Mutations et enjeux de la fraude fiscale face au développement de la cybercriminalité

William Gilles

▶ **To cite this version:**

William Gilles. Mutations et enjeux de la fraude fiscale face au développement de la cybercriminalité. Irène Bouhadana et William Gilles. Cybercriminalité, cybermenaces et cyberfraudes, Les éditions IMODEV, 2012, 979-10-90809. ⟨hal-05066304⟩

HAL Id: hal-05066304

https://hal.science/hal-05066304v1

Submitted on 20 May 2025

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons CC BY-NC-ND 4.0 - Attribution - Non-commercial use - No Derivative Works - International License

Mutations et enjeux de la fraude fiscale face au développement de la cybercriminalité

Le développement d'Internet et des nouvelles technologies de l'information et de la communication contribue à l'émergence d'un nouveau type de criminalité, à savoir la cybercriminalité. Deux types d'infractions doivent être distingués en matière de cybercriminalité. Il convient d'une part, d'identifier les infractions spécifiques aux technologies de l'information et de la communication comme les interceptions de données et les atteintes aux systèmes de traitement automatisé de données et d'autre part, les infractions favorisées par l'utilisation des technologies de l'information et de la communication telles que l'incitation au terrorisme et à la haine raciale sur Internet, l'escroquerie en ligne, la contrefaçon, les infractions aux cartes bancaires ou tout autre violation de la propriété intellectuelle.

Même si l'on pourrait penser à première vue que la matière fiscale en est éloignée, celle-ci est concernée par ces deux types d'infractions. En d'autres termes, la matière fiscale est amenée à évoluer pour s'adapter aux risques liés à la cybercriminalité. Or, en ce domaine des progrès restent à réaliser. En effet, le constat peut paraître sévère, mais il conduit à considérer que les dispositifs de lutte contre la cybercriminalité en matière fiscale présentent plus de faiblesses que de forces.

Certes, des nuances peuvent permettre d'atténuer la sévérité de ce constat. D'une part, la fraude a toujours existé. La cyberfraude fiscale n'est donc qu'une forme moderne de la fraude fiscale. D'autre part, si l'administration fiscale française est vulnérable, elle ne l'est pas davantage que d'autres administrations publiques françaises ou étrangères. Il importe de rappeler à cet égard que des institutions aussi prestigieuses que le Fonds monétaire international (FMI) ou que la CIA ont été victimes ces derniers mois de cyberattaques. Ce phénomène concerne également de grandes entreprises (Sony, la banque américaine City Group, RSA Security). Ce problème se manifeste donc à l'échelle mondiale et dans tous les secteurs, publics ou privés. Enfin, l'administration fiscale française peut se prévaloir de ses points forts, celle-ci étant réactive et figurant parmi l'une des plus modernes au monde. Cependant, au regard des avancées technologiques, la cybercriminalité met aux prises l'administration fiscale et le cyberfraudeur. L'administration fiscale est donc amenée à se doter des moyens adéquats pour se protéger dans le cyberespace où elle évolue désormais à l'instar des autres administrations.

Néanmoins, sa particularité la place en position de cible privilégiée par rapport aux cyberattaques. Or, son dispositif de protection présente un certain nombre de faiblesses. Ces dernières ouvrent la voie à des pistes d'amélioration que l'administration fiscale gagnerait à ne pas négliger dans un contexte où elle est exposée à des risques de tous ordres, qu'ils soient financiers ou technologiques.

1. La lutte contre la cybercriminalité visant les administrations fiscales : un dispositif à parfaire

Les points faibles de la lutte contre la cybercriminalité en matière fiscale s'expliquent par l'existence d'une frontière délicate de la notion de cyberfraude fiscale et d'un dispositif insuffisamment protecteur.

A) La cyberfraude fiscale, une notion aux frontières délicates

La notion de cyberfraude fiscale est complexe. Elle ne se résume pas à la simple fraude fiscale, celle-ci ne prenant pas suffisamment en considération l'impact des nouvelles technologies. Deux catégories de cyberfraudes fiscales sont à prendre en compte. En effet, doivent être envisagées non seulement les fraudes liées à une dimension matérielle, mais aussi celles qui résultent d'un montage financier. Ces dernières peuvent être difficiles à déceler au contraire de la première catégorie qui vise des cas de fraude avérée.

1) La cyberfraude fiscale liée à un montage financier

Aux termes du Code général des impôts, la fraude fiscale est le résultat de l'action de quiconque qui « s'est frauduleusement soustrait ou a tenté de se soustraire frauduleusement à l'établissement ou au paiement total ou partiel des impôts »[1]. Sont visées à la fois les omissions volontaires de déclaration fiscale dans les délais prescrits, les dissimulations volontaires d'une part des sommes sujettes à l'impôt, l'organisation d'insolvabilité, les manœuvres visant à faire obstacle au recouvrement de l'impôt ou encore toute autre pratique frauduleuse. En principe, ces pratiques illégales sont passibles, indépendamment des sanctions fiscales, d'une amende de trente-sept mille cinq cents euros et d'un emprisonnement de cinq ans. Cependant, l'amende peut atteindre soixante-quinze mille euros lorsque ces faits ont été réalisés ou facilités au moyen d'achats ou de ventes sans facture ou de facture ne se rapportant pas à des opérations réelles, ou encore, lorsqu'ils ont eu pour objet d'obtenir de l'État des remboursements injustifiés.

