

Le secret professionnel de l'avocat à l'épreuve de l'interception et de la captation de données informatiques à distance : un secret en lambeaux ?



Par **Vincent Nioré**
Avocat à la Cour,
Coordinateur des
délégués du bâtonnier de Paris aux
contestations des
perquisitions,
Membre du Conseil
national des barreaux,
Ancien membre du
Conseil de l'ordre,
Ancien secrétaire
de la Conférence

Dire du secret professionnel de l'avocat qu'il est devenu un secret de Polichinelle ou de la comédie est un euphémisme.

Il est traditionnel de souligner que le secret professionnel de l'avocat est général, absolu, illimité... et de l'enseigner de manière incessante, comme une litanie, un catéchisme dogmatique suranné, aux élèves-avocats, élevés dès la maternelle au biberon du *credo* du secret absolu qu'ils découvriront au fil du temps, comme un vieux rafirot prenant l'eau de toutes parts.

Il est en effet usuel de citer l'arrêt rendu par la Cour européenne des droits de l'Homme le 24 juillet 2008¹ qui prohibe la perquisition fiscale de l'article L16B du *Livre des procédures fiscales* pour appréhender en cabinet d'avocat « des documents susceptibles d'établir la fraude présumée » du client de l'avocat – non inquiété *es* qualités – « et de les utiliser à charge contre elle » ou encore la jurisprudence de la Cour de justice de l'Union européenne qui définit le secret professionnel comme une « garantie essentielle de la liberté de l'individu et du bon fonctionnement de la justice »².

Cela dit, l'avocat, qu'il conseille ou qu'il défende, n'est jamais à l'abri d'une inter-

ception sauvage ou judiciaire de ses correspondances téléphoniques, de ses courriels ou d'une captation informatique à distance de ses données informatiques, pourtant prohibée par la loi.

Le cabinet d'avocat est, comme le disait le bâtonnier Jean Lemaire, un « asile sacré », destiné à recueillir la confiance du client faite à l'avocat qu'il s'agit de protéger de manière absolue, illimitée dans le temps.

Cette confiance est couverte par le secret professionnel qui est d'ordre public sauf à imaginer la possibilité pour l'autorité judiciaire, pourtant « gardienne de la liberté individuelle » selon la Constitution, de sonriser en permanence les cabinets d'avocats pour y déceler à tout prix l'indice de telle infraction. Une telle démarche serait digne de la pire des dictatures.

Il est évident que, par nature, la conversation téléphonique entre l'avocat et son client est le prolongement de la conversation qui a lieu au cabinet et inversement.

Est pitoyable l'attitude qui consiste à fustiger n'importe quel propos tenu par un avocat à son client, écouté, sans qu'antérieurement le juge ou les enquêteurs aient pris la précaution d'entreprendre des investi-

¹ CEDH, 24 juill. 2008, n° 18603/03, *André c/ France*, .
² CJCE, 19 févr. 2002, n° C-309/99, *Wouters*,

gations permettant de caractériser contre l'avocat indiscutablement l'existence de différents indices de la commission d'une infraction.

Le secret professionnel est déjà en péril à travers les perquisitions « sauvages » en cabinet d'avocat destinées à rechercher des éléments intéressant le client alors que n'est pas démontrée antérieurement contre l'avocat l'existence d'indices laissant penser qu'il a pu participer à la commission d'une infraction.

La chambre criminelle de la Cour de cassation a rappelé cette condition d'antériorité par un arrêt du 25 juin 2013 (n° 12-88021) par lequel elle a décidé que préalablement à la perquisition, « il existait des indices plausibles de participation de l'avocat à des infractions et que les raisons et l'objet des perquisitions étaient déterminés » dans l'ordonnance de perquisition.

Le secret professionnel est également en péril du fait de certaines écoutes judiciaires du client de l'avocat, que l'on peut assimiler à des écoutes « sauvages » de l'avocat lui-même.

