique ou la possibilité de l'ouvrir et de le lire, le tribunal a semé la confusion dans les esprits et n'a pas tout à fait mis fin aux difficultés d'interprétation de la notion « en cours de transmission » des articles 314bis du Code pénal et 90ter du C.i.cr. En effet, nous avons vu précédemment qu'un e-mail qui n'aurait pas encore été téléchargé sur la boîte de réception du destinataire peut cependant déjà avoir été lu par celui-ci sur le serveur du fournisseur d'accès Internet via une application *webmail*.

*b. L'utilisation d'une messagerie web ou « webmail »*

**75.** L'utilisation d'une application *webmail* consiste, pour l'utilisateur, à accéder via son navigateur aux e-mails acheminés par le serveur web du fournisseur de messagerie. La transmission s'effectue donc de l'expéditeur vers une « boîte aux lettres » qui n'est pas située sur l'ordinateur du destinataire. Le *geïndiceerd noodzakelijk eindstation* est alors atteint, selon P. Van Linthout et J. Kerkhofs, lorsque le destinataire du message se connecte à sa boîte de réception en ligne mise à disposition par le fournisseur de messagerie<sup>69</sup>.

**76.** Dans cette hypothèse, si le juge d'instruction souhaite intercepter les e-mails sur le compte *webmail* d'un suspect, il ne pourra pas recourir à une ordonnance fondée sur

l'article 90ter du C.i.cr. étant donné que les messages ne sont plus « en cours de transmission » mais bien arrivés à destination. Dès lors, il faudra pratiquer une mesure de recherche dans un système informatique au moyen d'une ordonnance basée sur l'article 88ter du C.i.cr.

**77.** Cependant, le juge d'instruction pourrait être confronté à un autre type d'utilisation du compte *webmail*. Une pratique de plus en plus observée dans le milieu criminel consiste en effet à utiliser un compte *webmail* sous la forme de « valves » ou encore d'un forum afin d'éviter toute possibilité d'interception des messages par les autorités judiciaires. Concrètement, cette forme abusive de communication consiste à créer des e-mails et à les enregistrer dans l'application *webmail* (par exemple dans le dossier brouillon) mais à ne jamais les envoyer. Pour diffuser l'information contenue par le message, l'auteur de l'e-mail communiquera aux destinataires l'adresse de messagerie et le mot de passe du compte<sup>70</sup>.

Selon ce *modus operandi*, la phase de transmission ne paraît jamais débuter étant donné qu'à aucun moment l'émetteur ne donne l'ordre d'envoyer le message. P. Van Linthout et J. Kerkhofs suggèrent, au contraire, de considérer les e-mails comme étant en phase de transmission permanente. Selon eux, puisque la certitude ne peut jamais être acquise de ce que tous les destinataires du message en aient effectivement pris connaissance, la transmission ne s'achève pas. Dès lors, en vue de l'interception de ces e-mails, le juge d'instruction devra produire une ordonnance fondée sur l'article 90ter du C.i.cr.

**78.** Plus complexe encore est la situation où le compte *webmail* en question est soumis à un double usage, à la fois normal et à la fois abusif. Dans ce cas, le juge d'instruction devra,

<sup>68</sup> En ce sens, voy. L. CEULEMANS, *op. cit.*, p. 231. Voy. également P. DE HERT, « Internetrechten in het bedrijf. Controle op e-mail en Internetgebruik in Belgisch en Europees perspectief », *A&M*, 2001, p. 114 et P. DE HERT, « C.A.O. nr. 81 en advies nr. 10/2000 over controle van internet en e-mail », *op. cit.*, pp. 1284-1285, qui a inspiré le tribunal dans sa décision.

<sup>69</sup> P. VAN LINTHOUT et J. KERKHOFS, « Internetrecherche: informatie op zoek in een netwerk, licht aan het eind van de tunnel », *op. cit.*, p. 80.

<sup>70</sup> Le mot de passe est connu de toutes les personnes et est modifié régulièrement.

à nouveau, combiner les dispositions 88ter et 90ter du C.i.cr. dans le but de pouvoir intercepter l'entièreté des e-mails, quel que soit le mode de propagation de l'information utilisé.

**79.** La difficulté, pour le juge d'instruction, apparaît donc nettement. Celui-ci ne peut, *a priori*, savoir à quelle situation il sera confronté parmi les trois présentées ci-dessus. Alors qu'il devrait normalement recourir à une mesure fondée sur l'article 88ter du C.i.cr., la prudence l'invitera à invoquer également l'article 90ter du C.i.cr. et donc à cumuler deux bases légales afin d'anticiper un éventuel usage abusif du compte *webmail*<sup>71</sup>.

**80.** À titre d'illustration, analysons l'arrêt rendu par la chambre des mises en accusation de Gand le 27 septembre 2007<sup>72</sup>. Dans cette affaire, une mesure d'écoute a été ordonnée par un juge d'instruction vis-à-vis du numéro de GSM d'un suspect. Une conversation est alors interceptée au cours de laquelle le suspect communique à son interlocuteur une adresse *hotmail* ainsi qu'un mot de passe pour que celui-ci aille prendre connaissance d'un e-mail. Sur base de ces informations, le juge d'instruction ordonne alors une recherche sur le réseau qu'il fonde malencontreusement sur l'article 88bis du C.i.cr. au lieu de l'article 88ter du C.i.cr. L'e-mail dont il était question dans la conversation téléphonique est alors intercepté et s'avère contenir une image scannée d'un passeport et de données d'identité.