Le dispositif répressif est d'autant plus sévère que la fraude fiscale constitue un manque à gagner important pour l'État, évalué en 2007 par le Conseil des prélèvements obligatoires entre vingt et vingt-cinq milliards d'euros par an. À titre de comparaison, la fraude aux prélèvements obligatoires représenterait chaque année de huit à quinze milliards d'euros. S'agissant des impôts, la fraude concerne plus particulièrement la TVA (sept à douze milliards d'euros), mais également l'impôt sur les sociétés (cinq milliards d'euros), l'impôt sur le revenu (quatre milliards d'euros) et les impôts directs locaux (deux milliards d'euros)[2]. La lutte contre la fraude fiscale aurait rapporté à l'État français cinquante milliards d'euros depuis 2007[3]. Les contrôles fiscaux menés ont ainsi permis à la France de percevoir seize milliards d'euros de droits et pénalités en 2010 contre quinze milliards d'euros en 2009.

Si la fraude fiscale représente des enjeux importants pour l'État, il n'est pas toujours aisé d'établir une frontière entre la fraude fiscale et l'optimisation fiscale qui consiste en une utilisation habile des lois et conventions fiscales en vue de supprimer ou de réduire la charge fiscale. Dans la mesure où elles respectent le cadre légal, de telles pratiques ne peuvent être dénoncées par l'administration fiscale, à moins qu'elles ne soient constitutives d'un abus de droit[4].

La clarification des frontières est d'autant plus nécessaire qu'une troisième notion intervient pour caractériser les montages financiers à travers le concept d'évasion fiscale. Sont ainsi visés, dans leur ensemble, les comportements d'un contribuable destinés à réduire le montant des prélèvements normalement dus. Deux situations doivent alors être distinguées. Lorsque le contribuable recourt à des moyens légaux, l'évasion peut être considérée comme de l'optimisation fiscale. Au contraire, si le contribuable utilise des techniques illégales ou dissimule la portée véritable de ses opérations, l'évasion pourra être

1. Article 1741 du Code général des impôts.

2. Conseil des prélèvements obligatoires, *La fraude aux prélèvements obligatoires et son contrôle,* mars 2007.

3. Cf. le Discours de Valérie Pécresse, ministre du Budget, des Comptes publics et de la Réforme de l'État, Porte-parole du Gouvernement, lors de la conférence de presse « Lutte contre la fraude fiscale », Bercy, 24 novembre 2011.

4. Figurant à l'article 64 du Livre des procédures fiscales, cette notion renvoie à un détournement à des fins uniquement fiscales d'un dispositif juridique ayant pour objectif de produire d'autres effets. L'abus de droit peut se présenter sous différentes formes. Il peut d'une part, s'agir de l'abus de droit par dissimulation. Cette hypothèse recoupe celle de la dissimulation de la réalité par réalisation d'un acte fictif ou déguisé. L'abus de droit peut d'autre part résulter d'un montage juridique artificiel, régulier au regard des autres branches du droit, mais motivé uniquement par la volonté de se soustraire à une règle fiscale pour échapper à l'imposition. Enfin, depuis la loi n° 2008-443 du 30 décembre 2008, l'abus de droit peut être caractérisé par la recherche d'une application littérale des textes à l'encontre des objectifs poursuivis par les auteurs.

analysée comme un montage frauduleux, susceptible de sanction par conséquent.

Face à la difficulté de définir précisément les notions d'optimisation fiscale et d'évasion fiscale, la fraude fiscale peut s'en trouver facilitée. En la matière, l'apparition de l'économie numérique peut y contribuer dans la mesure où la législation fiscale ne prend pas toujours en considération cette évolution. Il en résulte des possibilités réelles pour certaines entreprises qui essaieront de tirer profit de ces failles[5]. L'objectif recherché consiste pour ces dernières à minorer leur imposition, voire à échapper à l'impôt en faisant varier à leur profit la limite entre la fraude fiscale et l'optimisation fiscale.

Un tel contexte incite à poser la question de savoir si le cyberespace est devenu un paradis fiscal. En ce sens, le cyberespace offre plus de facilités pour domicilier les comptes bancaires à l'étranger. De même, il faut évoquer le cas des déclarants exerçant leur activité grâce à Internet sans la déclarer parce qu'ils pensent que cette nouvelle technologie de la communication leur permet d'échapper au regard de l'administration fiscale en toute impunité. Or, il est vrai que les contrôles fiscaux sont plus difficiles à réaliser dans le cyberespace.

S'agissant de la volonté de lutter contre la fraude fiscale liée à l'économie numérique, la France a souhaité faciliter les obligations fiscales dans ce secteur en mettant en place en 2008 le statut de l'auto-entrepreneur[6]. Un régime fiscal et social simplifié et libératoire a été introduit pour permettre notamment à l'internaute détenteur d'un e-commerce d'exercer ses activités en toute légalité. Si ce statut ne vise pas spécifiquement les internautes, mais a été créé plus largement à destination de ceux qui souhaitent mener une activité indépendante, à titre principal ou de façon accessoire à un statut de salarié ou de retraité[7], les entrepreneurs du secteur de l'économie numérique en sont les principaux bénéficiaires dans la mesure où l'objectif de cette mesure était notamment d'endiguer le développement de l'économie parallèle. 23 % des auto-entrepreneurs auraient saisi l'occasion de professionnaliser une activité déjà exercée[8].

