SUPPRESSION ÉLECTRONIQUE DES VENTES: UNE MENACE POUR LES RECETTES FISCALES

OCDE

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

L'OCDE est un forum unique en son genre où les gouvernements de 34 démocraties œuvrent ensemble pour relever les défis économiques, sociaux et environnementaux que pose la mondialisation. L'OCDE est aussi à l'avant-garde des efforts entrepris pour comprendre les évolutions du monde actuel et les préoccupations qu'elles font naître. Elle aide les gouvernements à faire face à des situations nouvelles en examinant des thèmes tels que le gouvernement d'entreprise, l'économie de l'information et les défis posés par le vieillissement de la population. L'Organisation offre aux gouvernements un cadre leur permettant de comparer leurs expériences en matière de politiques, de chercher des réponses à des problèmes communs, d'identifier les bonnes pratiques et de travailler à la coordination des politiques nationales et internationales.

Les pays membres de l'OCDE sont : l'Allemagne, l'Australie, l'Autriche, la Belgique, le Canada, le Chili, la Corée, le Danemark, l'Espagne, l'Estonie, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Islande, Israël, l'Italie, le Japon, le Luxembourg, le Mexique, la Norvège, la Nouvelle-Zélande, les Pays-Bas, la Pologne, le Portugal, la République slovaque, la République tchèque, le Royaume-Uni, la Slovénie, la Suède, la Suisse et la Turquie. La Commission des Communautés européennes participe aux travaux de l'OCDE.

Photo crédits: couverture© © Patryk Kosmider - Fotolia.com

Table des matières

Résumé

Les techniques de « suppression électronique des ventes » facilitent la fraude fiscale et sont la cause de pertes fiscales très importantes au niveau mondial. Les systèmes de terminaux point de vente (PDV) utilisés dans le secteur de la vente au détail sont un élément essentiel des dispositifs généraux de vente et de comptabilité et constituent des outils comptables efficaces de gestion des entreprises. On attend d'eux, par conséquent, qu'ils contiennent des données primaires accessibles aux contrôleurs des impôts. En réalité, ces systèmes ne permettent pas seulement l'« écrémage » des recettes en espèces tout comme les systèmes manuels du type tiroir-caisse mais, équipés d'un logiciel de suppression électronique des ventes, ils rendent possibles des méthodes de fraude plus complexes du fait de leur aptitude à modifier les données enregistrées afin de dissimuler les pratiques d'écrémage.

Les administrations fiscales perdent des milliards de dollars ou d'euros à cause des ventes non déclarées et de la dissimulation de recettes à l'aide de ces techniques. Une association canadienne du secteur de la restauration estime le total des ventes ainsi supprimées dans les restaurants canadiens à environ 2.4 milliards CAD par an. Depuis que le Groupe d'action de l'OCDE sur les délits à caractère fiscal et autres délits a commencé son travail d'enquête et de sensibilisation à ce phénomène, plusieurs pays (notamment la France, l'Irlande, la Norvège et le Royaume-Uni) ont mené des enquêtes dans le secteur de la vente au détail et découvert des problèmes significatifs. Parmi ces pays, l'Irlande est intervenue rapidement pour mettre en place une législation réprimant ces pratiques. D'autre part, un certain nombre de pays considèrent que s'attaquer vigoureusement à ce problème doit constituer un élément important de leur stratégie pour réduire le « manque à gagner » fiscal.

Le présent document examine les fonctions des systèmes PDV, ainsi que les domaines de risque spécifiques. Il décrit en détail les techniques de suppression électronique des ventes qui ont été découvertes par des spécialistes, en particulier « Phantomware » et « Zappers », et montre de quelle façon ces méthodes de fraude peuvent être détectées par les contrôleurs et enquêteurs fiscaux. Il note l'évolution constante des techniques de suppression électronique des ventes et la nécessité d'être vigilants face à ces changements.

Ce document recense et analyse les diverses méthodes employées par les pouvoirs publics pour lutter contre la fraude liée à la suppression électronique des ventes, en signalant certaines pratiques exemplaires, notamment : le renforcement du respect des normes, en mettant l'accent sur la discipline volontaire sous la responsabilité des organismes sectoriels ; la sensibilisation de l'ensemble des parties prenantes, y compris le public ; l'amélioration des compétences en matière de contrôle et d'enquête ; l'acquisition et l'échange de renseignements ; et l'utilisation de moyens techniques comme les systèmes PDV certifiés.