Il ne s'agit pas, contrairement à ce qu'indique, de manière totalement erronée, Madame le garde des Sceaux, « d'assurer l'impunité à un avocat qui éventuellement serait impliqué dans une infraction ».

Il faut distinguer deux hypothèses d'écoutes, celles du client de l'avocat et celles de l'avocat lui-même.

Un avocat ne peut être placé sur écoutes, à charge pour le juge d'instruction d'en informer le bâtonnier³ que pour autant que soient démontrés préalablement contre lui un ou plusieurs indices graves ou concordants de sa participation à la commission d'une infraction.

Le juge d'instruction doit « avoir été à la date où il a prescrit l'interception en possession d'indices de participation de l'avocat à une activité délictueuse »⁴.

La conversation entre un client écouté et son avocat qui n'est pas placé sur écoutes, ne peut être retranscrite que pour autant « que les propos tenus par l'avocat étaient pour partie propres à faire présumer la commission par ce dernier de violations

du secret professionnel et, pour les autres, pouvaient constituer un outrage à magistrat »⁵.

Ainsi, pour pouvoir être retranscrite, la conversation entre le client écouté et son avocat doit faire présumer lors de l'écoute la commission de manière flagrante d'une infraction par l'avocat, ce qui serait le cas dans l'hypothèse d'une évidente violation délibérée du secret professionnel, par exemple à l'occasion d'une garde à vue dont le contenu serait diffusé à un tiers.

En dehors de cette hypothèse de « flagrance » et « d'évidence », la condition du constat de l'antériorité d'indices graves ou concordants est essentielle, faute de quoi la retranscription est illicite et doit être annulée sauf, par réflexe, à diaboliser la parole de l'avocat qui devient *ipso facto* le corps du délit.

Il est indispensable de réformer les textes relatifs aux écoutes téléphoniques (et aux perquisitions) qui ne pourraient être interceptées qu'à la condition que soient préalablement recueillis contre l'avocat des indices graves ou concordants de sa participation à la commission d'une infraction en qualité d'auteur ou de complice, bien sûr avec information préalable du bâtonnier.

De surcroît, le juge d'instruction qui recevrait la retranscription d'une écoute révélant une correspondance entre un avocat et son client écouté, devrait solliciter le bâtonnier, s'il ne décide pas lui-même de renoncer à la transcription de l'écoute, pour qu'il lui fasse part de son opinion sur son exploitation éventuelle.

En cas de désaccord du bâtonnier, la retranscription de l'écoute serait placée sous scellé fermé à charge pour le juge d'instruction de saisir le juge des libertés et de la détention (JLD) qui déciderait si la retrans-

En dehors de cette hypothèse de « flagrance » et « d'évidence », la condition du constat de l'antériorité d'indices graves ou concordants est essentielle, faute de quoi la retranscription est illicite et doit être annulée.

³ C. pr. pén., art. 100-7.

⁴ Crim. 15 janv. 1997, n° 96-83753 ; Crim. 14 nov. 2001, n° 01-85.965.

⁵ Crim., 17 sept. 2008, n° 08-85.229, Bull. crim. n° 191, AJ pénal. 2008. 467, obs. S. Lavric ; RSC 2009. 897, obs. J. Buisson.

⁶ C. pr. pén., art. 56-1.

cription de l'écoute doit ou non être versée au dossier d'instruction.

En effet, en charge d'une mission de protection des droits de la défense et du secret professionnel, le bâtonnier doit pouvoir exprimer un désaccord s'il estime que l'écoute est « irrégulière » comme en matière de perquisition chez l'avocat⁶.

Dans un autre registre, le journal *Le Monde* titrait dans son édition du 8 février 2014, « Le procès des pratiques douteuses d'un ancien gendarme en Corse », et révélait

« les étranges pratiques de certaines unités de gendarmerie corses. Effarés, les magistrats ont ainsi appris à l'audience qu'il était d'usage de vérifier « un tuyau » en formulant une demande d'écoute téléphonique dans le cadre d'une procédure en déshérence. Si le « branchement » se révélait utile, « on laissait tomber la fausse procédure et on entamait une vraie enquête sur la base des informations recueillies par les écoutes », a indiqué le prévenu. Autre méthode, utilisée pour « éclaircir des propos jugés obscurs dans des enquêtes : le recours à des informateurs priés de décrypter des écoutes pourtant couvertes par le secret et tenus ainsi au courant de l'état d'avancement des procédures ».