Dans son arrêt, la chambre des mises en accusation a prononcé la nullité de l'ordonnance du juge d'instruction fondée sur l'article 88bis du C.i.cr. et par laquelle l'image correspondant au scan du passeport incluse dans l'e-mail, avait

pu être ouverte. En effet, la chambre des mises en accusation, découvrant *ex post* l'usage abusif dont faisait l'objet le compte *hotmail* du suspect, a considéré qu'une ordonnance fondée sur l'article 90ter du C.i.cr. était requise pour permettre la prise de connaissance des données, qu'il s'agisse de texte ou d'images, contenues dans l'e-mail en question.

**81.** Cette décision confirme la nécessité, pour le juge d'instruction, d'avoir à l'esprit les différentes utilisations possibles d'un compte *webmail*. S'il ne peut, *a priori*, savoir à laquelle des trois situations exposées ci-avant il sera confronté, il peut par contre se prémunir contre tout risque de nullité de l'ordonnance et d'irrecevabilité des poursuites en prenant une ordonnance fondée sur l'article 88ter *juncto* 90ter du C.i.cr.<sup>73</sup>

#### IV. CONCLUSION

**82.** La loi du 30 juin 1994, lors de son adoption, a constitué un progrès important dans le cadre de la lutte contre la grande criminalité en permettant la mise sur écoute de suspects. Toutefois, les auteurs d'actes criminels ont très rapidement adapté leurs méthodes à l'évolution des technologies et les autorités judiciaires ont dû admettre que la loi était devenue en grande partie inapplicable aux nouveaux moyens de communication<sup>74</sup>. Malgré plusieurs interventions législatives venues modifier ou compléter la loi de 1994 pour adapter les mesures d'enquête et permettre leur application dans l'univers des réseaux numériques, des difficultés d'interprétation subsistent encore<sup>75</sup>.

<sup>71</sup> P. VAN LINTHOUT et J. KERKHOFS, « Internetrecherche: informatiecatap en netwerkzoekling, licht aan het eind van de tunnel », *op. cit.*, pp. 92-94.

<sup>72</sup> Gand (mise acc.), 27 septembre 2007, *T. Straf.*, 2008/2, p. 129.

<sup>73</sup> P. VAN LINTHOUT et J. KERKHOFS, « Internetrecherche: informatiecatap en netwerkzoekling, licht aan het eind van de tunnel », *op. cit.*, pp. 93-94.

<sup>74</sup> T. HENRION, *op. cit.*, pp. 56-57.

<sup>75</sup> E. LABBÉ, *op. cit.*, p. 159.

**83.** Le mécanisme d'interception des e-mails d'un suspect que nous venons d'examiner en est la preuve. Confrontés aux réalités d'Internet, le juge d'instruction n'aura d'autre choix que de «bricoler» et de combiner plusieurs dispositions du Code d'instruction criminelle pour couvrir les différentes possibilités dont dispose(nt) le(s) suspect(s). Une adaptation de la législation aux technologies actuelles est donc nécessaire. Une des solutions proposées par la doctrine serait de prévoir des dispositions analogues à celles existantes en matière d'écoutes téléphoniques, à la différence près qu'elles permettraient au juge d'instruction d'intercepter des données sur Internet à n'importe quel stade de leur transmission<sup>76</sup>.

Dans son dernier rapport annuel, le ministre de la Justice appelle d'ailleurs, au nom des instances de recherche et de poursuites, à une intervention législative visant à permettre l'interception d'informations et de communications sur Internet de manière structurelle, à l'instar de la téléphonie<sup>77</sup>.

**84.** Il faudra également réfléchir à l'opportunité d'allonger plus encore la liste des infractions susceptibles de donner lieu à une mesure

d'écoute ou d'interception des (télé)communications. La volonté initiale du législateur était en effet de ne recourir qu'exceptionnellement à une telle mesure. L'extension de la liste des infractions concernées par cette mesure, si elle a pour but de prendre en compte les nouvelles formes de criminalité, a également pour conséquence de «banaliser» le recours à cette pratique constitutive d'une ingérence dans la vie privée des citoyens<sup>78</sup>. Or, le souhait légitime de lutter plus efficacement contre le terrorisme et la criminalité organisée, dont les formes se multiplient et se diversifient, ne peut pour autant impliquer le risque de rompre l'équilibre nécessaire entre la recherche et la poursuite des criminels et les exigences strictes de l'article 8 de la C.E.D.H.

**85.** Outre l'aspect législatif, une utilisation effective de ces méthodes d'investigation nécessite la mobilisation d'importants moyens techniques et humains. L'engagement de personnel spécialisé et qualifié, ainsi que l'octroi d'un budget suffisant pour se procurer du matériel de pointe sont donc également des prérequis indispensables pour rendre de telles mesures efficaces.

<sup>76</sup> P. VAN LINTHOUT et J. KERKHOFS, «Internetrecherche: informatie op zoek naar de dader», *op. cit.*, p. 94.

<sup>77</sup> Rapport 2013 en application de l'article 90decies du Code d'instruction criminelle (2012), Service de la Politique criminelle, *op. cit.*, p. 46.

<sup>78</sup> T. HENRION, *op. cit.*, p. 57.