En outre, il importe de souligner que le législateur est certes intervenu à plusieurs reprises ces dernières années[9] pour renforcer le cadre existant et mieux lutter contre la fraude fiscale et l'évasion fiscale, mais les mesures en question ne traitent pas spécifiquement les montages financiers liés au développement de l'économie numérique qui constituent pourtant une problématique particulière.

Aussi, est-il possible de considérer que ces dispositifs, restent insuffisants pour lutter contre la fraude fiscale liée à l'économie numérique, d'autant que la perte de recettes fiscales de l'État liée au développement du numérique ne résulte pas uniquement des montages financiers qui sont favorisés par les possibilités offertes par les nouvelles technologies, mais s'explique également par une dimension matérielle. Si les cyberfraudes résultant des montages financiers souvent complexes sont pour cette raison difficiles à déceler, cette deuxième catégorie de pratique frauduleuse en matière fiscale est au contraire plus facile à identifier.

2) La cyberfraude fiscale liée à une dimension matérielle

Les fraudes fiscales liées à une dimension matérielle se présentent sous deux formes puisque sont visées à la fois celles qui sont consécutives aux attaques contre le réseau informatique des administrations fiscales et celles qui sont favorisées par l'inadaptation des logiciels comptables.

a. Les attaques contre le réseau informatique des administrations fiscales

Les attaques contre le réseau informatique des administrations fiscales poursuivent deux objectifs : la subtilisation des données sensibles (données bancaires ou autres données personnelles) et le détournement de celles-ci. Dans ce dernier cas, l'objectif est de modifier directement les informations concernant un ou plusieurs contribuables, soit pour minorer son imposition, soit, à l'inverse, pour augmenter l'imposition d'un tiers… à travers par exemple une hausse artifi-

5. Concernant ces failles et l'inadaptation de la législation fiscale à l'économie numérique, cf. W. Gilles, « Les transformations du droit fiscal à l'ère du numérique », *Revue de l'Institut du Monde et du Développement* (RIMD), n° 1, 2011.
6. Cf. la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie.
7. Cf. l'exposé des motifs de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie.
8. Cf. « L'auto-entreprise au service de la lutte contre le travail illégal », *La Tribune*, 26 septembre 2010.
9. Cf. *infra*.

cielle des revenus. S'il est vrai qu'une telle situation apparaît moins probable, il n'en demeure pas moins qu'elle reste possible et ne serait-ce que pour cette raison, il convenait également de la mentionner brièvement.

La subtilisation des données sensibles constitue, quant à elle, un cas avéré. Pour illustrer cette problématique, il est possible de rappeler les deux catégories d'attaques dont a été victime en 2011 le ministère français du Budget.

D'une part, cette institution a été victime d'une intrusion informatique d'ampleur pendant plusieurs mois. Révélé en mars 2011, le piratage en question avait été considéré à l'époque comme le plus important auquel l'État français avait dû faire face jusqu'à présent. Ayant concerné plus de cent cinquante ordinateurs du ministère, il avait été mené à partir d'une adresse e-mail piratée qui avait permis au pirate de prendre le contrôle de l'ordinateur ciblé après avoir envoyé une pièce jointe contenant un cheval de Troie. Ce procédé avait ensuite permis d'infiltrer à leur tour les correspondants de l'ordinateur cible au sein de l'administration. Officiellement, le piratage informatique avait certes, en l'espèce, visé uniquement des informations relatives à l'organisation du G20 et la Direction centrale du renseignement extérieur avait été saisie, mais il n'en demeure pas moins que l'intrusion dans le réseau de l'administration fiscale aurait pu potentiellement être réalisée à d'autres fins. Il n'est donc pas à exclure qu'à l'avenir le ministère du Budget soit victime de nouvelles attaques ayant pour objectif, cette fois, une dimension plus préjudiciable s'agissant de la fraude fiscale, d'autant que d'autres tentatives d'intrusion ont été menées par la suite, mais en vain, cette fois-ci.

D'autre part, début décembre 2011, le ministère du Budget a porté plainte contre X pour escroquerie après avoir constaté que des pirates informatiques avaient usurpé le nom du site officiel de l'administration pour extorquer à des contribuables leurs numéros de comptes et de cartes bancaires. En l'espèce, procédant selon la technique de l'hameçonnage (ou phishing) qui est destinée à récupérer des données personnelles d'un internaute, les « cyberescrocs » leur avaient envoyé un courriel imitant le site officiel de l'administration fiscale et annonçant une erreur des impôts en leur faveur. Afin de régulariser sa situation, le destinataire du message devait, en retour, se rendre sur un site particulier pour remplir une fiche contenant ses coordonnées bancaires précises. Les « cyberescrocs » avaient agi depuis un faux site Internet qui appartenait à une société néerlandaise. Cependant, comme l'a rappelé le ministère du Budget, l'administration fiscale ne demande jamais aux contribuables de lui communiquer les coordonnées de ses comptes ou les numéros de ses cartes bancaires. En outre, le courriel comportait de nombreuses fautes d'orthographe et des mentions impropres, le message employant notamment le terme d'« usager » en lieu et place de celui de « contribuable ».