Le danger qui pèse sur la profession d'avocat est bien celui d'une destruction du secret professionnel, notamment par les perquisitions au domicile et en cabinet d'avocats qui, paradoxalement, présenteront l'avantage de prévoir une garantie spéciale de procédure à peine de nullité, qui consiste dans la présence du bâtonnier ou de son délégué en charge d'une mission légale de contestation aussi systématique qu'impitoyable.

Si les perquisitions en cabinet d'avocats, qu'elles émanent de l'autorité judiciaire ou de l'autorité administrative, doivent être prohibées (au profit d'un nouveau régime prévoyant le filtre du bâtonnier) cepen-

dant, par la garantie spéciale que leur régime prévoit, doivent au final être considérées comme constituant le moyen le plus sûr de tenir en échec toute saisie de la part de certains juges qui d'ailleurs en ont bien pris conscience.

Pour contourner la contestation du bâtonnier, il serait tentant de capter à distance, ce qui ne pourrait être saisi que lors d'une perquisition, susceptible d'être contestée, précisément les courriels de l'avocat, lequel serait de surcroît l'objet d'une réquisition de la part du juge ou des enquêteurs aux fins de communication de documents couverts par le secret professionnel.

Prenons garde contre cette dérive qui consiste à espionner les avocats à leur insu ou à vouloir les séduire en exigeant d'eux la communication spontanée de documents confidentiels contre la promesse exprimée du bout des lèvres d'en rester là ou d'être simplement convoqués en qualité de témoin.

Les perquisitions à distance en cabinet d'avocats sont prohibées.

Aucun avocat ne doit répondre à une réquisition de l'autorité judiciaire sans en avoir préalablement informé et discuté avec son bâtonnier.

LES PERQUISITIONS INFORMATIQUES À DISTANCE

La première difficulté concerne le régime des perquisitions informatiques à distance.

Il est indispensable de légiférer sur la question du transfert des données dans un lieu autre que le cabinet d'avocat et d'inscrire dans la loi que la protection du secret professionnel s'applique dans ce cas.

À titre d'exemple, le législateur a d'ores et déjà par le passé soumis des prestataires informatiques au secret professionnel.

Tel est précisément le cas dans le domaine de la santé : l'article R1111-12 du code de la santé publique contraint le prestataire hébergeur de prendre des dispositions pour assurer la sécurité des données et la garantie des secrets protégés par la loi. Le

⁷ Loi n° 2011-267 du 14 mars 2011.

prestataire est tenu de veiller au respect du secret professionnel.

En l'état, il semble que nous nous heurtions à un vide juridique qui constitue un risque majeur pour tous les cabinets d'avocats qui ont recours à de tels traitements.

L'enjeu est d'autant plus grand que les données du cabinet d'avocat sont susceptibles, chez le prestataire, d'être mutualisées au sein des mêmes moyens techniques que ceux d'une agence immobilière, d'une grande surface...

Aussi, il faut inscrire dans la loi que le secret professionnel d'ordre public s'applique impérativement aux données transférées du cabinet d'avocat quels que soient les moyens et le lieu du traitement, y compris dans l'hypothèse où la convention de prestations de services ne mentionne pas l'obligation au respect du secret professionnel.

La deuxième difficulté concerne l'atteinte aux droits de la défense par « l'interception » et la « captation » de correspondances.

La loi du 14 mars 2011⁷ permet aux officiers et agents de police judiciaire agissant sur commission rogatoire dans le domaine de la criminalité organisée, de mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères :

Article 706-102-1 du code de procédure pénale :

« Lorsque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application de l'article 706-73 l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles

s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction ».