Le document formule les recommandations suivantes :

- Les administrations fiscales devraient établir une stratégie de lutte contre la suppression électronique des ventes dans le cadre de leur approche générale de discipline fiscale, afin que celle-ci tienne effectivement compte des risques posés par les systèmes de suppression électronique des ventes et encourage la discipline volontaire à l'impôt, et elles devraient renforcer les mesures de détection et de répression en ce domaine.
- Il faudrait mettre en place un programme de communication en vue de sensibiliser l'ensemble des parties prenantes au caractère criminel de l'utilisation de méthodes de suppression électronique des ventes et aux graves conséquences d'enquêtes et de poursuites qui peuvent en résulter.
- Les administrations fiscales devraient s'assurer que la législation leur accorde des pouvoirs adéquats aux fins du contrôle et de l'expertise légale des systèmes PDV.
- Les administrations fiscales devraient investir en vue d'acquérir les compétences et les outils nécessaires pour mener des contrôles et des enquêtes concernant les systèmes PDV, y compris en créant les fonctions de contrôleur numérique spécialisé et en recrutant, le cas échéant, des spécialistes de l'expertise légale numérique.
- Les administrations fiscales devraient envisager de recommander que la législation incrimine l'offre, la possession et l'utilisation d'un logiciel de suppression électronique des ventes.

Introduction

Contexte

L'utilisation de techniques de suppression électronique des ventes dans les systèmes de terminaux point de vente représente un développement inquiétant du point de vue de la fraude fiscale. Ce type de pratiques s'accroît depuis plus d'une décennie. Pendant cette période, des efforts localisés ont été engagés pour y répondre, tout particulièrement au Canada, en Allemagne, aux Pays-Bas et en Suède. Depuis que le Groupe d'action de l'OCDE sur les délits à caractère fiscal et autres délits a commencé son travail d'étude et de sensibilisation à ce sujet, plusieurs autres pays (notamment la France, l'Irlande, la Norvège et le Royaume-Uni) ont pris des mesures vigoureuses pour lutter contre ce phénomène. Le présent document vise à présenter la question à un public plus large, en montrant que, pour s'attaquer à ce problème, diverses formes d'intervention – techniques et opérationnelles, mais aussi politiques et stratégiques – sont nécessaires, et en formulant des recommandations d'action à l'intention des administrations fiscales et des pouvoirs publics en général.

Dans le secteur de la vente au détail, les caisses enregistreuses modernes fonctionnent comme des systèmes complets de vente et de comptabilité, en s'appuyant fréquemment sur des logiciels commerciaux standards, et constituent des outils de comptabilité commerciale efficaces pour la gestion de l'entreprise. On attend d'elles, par conséquent, qu'elles contiennent des données primaires accessibles aux contrôleurs des impôts, en particulier aux fins du contrôle de la taxe sur la valeur ajoutée (TVA) ou de la taxe sur les ventes. Cependant, il est clair aujourd'hui que ces systèmes peuvent être manipulés pour permettre l'« écrémage » des recettes en espèces, tout comme les systèmes manuels (tiroir-caisse ou double caisse), mais aussi qu'équipés d'un logiciel de suppression électronique des ventes, ils rendent possibles des méthodes de fraude beaucoup plus complexes du fait de leur aptitude à modifier les données enregistrées afin de dissimuler les pratiques d'écrémage.

Les termes de « caisse enregistreuse électronique » (ECR) et de « terminaux point de vente » (TPV) sont généralement utilisés pour désigner les caisses enregistreuses modernes mais, dans ce document, le terme générique de « systèmes PDV » est employé pour désigner ces deux types de machines et les systèmes hybrides.

Des experts légistes, des spécialistes du contrôle numérique, des enquêteurs criminels spécialisés dans la fraude fiscale, ainsi que des responsables de l'action publique ont contribué à réunir les informations nécessaires à la rédaction de ce rapport.[1] Ce groupe d'experts a aussi produit un ensemble d'outils (notamment des kits de formation, des directives et une bibliothèque d'informations techniques) à l'intention des contrôleurs et enquêteurs fiscaux. Les participants au groupe ont mis à profit cette expérience pour faire évoluer leur propre travail et les outils qu'ils ont conçus seront très utiles à d'autres administrations fiscales.