Ces exemples, qui sont récents, ne sont pas exhaustifs et se rencontrent dans de nombreux autres pays occidentaux, sont certainement appelés à se multiplier à l'avenir, ce qui suppose une vigilance accrue du contribuable-internaute.

b. L'inadaptation persistante des logiciels à la fraude aux comptabilités informatisées

Les fraudes issues de l'inadaptation des logiciels comptables posent le problème du contrôle des comptabilités informatisées des entreprises assujetties à l'impôt. Pour saisir les enjeux liés à ces mutations, il importe de rappeler qu'à l'ère prénumérique, les comptabilités tenues sur papier permettent plus facilement à l'administration fiscale de vérifier que les comptes des entreprises n'avaient pas été modifiés *a posteriori* et reflétaient une image fidèle de l'activité de l'entreprise. Au contraire, à l'ère numérique, les comptabilités tenues sur des logiciels informatiques n'offrent pas les mêmes garanties en terme de vérification, en particulier parce qu'ils permettent des retraitements ou des modifications de l'information à tout moment.

Toutefois, l'administration fiscale est consciente des lacunes générées par ces logiciels. La publication en 2006 d'une Instruction fiscale relative au contrôle des comptabilités informatisées[10] était destinée à répondre à ces préoccupations. Remplaçant les instructions 13 L-6-91 du 14 octobre 1991 et 13 L-9-96 du 24 décembre 1996, elle commente les règles applicables pour le contrôle des comptabilités informatisées dont le cadre juridique est défini

10. Instruction fiscale 13 L-1-06, Bulletin officiel des impôts, n° 12 du 24 janvier 2006.

par les articles L. 13[11], L. 47 A[12], L. 57[13], L. 74[14] et L. 102 B du Livre des procédures fiscales[15]. La nouvelle réglementation, qui prend davantage en compte l'évolution technologique, s'applique à tous les contribuables, indépendamment de leur activité et de leur régime d'imposition, qui sont astreints à tenir et à présenter des documents comptables et qui choisissent de le faire au moins partiellement au moyen de systèmes informatisés lorsque ces systèmes servent à justifier une écriture comptable.

La nouvelle instruction précise quelles sont les fonctions indispensables d'un logiciel comptable et le périmètre informatique d'un contrôle, mais également les obligations qui pèsent en matière de conservation. En particulier, elle rappelle le caractère non sincère, non régulier et probant pour les comptabilités informatisées qui sont tenues à partir d'un logiciel comptable ne garantissant pas l'irréversibilité et l'intangibilité des écritures validées. S'agissant des comptabilités informatisées, l'administration fiscale conclura, sauf exception, à leur irrégularité ou à leur caractère non probant si les documents comptables et les pièces justificatives dématérialisés qui sont obligatoires sont présentés sous des formats non recevables (absence de lisibilité, doute sur le propriétaire), lorsque les écritures comptables ne permettent pas de valider les pièces justificatives ou inversement, si les exercices comptables ne sont pas clôturés ou ne permettent pas de retracer correctement les écritures (absence de traçabilité ou de chronologie des enregistrements), lorsqu'il n'existe pas de permanence du chemin de révision ou encore, en cas d'insuffisance de l'archivage des données, par exemple pour une entreprise qui aurait archivé uniquement des données agrégées ou des échantillons de données.

En effet, l'entreprise doit recourir à des procédures de conservation et d'archivage permettant de présenter tous documents et données à l'Administration fiscale lorsqu'elle en fait la demande. À cet égard, la signature électronique est admise dès lors qu'elle est considérée comme fiable, la charge de la preuve étant inversée conformément à l'article 1316-4 du Code civil qui prévoit que « la fiabilité de ce procédé est présumée, jusqu'à preuve du contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées en Conseil d'État ». Or, ces dernières ont été fixées en 2001[16]. Pour qu'elle soit considérée comme fiable, la signature électronique doit remplir trois conditions. Elle doit d'une part, être sécurisée (i) et d'autre part être établie grâce à un dispositif sécurisé de création de signature (ii).

Pour répondre à ces exigences, il importe de prévoir des moyens techniques et des procédures appropriées qui garantissent que les données de création de la signature électronique ne pourront être qu'à usage unique, qu'elles seront confidentielles, qu'elles ne pourront être trouvées par déduction et que la signature ne pourra faire l'objet d'une falsification ou qu'elle sera protégée de manière satisfaisante par le signataire contre toute utilisation par des tiers. Par ailleurs, la signature ne doit permettre aucune altération du contenu de l'acte à signer et ne pas altérer la connaissance exacte que le signataire pourrait avoir sur le document avant de le signer.

Enfin, et c'est la troisième condition, la signature électronique doit être certifiée conforme aux exigences définies précitées (iii). Cette certification peut être réalisée soit par les services du Premier ministre chargés de la sécurité des systèmes d'information ou par des organismes agréés par ces services, soit par un organisme désigné à cet effet par un État membre de l'Union européenne.