Cependant, la mise en place de ce dispositif technique ne peut concerner les systèmes automatisés de traitement des données se trouvant dans les lieux visés notamment aux articles 56-1 et suivants (cabinet et domicile d'avocat) ni être réalisé dans le véhicule d'un avocat :

Article 706-102-5 du code de procédure pénale :

« En vue de mettre en place le dispositif technique mentionné à l'article 706-102-1, le juge d'instruction peut autoriser l'introduction dans un véhicule ou dans un lieu privé, y compris hors des heures prévues à l'article 59, à l'insu ou sans le consentement du propriétaire ou du possesseur du véhicule ou de l'occupant des lieux ou de toute personne titulaire d'un droit sur celui-ci. S'il s'agit d'un lieu d'habitation et que l'opération doit intervenir hors des heures prévues à l'article 59, cette autorisation est délivrée par le juge des libertés et de la détention saisi à cette fin par le juge d'instruction.

Ces opérations, qui ne peuvent avoir d'autre fin que la mise en place du dispositif technique, sont effectuées sous l'autorité et le contrôle du juge d'instruction. Le présent alinéa est également applicable aux opérations ayant pour objet la désinstallation du dispositif technique ayant été mis en place.

En vue de mettre en place le dispositif technique mentionné à l'article 706-102-1, le juge d'instruction peut également

L'enjeu est d'autant plus grand que les données du cabinet d'avocat sont susceptibles, chez le prestataire, d'être mutualisées au sein des mêmes moyens techniques que ceux d'une agence immobilière, d'une grande surface...

autoriser la transmission par un réseau de communications électroniques de ce dispositif. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction. Le présent alinéa est également applicable aux opérations ayant pour objet la désinstallation du dispositif technique ayant été mis en place.

La mise en place du dispositif technique mentionné à l'article 706-102-1 ne peut concerner les systèmes automatisés de traitement des données se trouvant dans les lieux visés aux articles 56-1, 56-2 et 56-3 ni être réalisée dans le véhicule, le bureau ou le domicile des personnes visées à l'article 100-7 ».

Ainsi, doit être, à notre avis, radicalement prohibée la perquisition à distance de l'ordinateur de l'avocat contenu à son cabinet ou à son domicile.

Ainsi, doit être, à notre avis, radicalement prohibée la perquisition à distance de l'ordinateur de l'avocat contenu à son cabinet ou à son domicile.

Un magistrat instructeur qui entreprendrait d'informer le bâtonnier de ce qu'il envisage d'intercepter les courriels d'un avocat en organisant délibérément une confusion entre l'interception d'une ligne téléphonique et la captation de données informatiques, commettrait

une violation de la loi et s'exposerait au risque d'une annulation de cette mesure intrusive illicite.

En effet, une telle démarche, condamnable à tous égards, reviendrait à contourner le dispositif protecteur de l'article 56-1 du code de procédure pénale.

Les articles 100 et 100-7 du code de procédure pénale prévoient l'interception des correspondances émises par la voie des télécommunications, à savoir les conversations téléphoniques, les télécopies.

Certes, le code des postes et des communications électroniques régit les communications électroniques, donc l'échange de courriels, si bien qu'une analyse rapide des textes pourrait permettre de conclure à l'interception de courriels parce qu'ils

constituent des communications électroniques échangées par la voie des télécommunications.

Insistons sur ce point sur l'arrêt rendu par la chambre criminelle de la Cour de cassation le 22 octobre 2013 (n° 13-81.945) qui retient que « pour rejeter le moyen de nullité pris de l'irrégularité, au regard des dispositions de l'article 34-1, VI, du code des postes et télécommunications électroniques, des réquisitions délivrées aux fins d'obtenir des renseignements relatifs à des adresses électroniques en ce qu'il était demandé également aux détenteurs des données de fournir le contenu des messages envoyés et reçus, l'arrêt retient que, selon les mentions des procès-verbaux, et en l'absence de transcription d'un quelconque message en procédure, ce contenu n'a pas été porté à la connaissance des enquêteurs ; que les juges ajoutent qu'ainsi, il n'a pas été porté atteinte ni à la vie privée, ni au secret des correspondances à l'égard de M. X. Attendu qu'en statuant de la sorte et dès lors que l'irrégularité invoquée n'a pas eu pour effet de porter atteinte aux intérêts de la personne concernée, la chambre de l'instruction a justifié sa décision ».