Ce document décrit les fonctions des caisses enregistreuses modernes, ainsi que le rôle des fabricants, fournisseurs et autres acteurs impliqués dans leur utilisation. Il passe en revue les divers moyens et techniques de suppression des ventes qui ont été découverts et les indices susceptibles d'en permettre la détection. Il examine aussi les estimations actuelles quant à l'ampleur de l'utilisation des techniques de suppression des ventes et des pertes fiscales qui en résultent. Enfin, il présente les différentes stratégies que peuvent adopter les pays à des fins de contrôle et d'enquête et formule des recommandations sur les mesures à prendre.

Autres travaux pertinents

Cette étude porte spécifiquement sur les conduites criminelles qu'impliquent les pratiques de suppression électronique des ventes, ainsi que sur le travail des enquêteurs criminels pour détecter, faire cesser et poursuivre de telles conduites. D'autres travaux davantage axés sur le respect de la législation et les problèmes que rencontrent les contrôleurs des impôts ont été réalisés dans le cadre du Forum de l'OCDE sur l'administration de l'impôt et du programme Fiscalis de l'UE.

Le **Groupe de projet sur les caisses enregistreuses**[2] du programme Fiscalis de l'Union européenne a produit en 2006 un « Guide de bonnes pratiques sur les caisses enregistreuses » (en anglais)[3], qui inclut une présentation détaillée de la législation de tous les États membres de l'UE, la liste des matériels et logiciels de caisses enregistreuses existants, un catalogue des risques spécifiques et des recommandations sur les bonnes pratiques de contrôle des caisses enregistreuses et des systèmes PDV.

Le **Forum sur l'administration de l'impôt** a produit en avril 2010 une note d'information qui comprend des recommandations sur les procédures à suivre pour assurer la fiabilité des données informatiques.[4]

Au cours du second semestre de 2010, l'équipe ZAPAT (Activity Team on Zappers and Phantomware) a été créée dans le cadre du **Project Group on E-Audit** de l'UE. S'appuyant sur les nouvelles modalités et méthodes de contrôle adoptées par les administrations fiscales des États membres de l'UE, la ZAPAT fédérera les bonnes pratiques et contribuera ainsi à améliorer encore le contrôle numérique des systèmes PDV. Elle produira ensuite, sur la base des résultats obtenus, une note d'orientation sur le contrôle numérique des systèmes PDV qui sera mise à la disposition des contrôleurs fiscaux des États membres de l'UE et complètera le travail présenté dans ce rapport.

Estimations des pertes dues à la fraude fiscale etautres formes de fraude

L'Association canadienne des restaurateurs et des services alimentaires a estimé que le total des ventes supprimées dans le secteur de la restauration atteignait environ **2.4 milliards CAD** pour l'année 2009.

Les pertes fiscales du Québec ont été estimées à **417 millions CAD** pour 2007-2008.

La Suède a recouvré **150 millions EUR** au moyen de 2 000 contrôles réalisés sur une période de quatre ans.

En Afrique du Sud, dans une seule affaire de fraude, des fonds totalisant **22 millions EUR** avaient été transférés à l'étranger.

En Norvège, le montant des ventes minorées a atteint **7 millions EUR** dans une seule affaire.

Des estimations des pertes dues à l'utilisation de techniques de suppression électronique des ventes ont été réalisées dans certains secteurs et certaines régions géographiques en particulier. Ces données donnent une indication des pertes possibles dans d'autres régions. On dispose à cet égard de statistiques utiles du Canada, qui reposent sur des données solides basées sur les cas de fraude détectés. Revenu Québec, l'autorité chargée de l'administration et de la collecte de l'impôt sur le revenu et des taxes à la consommation dans la province canadienne du Québec, a estimé que les pertes fiscales imputables à ces techniques s'élevaient à 417 millions CAD en 2007-2008.