La nouvelle réglementation rappelle également

11. L'alinéa 2 de cet article prévoit que « lorsque la comptabilité est tenue au moyen de systèmes informatisés, le contrôle porte sur l'ensemble des informations, données et traitements informatiques qui concourent directement ou indirectement à la formation des résultats comptables ou fiscaux et à l'élaboration des déclarations rendues obligatoires par le Code général des impôts ainsi que sur la documentation relative aux analyses, à la programmation et à l'exécution des traitements ».

12. Cet article précise les garanties accordées au contribuable en matière de vérification lorsque la comptabilité est tenue au moyen de systèmes informatisés.

13. Article relatif à la procédure de rectification contradictoire.

14. Cette disposition rappelle que la procédure d'évaluation d'office s'applique en cas d'opposition à la mise en œuvre d'un contrôle qui porte sur une comptabilité tenue au moyen de systèmes informatisés.

15. Ces dispositions sont issues de la loi de finances 1990 n° 89-935 du 29 décembre 1989.

16. Cf. l'article 2 du décret n° 2001-272 du 30 mars 2001.

quelles sont les responsabilités de chaque intervenant, qu'il soit éditeur de logiciel comptable ou utilisateur de celui-ci. En cas de contrôle effectué sur place de la comptabilité informatisée, les traitements demandés par l'administration respectent la procédure de rectification contradictoire des articles L. 55 et suivants du Livre des procédures fiscales. Ils font donc l'objet d'un débat oral et contradictoire comme dans le cadre du contrôle des comptabilités « papier », mais peuvent aussi déboucher sur une procédure d'imposition d'office en cas d'opposition à la mise en œuvre du contrôle des comptabilités informatisées, selon les modalités de l'article L. 47 A précité du Livre des procédures fiscales.

Le cadre juridique mis en place est donc assez contraignant et l'instruction de 2006 a permis d'améliorer le contrôle sur les comptabilités informatisées. Cependant, malgré ces avancées, cette instruction demeure insuffisante parce qu'elle ne permet pas de régler l'ensemble des lacunes.

À cet égard, le Conseil des prélèvements obligatoires[17] a relevé en 2007 l'absence d'homogénéité s'agissant de la sécurité des logiciels de comptabilité dans la mesure où « la plupart d'entre eux ont un caractère permissif ». Il en résulte que les entreprises qui tiennent une comptabilité informatisée disposent « d'une grande souplesse au niveau des modalités d'élaboration des écritures comptables » puisque ces logiciels permettent de redonner *a posteriori* une cohérence à des écritures comptables pourtant biaisées par certains procédés de fraude.

De même, il importe de souligner que 10 % des redressements débouchant sur des pénalités exclusives de bonne foi concernent des situations d'impossibilité d'exercer un véritable contrôle du fait de la présence de comptabilités informatisées. Or, cette situation est appelée à perdurer tant que les éditeurs de logiciels refuseront de proposer des produits garantis contre la fraude et que l'administration fiscale ne disposera pas de moyens matériels et des ressources humaines suffisamment formées pour déceler ces nouvelles irrégularités. En ce sens, le Conseil des prélèvements obligatoires a préconisé dès 2007 de former les vérificateurs à l'utilisation des progiciels et à la mise en place d'un contrôle fiscal qui sorte des seules données comptables pour apprécier la cohérence d'ensemble de ces dernières avec les données de gestion.

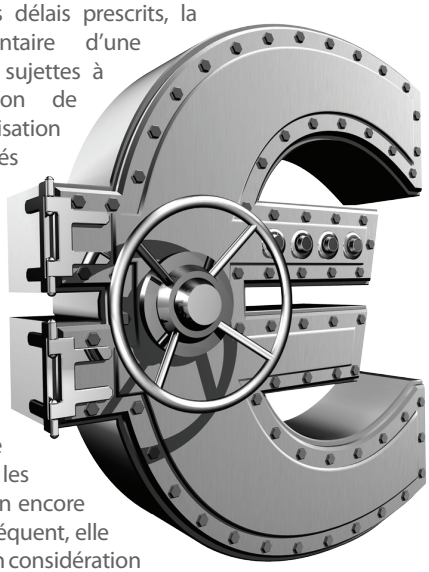
17. Conseil des prélèvements obligatoires, *La fraude aux prélèvements obligatoires et son contrôle,* 2007.

B) Un dispositif insuffisamment protecteur

1) Une législation fiscale inadaptée

Les lacunes de la législation fiscale tiennent principalement à une adaptation insuffisante de cette dernière aux enjeux de la société numérique.

À cet égard, il convient de se référer en premier lieu à la fraude fiscale qui est envisagée à l'article 1741 du Code général des impôts. Sur les quatre catégories de fraude fiscale énoncées par ce texte, seule la dernière peut, en raison de son caractère *sus generis,* permettre d'appréhender la fraude fiscale. La situation n'est pourtant pas satisfaisante dans la mesure où la cyberfraude fiscale n'est pas envisagée en tant que telle, mais uniquement dans une catégorie *sus generis.* Les catégories de fraude fiscale évoquées sont constituées par l'omission volontaire de la déclaration dans les délais prescrits, la dissimulation volontaire d'une partie des sommes sujettes à l'impôt, l'organisation de l'insolvabilité ou l'utilisation d'autres procédés visant à empêcher le recouvrement de l'impôt, ainsi que par le recours à tout autre agissement frauduleux. Cette dernière catégorie se caractérise par une formulation suffisamment large pour appréhender les formes de fraude non encore envisagées. Par conséquent, elle permet de prendre en considération la cyberfraude fiscale.