En effet, le texte de l'article 34-1VI du code des postes et télécommunications électroniques prévoit que « les données permettant de localiser l'équipement terminal de l'utilisateur [...] ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications » et ce dans l'hypothèse de la délivrance d'une réquisition dans le cadre « d'une enquête judiciaire ».

À notre avis, l'interception de courriels reviendrait en fait également à accéder à des données informatiques qui s'affichent sur un écran et devrait être prohibée au visa de l'article 706-102-5 du code de procédure pénale. En effet, le courriel obéit à un régime particulier puisque, par définition, la captation d'un courriel permet d'en capter toute la lignée.

En outre, l'article 706-102-1 du code de procédure pénale évoque « l'utilisateur d'un système de traitement automatisé de données » (STAD). Or, il n'existe aucune définition précise du STAD qui peut s'appliquer indifféremment à toute forme de réseau.

Les textes doivent être clarifiés mais il est certain que la correspondance téléphonique ne peut s'entendre que de la conversation au téléphone et de la communication des télécopies.

Doivent faire exception les courriels et les SMS qui, par définition, constituent des « données informatiques [...] telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères », si bien que leur saisie à distance chez l'avocat doit être prohibée puisque la loi pénale est d'interprétation stricte.

Rappelons pour mémoire les dispositions de l'article 100 du code de procédure pénale :

« En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications. Ces opérations sont effectuées sous son autorité et son contrôle.

La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours ».

Et celles de l'article 100-7 du code de procédure pénale :

« Aucune interception ne peut avoir lieu sur la ligne d'un député ou d'un sénateur sans que le président de l'assemblée à laquelle il appartient en soit informé par le juge d'instruction.

Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un avocat ou de son domicile sans que le bâtonnier en soit informé par le juge d'instruction.

Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un magistrat ou de son domicile sans que le premier président ou le procureur général de la juridiction où il réside en soit informé.

Les formalités prévues par le présent article sont prescrites à peine de nullité ».

L'article 706-102-1 du code de procédure pénale permet aux enquêteurs de mettre en place un dispositif technique pour accéder « en tous lieux ».

Or, le lieu d'un prestataire de traitement de données, notamment en *cloud computing*, qui détiendrait des informations externalisées par le cabinet d'avocats, ne bénéficie d'aucune protection en droit positif au plan du respect du secret professionnel puisque seul le cabinet d'avocat est protégé en tant que tel.

Il est donc nécessaire d'étendre la protection de l'article 56-1 du code de procédure pénale aux lieux d'externalisation du traitement des données.

Nous suggérons également que l'avocat déclare à son Ordre, le recours à des prestataires informatiques pour le traitement des données du cabinet d'avocats, notamment en *cloud computing*.

Enfin, la protection du secret professionnel doit également s'appliquer lorsqu'une perquisition a lieu au plan informatique dans les locaux du client de l'avocat, si bien que doit être inscrit dans la loi que de telles pièces ou données saisies ou bien par un juge ou bien par une autorité administrative, doivent être d'office placées sous scellés fermés jusqu'à ce que la contestation soit tranchée par le juge de la liberté et de la détention.

En sens contraire, la chambre criminelle de la Cour de cassation a validé la saisie chez un tiers non-avocat, de documents couverts par le secret professionnel de l'avocat⁸.