En 2008, l'Agence du revenu du Canada a accusé les propriétaires de quatre restaurants de fraude fiscale impliquant le « camouflage » d'environ 200 000 transactions en espèces pour un total de 4.6 millions CAD. L'Association canadienne des restaurateurs et des services alimentaires cite l'estimation selon laquelle les ventes « fantômes » en espèces pourraient atteindre 2.4 milliards CAD en 2009.

En Allemagne, la Bundesrechnungshof (Cour des comptes fédérale) s'inquiète dans son « Rapport annuel 2003 sur la gestion financière fédérale » des pertes dues à l'utilisation de techniques de suppression électronique des ventes et déclare en conclusion que « le montant des transactions en espèces atteignant des dizaines de milliards d'euros, le risque de fraude fiscale ne doit pas être sous-estimé ».[5]

Les données suivantes valent également d'être mentionnées :

- dans une affaire ayant donné lieu à une enquête en Norvège, le montant des transactions non déclarées s'élevait à 7 millions EUR ;
- dans une affaire en Afrique du Sud, des grossistes avaient transféré à l'étranger une somme équivalente à 22 millions EUR ;
- dans une enquête menée en Slovénie, les inspections effectuées chez des détaillants après les heures d'ouverture ont permis d'établir que les ventes enregistrées dans les systèmes informatiques étaient trois fois supérieures à celles déclarées les autres jours.

L'administration suédoise a étudié ce problème dans le cadre d'une évaluation du manque à gagner fiscal au niveau national. Elle estime à 100 milliards EUR le chiffre d'affaires correspondant à la totalité des transactions en espèces en Suède. Le manque à gagner en relation avec ces transactions atteindrait 2 milliards EUR par an, soit environ un sixième du total du manque à gagner pour l'administration fiscale en Suède.

De 2006 à 2010, la Suède a réalisé environ 2 000 contrôles fiscaux de restaurants, de salons de coiffure, de boutiques d'habillement et de magasins d'alimentation, etc. Le montant des sommes non versées par les entreprises contrôlées, notamment au titre de l'impôt sur les bénéfices, de la TVA et des charges sociales, avoisinait 150 millions EUR. Ces contrôles ont montré que ces entreprises minoraient 20 à 40 % de leur chiffre d'affaires. Les ventes non déclarées alimentent l'économie clandestine ou souterraine et profitent, dans certains cas, à la criminalité organisée.

Divers éléments indiquent que l'utilisation de Zappers et de Phantomware se répand dans le monde ; par conséquent, la menace pour les recettes fiscales ne cesse de grandir. Certains fournisseurs, par exemple ceux des logiciels PDV pour restaurants, commercialisent au niveau international leurs systèmes équipés de fonctions de suppression électronique des ventes. Quant aux perspectives d'avenir, les contrôleurs et enquêteurs qui travaillent dans ce domaine font état d'un développement constant et d'une sophistication croissante des techniques utilisées pour échapper à la détection.

On n'a pas encore pu établir que des entreprises utilisent des techniques similaires pour gonfler leurs chiffres de ventes, par exemple dans le but de blanchir des produits du crime. Néanmoins, ce risque existe et les administrations fiscales doivent en être conscientes.

Notes

1. Le groupe d'experts était coordonné par la Norvège et comprenait des participants des pays suivants : Allemagne, Belgique, Canada, États-Unis, France, Grèce, Irlande, Norvège, Pays-Bas, Portugal, Royaume-Uni, Suède et Turquie.

2. Le Groupe de projet était chargé d'identifier les risques liés aux caisses enregistreuses et aux systèmes PDV et de faire des propositions sur les moyens de prévenir ces risques. Ses objectifs détaillés étaient les suivants :
   - recueillir des informations sur les différentes règles et normes requises par les autorités fiscales des États membres de l'UE au sujet des caisses enregistreuses et des systèmes PDV, ainsi que sur leur application en pratique, et inventorier les règles et conditions imposées aux fabricants de matériels et logiciels de caisses enregistreuses ;
   - recueillir, échanger et améliorer les connaissances et pratiques relatives aux caractéristiques techniques des caisses enregistreuses et des systèmes PDV ;
   - mettre au point différents concepts et confronter les expériences en vue d'améliorer l'utilisation des données sur les transactions commerciales dans les contrôles fiscaux ; et
   - recueillir des informations sur les formes d'utilisation abusive dont peuvent faire l'objet différents systèmes.