En second lieu, il est possible d'invoquer le délit général de passation d'écritures fictives et

d'entremise[18], notamment en cas d'omission volontaire d'écriture comptables ou de passation d'écritures inexactes ou fictives, ce qui permet par conséquent d'appréhender les fraudes fiscales résultant de retraitements ou des modifications de la comptabilité informatisée.
Ces deux fondements offrent certes une base légale pour faire face à la cyberfraude fiscale. Cependant, ils demeurent insuffisants et trop indirects. En effet, l'ampleur des enjeux pose la question de savoir s'il ne faudrait pas actualiser la définition de la fraude fiscale pour envisager expressément les cas de cyberfraude… d'autant que ni la définition de l'article 1741 du Code général des impôts, ni le délit évoqué à l'article 1743 de ce Code ne permettent d'appréhender les cyberattaques à l'encontre de l'administration fiscale. Une cyberattaque n'est en effet pas de la fraude fiscale au sens traditionnel !
En l'absence de sanctions spécifiques aux cyberfraudes dans le Code général des impôts et dans le Livre des procédures fiscales, il faut se référer au droit commun prévu par le Code pénal en matière de cybercriminalité.

2) Des sanctions pénales insuffisantes au regard des enjeux économiques

Le Code pénal prévoit certes des sanctions visant à réprimer des actes de cybercriminalité en cas d'usurpation en ligne et d'atteintes aux systèmes de traitement automatisé de données. Ainsi, une personne qui usurpe l'identité d'un tiers ou utilise une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, risque une peine d'un an d'emprisonnement et de quinze mille euros d'amende, y compris si cette infraction est commise sur un réseau de communication au public en ligne[19]. Cependant, ces peines sont dérisoires au regard de ce que peut rapporter l'hameçonnage au cyberfraudeur qui usurpe le nom du site officiel de l'administration fiscale pour se procurer les numéros de comptes et de cartes bancaires. En outre, de tels agissements obligent le ministère du Budget à mener une campagne de communication importante sur Internet et dans les médias pour rappeler aux contribuables qu'ils ne doivent jamais communiquer leurs numéros de comptes et de cartes bancaires dans la mesure où l'administration fiscale ne demande jamais ces renseignements.
Par ailleurs, en ce qui concerne les atteintes aux systèmes de traitement automatisé de données, les sanctions pénales[20] sont de deux ans d'emprisonnement et de trente mille euros d'amende pour l'accès ou le maintien, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données. Les sanctions atteignent trois ans d'emprisonnement et quarante-cinq mille euros d'amende si l'accès ou le maintien, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données a eu pour conséquence soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système.
Dans le même sens, le cyberfraudeur encourt cinq ans d'emprisonnement et soixante-quinze mille euros d'amende pour toute action entravant ou faussant le fonctionnement d'un système de traitement automatisé ou encore toute introduction frauduleuse des données dans un système de traitement automatisé ou suppression ou modification frauduleuse des données qu'il contient. En outre, est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée, le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions susmentionnées. Il en est de même pour la participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions susmentionnées.
Des peines complémentaires existent pour les personnes physiques coupables des délits susmentionnés, mais celles-ci restent mineures au regard des faits reprochés en cas de cyberattaque contre l'administration fiscale. Il s'agit de l'interdiction, pour une durée de cinq ans au

18. Cf. l'article 1743 du Code général des impôts.
19. Cf. l'article 226-4-1 du Code pénal.
20. Cf. les articles 323-1 à 323-4 du Code pénal.

plus, de bénéficier des droits civiques, civils et de famille ; d'exercer une fonction publique ou une activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ; ou encore, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés. D'autres peines complémentaires s'appliquent, à savoir la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution (en l'occurrence, il peut ne s'agir que d'un simple ordinateur !) ; la fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ; l'exclusion, pour une durée de cinq ans au plus, des marchés publics ; l'affichage ou la diffusion de la décision prononcée.

Un dispositif de sanctions pénales existe donc pour réprimer les cyberattaques menées contre l'administration fiscale. Cependant, sont-elles adaptées aux enjeux en cause ? En d'autres termes, le fait de supprimer des données dans le serveur de l'administration fiscale vaut-il quarante-cinq mille euros ?

L'attaque dont a été victime le ministère français du Budget et qui a été révélée en mars 2011 a obligé l'État à mener des recherches importantes pour identifier les cent cinquante fonctionnaires ciblés par les pirates et s'assurer que le piratage ne concernait pas d'autres administrations publiques. Elle l'a aussi conduit à entreprendre, pendant plusieurs semaines, une vaste opération de maintenance pour sécuriser le réseau informatique de l'administration fiscale. De plus, comme souvent dans des circonstances similaires, il est nécessaire de mener des investigations importantes pour pouvoir remonter à la source de ces attaques. En effet, non seulement les pirates, avant d'atteindre leur cible, transitent par plusieurs pays à travers de nombreux ordinateurs qui servent de relais à l'insu de leurs propriétaires, mais en outre, de tels agissements sont fréquemment menés par des professionnels organisés à partir d'un mode opératoire sophistiqué et des moyens importants, ce qui complique les investigations menées. Ces attaques engendrent donc souvent un coût important en plus, en plus de celles liées à la fraude fiscale qui peut en résulter.