LES RÉQUISITIONS À PERSONNE

Les articles 60-1, 77-1-1 et 99-3 du code de procédure pénale prévoient que le Procureur de la République, le juge d'instruction ou l'OPJ sur autorisation, peuvent par tout moyen requérir de toute personne susceptible de détenir des documents intéressant l'enquête de remettre des documents y compris ceux issus d'un système informatique

Il est certain que la correspondance téléphonique ne peut s'entendre que de la conversation au téléphone et de la communication des télécopies.

⁸ Crim. 17 déc. 2013, n° 13-85717.

sans que puisse leur être opposé sans motif légitime l'obligation au secret professionnel.

Lorsque les réquisitions concernent des avocats mentionnés à l'article 56-1 du code de procédure pénale, la remise des documents ne peut intervenir qu'avec leur accord. Le défaut de réponse à réquisition n'est pas sanctionné pour les avocats de la peine d'amende délictuelle de 3 750 €.

Aucune remise de document couvert par le secret professionnel ne devrait intervenir sur réquisition du Parquet ou injonction d'un juge spontanément par un avocat sans consultation préalable du bâtonnier ou de son délégué qui peut s'opposer à une telle remise en notifiant son opposition au magistrat poursuivant.

Le code de procédure pénale comporte, en effet, des dispositions susceptibles de ruiner la protection de la présence du bâtonnier ou de son délégué lors d'une mesure de saisie.

Soulignons que par arrêt rendu le 17 décembre 2013⁹, la chambre criminelle

de la Cour de cassation a jugé que « l'accord des personnes mentionnées aux articles 56-1 à 56-3 du code de procédure pénale, parmi lesquelles figurent les avocats, n'est requis [...] que pour la remise des documents détenus par cette personne-même ».

La Cour suprême maintient le raisonnement de la chambre de l'instruction selon lequel « il ressort des travaux parlementaires, repris par la circulaire du 14 mai

2004, que les dispositions de l'article 99-3 du code de procédure pénale concernent les personnes mentionnées aux articles 56-1 à 56-3, parmi lesquelles figurent les avocats, lorsque ces personnes sont susceptibles de détenir des documents intéressant l'instruction ; que ce texte donne donc le choix aux avocats, médecins, huissiers, notaires et journalistes d'accepter ou de refuser de répondre à la réquisition, et ce, sans commettre une violation du secret professionnel, ni encourir l'amende prévue au deuxième alinéa de l'article 60-1 du code de procédure pénale ».

En d'autres termes, la chambre criminelle valide la saisie de documents couverts par le secret professionnel chez un tiers, alors que ces mêmes documents demandés à l'avocat, pourraient faire l'objet d'un refus de communication parfaitement licite de sa part.

Ainsi, le secret professionnel de l'avocat ne serait protégé que par le lieu, cabinet ou domicile de l'avocat, et non plus par la nature-même, intrinsèque, des documents saisis.

Par ce raisonnement, la Cour suprême contourne la garantie spéciale de procédure prévue par l'article 56-1 du code de procédure pénale dont la réforme s'impose, effectivement, de manière urgente.

En effet, la tentation du juge est forte de convoquer l'avocat en qualité de témoin pour se faire remettre spontanément des documents couverts par le secret professionnel, plutôt que de perquisitionner et de devoir subir la contestation du bâtonnier. Il arrive aussi que l'avocat soit tout simplement convoqué par l'OPJ, agissant sur commission rogatoire, pour un placement en garde à vue destiné également à obtenir la communication de documents couverts par le secret professionnel.

Vigilance et résistance demeurent de rigueur.¹⁰

Ainsi, le secret professionnel de l'avocat ne serait protégé que par le lieu, cabinet ou domicile de l'avocat, et non plus par la nature-même, intrinsèque, des documents saisis.

⁹ Crim. 17déc. 2013, n° 13-85717.

¹⁰ Ces difficultés sont traitées de manière exhaustive dans un prochain ouvrage de l'auteur avec préface de François Saint-Pierre, à paraître aux éditions Lamy collection Axe Droit « Perquisitions chez l'avocat. Défense des secrets et inviolabilité de l'asile sacré »