3. *Cash Register Good Practice Guide*, EU Fiscalis Project Group 12, 2006 (non accessible au public).

4. *Guidance and Specifications for Tax Compliance of Business and Accounting Software*, Forum sur l'administration de l'impôt, OCDE, avril 2010.

5. Circulaire 15/2020 du Parlement fédéral, p. 197-198 (24 novembre 2003).

Systèmes de terminaux point de vente

Systèmes PDV

Lorsque James Ritty a inventé la première caisse enregistreuse en 1879, son but était de créer un système d'enregistrement des transactions en espèces pour empêcher les employés de son saloon de dérober une partie de ses bénéfices. L'un de ses premiers modèles était présenté dans la publicité comme un « caissier incorruptible ». La caisse enregistreuse est rapidement devenue un outil essentiel de gestion des fonds d'une entreprise. L'enregistrement exact des opérations de vente et la préservation des pièces à l'appui de chaque transaction demeurent une fonction essentielle des caisses enregistreuses pour les entreprises. Ces caisses produisent des reçus qui attestent la réalité de la vente de l'entreprise à ses clients. Le ticket de caisse est le premier document ou relevé qui montre le contenu d'une transaction. Avec le temps, les caisses enregistreuses ont évolué, et elles ne se limitent plus à documenter des ventes mais englobent des fonctions comptables et d'audit.

Cette évolution s'est poursuivie et, aujourd'hui, les entreprises emploient des systèmes PDV modernes pour diverses raisons. Ceux-ci leur assurent sécurité et contrôle des espèces, sont rapides, réduisent les erreurs de transaction, facilitent la conservation des documents et les déclarations, permettent le contrôle des stocks et la surveillance du personnel, produisent des reçus et donnent d'une manière générale une image de professionnalisme aux entreprises.

Dans le secteur de la vente au détail et dans l'hôtellerie, les caisses enregistreuses jouent un rôle important dans la gestion de l'entreprise. La saisie d'une commande ou d'une transaction avec un client déclenche automatiquement d'autres actions, par exemple dans un restaurant où la commande d'un repas par un client est communiquée automatiquement aux cuisines, tandis que la prise en charge du client est confiée à un serveur en particulier. Du point de vue de l'intégration générale des opérations de l'entreprise, le système PDV ne constitue qu'un sous-système parmi beaucoup d'autres, mais c'est lui qui initie la transaction commerciale et qui transmet l'information à d'autres processus, et les caisses enregistreuses communiquent avec les systèmes logistiques, les systèmes comptables et d'autres systèmes de l'entreprise.

Les systèmes PDV ont des fonctionnalités plus ou moins complexes, parfois très simples ou extrêmement sophistiquées. Toutes les fonctions offertes par le fournisseur ne sont pas toujours activées dans le système qui est livré et installé chez un usager en particulier. Les systèmes milieu ou haut de gamme comportent souvent des tablettes ou des écrans tactiles et peuvent être reliés en réseau à des ordinateurs et connectés à des systèmes de lecture optique. La sophistication et la diversité de ces systèmes peuvent constituer un défi pour les contrôleurs fiscaux, qui doivent apprendre à mener des vérifications efficaces.

Contrôle des systèmes PDV : le cadre juridique

Il est essentiel que le cadre juridique dans lequel s'exercent les contrôles tienne compte de la nécessité de procéder à la vérification des systèmes numériques des entreprises et, en particulier, des terminaux PDV. La plupart des pays ont adopté une législation exigeant des entreprises qu'elles mettent en place des systèmes d'information et de comptabilité adéquats. Les chefs d'entreprises, cependant, sont libres de choisir en toute indépendance les systèmes conformes à ces principes. Voici quelques éléments communs à ce type de législation ou de réglementation :

- l'obligation de conserver pendant une certaine durée les données générées par les systèmes d'information et les systèmes comptables de l'entreprise qui sont pertinentes d'un point de vue fiscal ;
- la responsabilité du propriétaire de l'entreprise d'assurer que la comptabilité est tenue sous une forme qui en permet la vérification dans un délai raisonnable ;
- l'autorisation de convertir sur papier les données traitées électroniquement, à condition que cette conversion ne nuise pas à la réalisation d'une vérification.