Pour ces raisons, il semble possible d'affirmer que les sanctions prévues par le législateur sont dérisoires au regard des bénéfices pour le cyberescroc ou le cyberfraudeur, mais également pour les préjudices subis par l'administration fiscale. Or ceux-ci sont potentiellement doubles pour l'administration fiscale en cas de cyberattaque. En effet, comme il l'a été souligné précédemment, un premier coût résulte de l'attaque du réseau de l'administration fiscale, à l'instar cependant des autres administrations publiques qui seraient attaquées. Mais un second coût peut également apparaître si la cyberattaque a conduit à supprimer ou à détourner une partie de l'information que l'administration fiscale possède sur le contribuable (soit pour minorer le revenu d'un contribuable, soit pour rendre plus difficiles les contrôles fiscaux en effaçant les données compromettantes). Certes une directive visant à renforcer les sanctions pénales en matière de cyberattaques est en cours d'adoption. Il s'agit d'une proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil. Cette directive prévoit une peine maximum de cinq ans à l'instar de ce qui est déjà prévu par le Code pénal en France. Aussi, la question de l'insuffisance des sanctions n'est-elle pas encore résolue. D'où la nécessité de rechercher des voies d'amélioration.

2. Les pistes d'amélioration en matière de lutte contre la cyberfraude fiscale

Des solutions peuvent être envisagées selon trois axes : inciter l'administration fiscale à renforcer la sécurité de son réseau, concevoir de nouveaux procédés de stockage des justificatifs fiscaux, adapter le droit fiscal à l'évolution de la société numérique.

A) L'administration fiscale dans l'obligation de renforcer la sécurité de son réseau

Il va de soi que l'ampleur des risques liés à la cyberfraude fiscale impose à l'administration fiscale de mettre en œuvre les moyens adéquats pour se prémunir contre les cyberattaques dont elle peut faire l'objet. Une telle nécessité s'impose à un double niveau. Il importe d'une

part, pour l'administration fiscale, à l'instar des autres administrations de l'État, de sécuriser son système d'informations pour se prémunir contre une pénétration frauduleuse sur son réseau destinée à récupérer les données sensibles, à les effacer, ou à les détourner. Il s'avère d'autre part indispensable de sécuriser les télédéclarations fiscales, autrement dit, de veiller à la fiabilité des télétransmissions et mettre en place tous les outils nécessaires pour lutter contre les interceptions de données.

Ce renforcement de la lutte contre la cybercriminalité suppose bien entendu de se doter des logiciels informatiques contre le piratage. Au-delà, l'administration fiscale doit désormais également veiller à mieux former les personnels aux risques qu'ils sont susceptibles de véhiculer (précaution dans l'ouverture des courriels et des clés USB. La cyberattaque contre les ordinateurs de Bercy en mars 2011 rappelle que les agents qui ne sont pas suffisamment vigilants dans la consultation de leur messagerie électronique peuvent être à l'origine, malgré eux, de l'intrusion du pirate dans le système d'informations des administrations publiques.

Outre, le renforcement de la sécurité en ce qui concerne l'accès au réseau, l'administration fiscale se trouve dans l'obligation de renforcer ses procédures d'authentification. Plus précisément, l'administration fiscale doit se prémunir également contre l'usurpation d'identité. Autrement dit, il s'agit d'éviter que des personnes ou des entités malveillantes se fassent passer pour l'administration fiscale pour récupérer des données sensibles[21]. D'où la nécessité pour l'administration fiscale de se doter d'un système d'identification infalsifiable vis-à-vis des contribuables utilisateurs des services en ligne afin de garantir l'absence de doute quant à l'auteur des messages et d'intensifier les campagnes de communication à destination des contribuables pour informer de ces pratiques.

L'obligation pour l'administration fiscale de renforcer la sécurité de son réseau et ses procédures d'authentification est une nécessité actuelle destinée à se prolonger à l'avenir. La pénétration frauduleuse sur le réseau de l'administration fiscale et l'usurpation d'identité de l'administration fiscale sont des problèmes réels aujourd'hui, et ce, alors même que les contribuables n'ont pas encore la possibilité de payer leurs impôts directement en ligne au moyen d'une carte bancaire comme ils peuvent déjà le faire sur les sites marchands. Or, on peut espérer qu'à l'avenir l'administration fiscale développe ce mode de paiement, ce qui suppose, bien entendu, de renforcer la sécurité de son réseau afin de se prémunir en particulier contre le piratage des réseaux et l'hameçonnage.

21. Technique de l'hameçonnage évoquée précédemment.

B) Vers de nouveaux procédés de stockage des justificatifs fiscaux ?

L'émergence d'une e-administration fiscale permet d'offrir de nouveaux services aux contribuables et en particulier la télédéclaration fiscale. Cette évolution n'est pas sans conséquence sur les contrôles réalisés par l'administration fiscale. En effet, ces transformations conduisent à créer un décalage entre l'émergence de l'e-administration fiscale et les formes traditionnelles des contrôles opérés par l'administration fiscale.