Un certain nombre de pays ont adopté une réglementation spécifique sur les normes comptables applicables aux entreprises qui effectuent des transactions en espèces et cette réglementation prend en compte l'utilisation des systèmes PDV. Elle précise dans certains cas les rapports à établir, leur format, leur langue et leur durée de conservation. C'est l'approche suivie par la Norvège.

Dans un autre groupe de pays, l'utilisation de systèmes PDV certifiés spécifiques est imposée à l'ensemble des entreprises ou seulement à certains secteurs de services ou de la vente au détail. Ces systèmes, appelés « caisses enregistreuses sécurisées », sont décrits plus loin dans le chapitre « Réponses des pouvoirs publics ».

Obligations à respecter en vue des contrôles fiscaux

Les exigences relatives aux contrôles fiscaux sont parfaitement compatibles avec les besoins normaux d'une entreprise en termes de gestion de l'information commerciale. Outre les éléments mentionnés ci-dessus, les exigences spécifiques aux fins des contrôles fiscaux comprennent :

- la conservation électronique de données détaillées sur les transactions ;
- la tenue de registres comptables détaillés pouvant être mis, sur demande, à la disposition des contrôleurs des impôts ;
- la conservation de pistes complètes pour la vérification ; et
- l'adoption de mesures adéquates pour empêcher toute altération ultérieure des données et garantir leur intégrité.

Des données détaillées sur les transactions commerciales sont nécessaires pour vérifier que la totalité des ventes ont bien été déclarées. Du point de vue des contrôles, les exigences auxquelles les informations commerciales doivent répondre sont assez simples : les données archivées doivent donner une image exacte et complète des ventes. Ces registres doivent permettre aux contrôleurs des impôts de vérifier dans un délai raisonnable que les chiffres présentés sont le reflet exact et complet des ventes. Les données doivent donner une image vérifiable, complète et juste des ventes.

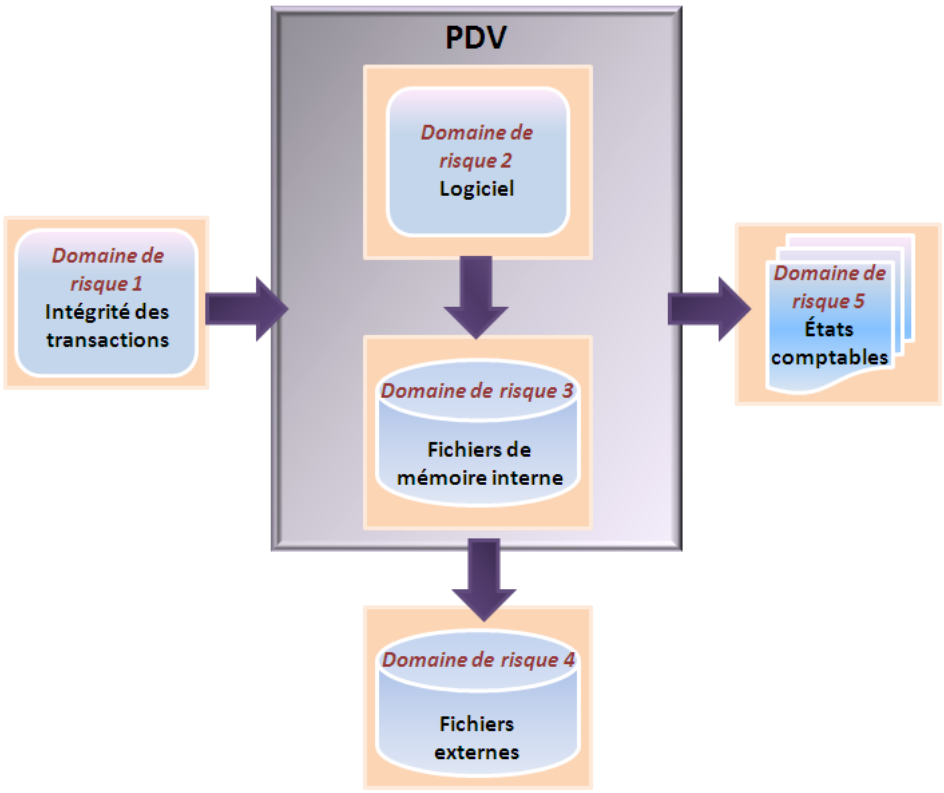
Ces exigences sont conformes aux besoins généraux de toute entreprise au regard des technologies utilisées à l'appui de ses systèmes commerciaux : dès l'enregistrement d'une transaction, une entreprise doit avoir la garantie que l'information correspondante est correctement conservée. Il faut également que ces transactions soient répercutées de façon fiable et complète dans les états comptables pouvant être générés à tout moment, au moins jusqu'au rapprochement des comptes.