Ainsi, la dématérialisation des systèmes d'information pose un certain nombre de difficultés. Il s'agit notamment de l'absence de justificatifs à fournir à l'appui de la télédéclaration, ceux-ci étant seulement conservés par le contribuable. Dans ce contexte, la fraude pourrait être tentante même si l'administration fiscale est en droit de réclamer ultérieurement ces justificatifs lors d'un contrôle à venir. Aussi, ces éléments laissent-il entrevoir que le dispositif actuel pourrait devenir une source de contentieux important à l'avenir, notamment dans le cas de la perte des justificatifs que les contribuables ne devraient plus fournir, mais seulement conserver. Cette perspective incite donc à élaborer de nouveaux procédés de stockage des justificatifs fiscaux. En effet, cela pourrait être un des moyens susceptibles d'atténuer le développement d'un tel contentieux pour favoriser au contraire, les relations amiables entre l'administration fiscale et les contribuables. En particulier il serait opportun de développer le coffre-fort électronique au niveau de l'administration fiscale. Par ce procédé, le contribuable pourrait stocker tous ces justificatifs qu'il aurait lui-même numérisés. Néanmoins, des dispositifs de

sécurité s'imposent pour garantir l'efficacité de ce système. Il faudrait en revanche s'assurer que du côté de l'administration fiscale, il n'y ait pas de moyen de supprimer les justificatifs stockés, non par crainte que l'agent de l'administration fiscale suscite un redressement en supprimant l'archive électronique du justificatif (si bien que l'administré ne disposerait plus de preuve !), mais surtout pour se prémunir des attaques extérieures qui pourraient aboutir à détruire une partie de ces données personnelles et/ou sensibles.
Les cyberattaques menées récemment montrent que même pour les institutions les mieux protégées au monde, cette éventualité ne relève pas de la fiction. En plus de ces avancées, le droit fiscal doit aussi mieux appréhender les mutations résultant du développement de la cyberfraude fiscale.

C) Adapter le droit fiscal à l'évolution de la société numérique

Le droit fiscal doit se doter d'un dispositif répressif plus adapté. À cet égard et même si cette mesure n'est pas spécifique à la cyberfraude fiscale, il importe de rappeler que la loi de finances rectificative pour 2008[22] a étendu le délai de reprise de l'administration fiscale à dix ans pour permettre à cette dernière de disposer des moyens de lutter plus efficacement contre les fraudes dont la détection est particulièrement complexe. Si positive soit-elle, cette première avancée doit être poursuivie en prévoyant, cette fois, un dispositif centré sur les cyberfraudeurs ou les cyberescrocs qui visent l'administration fiscale. Autrement dit, le droit fiscal doit se doter d'un dispositif de sanctions pénales plus adapté à ces manœuvres frauduleuses.
Toutes les cyberattaques ne sont pas d'importance égale. Les cyberattaques contre l'administration fiscale semblent figurer parmi celles qui ont les conséquences les plus dommageables, avec sans doute, les cyberattaques contre le ministère de la Défense et les institutions qui protègent la sécurité nationale. Se pose alors la question de savoir s'il ne faudrait pas prévoir des sanctions spécifiques pour les cyberattaques à l'encontre des administrations fiscales ? À cet égard, le débat est ouvert et les termes de ce dernier sont identifiés. Mais quoi qu'il en soit, les sanctions doivent être davantage dissuasives et proportionnelles à l'enjeu de l'infraction : quel est en effet l'impact d'une amende de cinq ans d'emprisonnement et de soixante-quinze mille euros quand des millions d'euros sont potentiellement en jeu ?
Enfin, adapter le droit fiscal à l'évolution de la société numérique invite à envisager d'autres prolongements. Il importe en ce sens de former les agents de l'administration des finances publiques, mais aussi les étudiants aux problématiques liées à l'évolution du droit fiscal à l'ère du numérique. Il est également souhaitable de développer des réflexions sur ce sujet, notamment en approfondissant le lien entre fiscalité et économie numérique afin notamment d'éviter qu'Internet ne devienne un paradis fiscal ; ou encore, en étudiant davantage les conséquences du passage de l'administration fiscale vers l'e-administration fiscale, et en particulier la sécurité des réseaux.
De façon plus transversale, il conviendrait de développer une réflexion sur les nouvelles relations qui s'instaurent entre l'e-administration fiscale et l'e-contribuable. Parmi les voies à envisager, il est nécessaire de réfléchir à la mise en place de moyens adéquats visant à renforcer le dialogue entre l'e-administration fiscale et l'e-contribuable. Il faudrait aussi s'attacher à favoriser le développement des nouveaux procédés de stockage des justificatifs fiscaux et de veiller à leur fiabilité. Il importe enfin de s'intéresser à la possibilité pour le contribuable de payer directement en ligne ses impôts par carte bancaire et de manière sécurisée.
Ces pistes de réflexion ouvrent la voie à des transformations du droit fiscal qu'il importe au législateur et à l'administration fiscale d'appréhender afin d'éviter que le décalage entre les avancées technologiques et le droit ne conduise à des impasses ou à des vides juridiques.

William GILLES
Maître de conférences (HDR) à l'Université Paris 1 Panthéon-Sorbonne
Directeur du Master Droit du numérique Administration-Entreprises
Président de de l'Institut du Monde et du Développement (IMODEV)

22. Cf. l'article 52 de la loi n° 2008-1443 du 30 décembre 2008 de finances rectificative pour 2008.