Les grandes entreprises prennent des mesures adéquates pour conserver en toute sécurité les données essentielles aux activités commerciales. Leurs dirigeants doivent, en effet, garder une parfaite maîtrise de l'activité. Ils ont besoin de ces données pour appuyer leurs décisions de rentabilité à long terme, mais aussi pour remettre des états financiers et des bilans comptables fiables à leurs actionnaires et aux autorités de tutelle.

Risques liés aux systèmes PDV

Examinons maintenant les vulnérabilités liées aux techniques de suppression électronique des ventes dans certains domaines de risque spécifiques découlant de la configuration des systèmes PDV. Dans chacun de ces domaines de risque, la possibilité existe de supprimer ou de modifier des données sur les ventes, ou encore de ne pas enregistrer des transactions ayant bien eu lieu. Le diagramme ci-dessous[1] montre quels sont les cinq domaines de risque.

Graphique 1. Typologie des risques liés aux systèmes de terminaux point de vente



Source : Informations fournies par les Pays-Bas

Intégrité des transactions. Pour garantir l'intégrité des transactions, la caisse enregistreuse doit contenir un dispositif assurant que les données de chaque transaction sont complètes, exactes et saisies en temps voulu. À défaut, le système génère une information commerciale qui n'est pas fiable, avec tous les risques que cela peut entraîner du point de vue de l'aptitude à prendre des décisions de gestion judicieuses et à produire des déclarations fiscales exactes.

Logiciel. Le logiciel utilisé par l'entreprise doit être conçu de manière à assurer l'intégrité, la confidentialité et l'accessibilité des données traitées par le système de caisses enregistreuses. Si le système ne peut garantir l'intégrité, la confidentialité et l'accessibilité de ces données, il risque encore une fois de produire une information commerciale non fiable, avec toutes les conséquences négatives qui en résultent sur les décisions de gestion et le calcul de l'impôt. Il faut faire en sorte que le logiciel conserve en mémoire toutes les opérations effectuées sur la caisse enregistreuse, en créant des pistes claires pour la vérification. C'est une condition nécessaire à l'efficacité de la gestion et du contrôle de l'ensemble du processus.

Mémoire interne. Les données de transaction archivées en mémoire et dans les fichiers internes constituent la base de tous les rapports établis par l'entreprise et entrent dans le champ des examens menés en cas de contrôle ou d'enquête. C'est à ce niveau qu'existe le risque le plus aigu d'utilisation de logiciels de suppression électronique des ventes (ou d'autres méthodes de manipulation des fichiers) pour falsifier les données relatives aux transactions.

Fichiers externes. Le risque concerne le transfert et le stockage des données de transaction dans des fichiers hors ligne, qui sont nécessaires par exemple lorsque la mémoire du journal électronique d'une caisse ECR est pleine. En général, la législation exige des entreprises qu'elles conservent pendant une certaine période des livres et états comptables adéquats, y compris les supports de données sur lesquels ils sont enregistrés. Aux termes de certaines lois, les livres et états comptables doivent être organisés de manière à permettre aux contrôleurs des impôts de les examiner dans un délai raisonnable. Les fichiers externes comprennent aussi parfois les fichiers transférés quotidiennement du système PDV au service administratif sur un ordinateur séparé. Ils peuvent inclure également les fichiers de sauvegarde du système PDV, qui peuvent être conservés soit sur un support externe, soit sur le disque dur du système lui-même mais dans un dossier différent. Les fichiers de sauvegarde contiennent parfois des informations essentielles pour détecter l'utilisation d'un logiciel de suppression électronique des ventes dans un système de caisses enregistreuses.

États comptables. Il existe un lien étroit entre ce domaine de risque et le deuxième mentionné plus haut, celui du logiciel, car celui-ci régit l'établissement des états financiers, ouvrant des possibilités de manipulation au niveau de la conception et de la production de ces états. Les états comptables sont importants pour la gestion de l'entreprise et servent à transmettre des informations à la comptabilité générale, à établir les déclarations fiscales, etc. En cas de perte de données, il est très important pour le propriétaire de l'entreprise de pouvoir s'appuyer sur des copies papier des états qui recensent l'ensemble des données de transaction saisies et conservées dans les caisses enregistreuses.

Notes

1. Aux Pays-Bas, les fournisseurs de systèmes PDV ont établi, conjointement avec l'administration des impôts, une typologie des risques liés aux systèmes PDV, afin d'améliorer la discipline fiscale. Ce travail faisait partie du projet néerlandais d'un « Label de qualité pour la fiabilité des systèmes PDV », qui est décrit dans le chapitre « Réponses des pouvoirs publics ». Le groupe d'experts de l'OCDE sur la suppression électronique des ventes a adapté la typologie néerlandaise de façon à établir une typologie générale pour l'analyse des risques liés aux systèmes PDV.

Techniques de suppression électronique des ventes

Le problème que posent les techniques de suppression électronique des ventes est l'ampleur de la fraude fiscale qu'elles rendent possible en minorant les ventes et les bénéfices. Ce chapitre décrit comment certaines méthodes simples de fraude, qui sont toujours d'actualité, ont été automatisées et intégrées aux systèmes PDV.

La suppression des ventes, que l'on appelle aussi « écrémage », a toujours existé sous une forme ou une autre, notamment à des fins de fraude fiscale. Il existe plusieurs méthodes simples d'écrémage, par exemple :

- ne pas enregistrer certaines ventes en espèces dans la caisse enregistreuse, le propriétaire de l'entreprise conservant le produit de ces transactions ; ou
- détourner certaines ventes vers une seconde caisse enregistreuse « occulte ».

Ces pratiques sont particulièrement fréquentes dans les entreprises petites et moyennes, où les contrôles internes sont généralement moins nombreux et qui comptent souvent un nombre restreint d'actionnaires. Dans certains cas, l'entreprise qui pratique l'écrémage tient deux séries de livres et d'états comptables, la première pour l'administration fiscale et la seconde pour le propriétaire de l'entreprise, afin qu'il puisse faire état du chiffre d'affaires réel en cas de revente de l'entreprise. Ainsi, l'écrémage pratiqué en fermant les caisses enregistreuses à une certaine heure de la soirée dans une affaire de fraude à grande échelle concernant un restaurant en Australie s'est soldé par un rappel d'impôts de 8.4 millions AUD, taxes impayées et pénalités incluses, à la charge des propriétaires de l'entreprise.

Les technologies commerciales modernes ont permis d'automatiser ce type de fraude à l'aide de logiciels de suppression électronique des ventes comme « Phantomware » (logiciel installé à l'intérieur du système PDV) ou « Zappers » (programmes externes souvent transportés au moyen d'une clé USB). Ces logiciels donnent désormais la possibilité de pratiquer l'écrémage dans un environnement entièrement informatisé, en permettant au propriétaire de l'entreprise d'opérer d'une manière en apparence parfaitement normale (toutes les ventes étant enregistrées par le personnel dans une caisse enregistreuse en tant que transactions de vente). Grâce aux nouvelles technologies, le propriétaire de l'entreprise peut réaliser la suppression électronique des ventes à un moment adéquat, généralement après les heures d'ouverture, en optant pour une valeur monétaire préétablie chaque jour ou un simple pourcentage des ventes en espèces. Il n'est plus nécessaire de tenir une « deuxième caisse » ; tout le processus est informatisé et le propriétaire de l'entreprise a accès au logiciel de suppression à l'aide de méthodes assez simples, par exemple une carte magnétique ou un bouton caché sur l'écran permettant d'activer un menu spécial. Selon certains enquêteurs, l'accès au menu spécial peut aussi se faire en pressant plusieurs touches à la fois.

L'existence de nombreuses transactions en espèces était autrefois une condition essentielle des différentes formes d'écrémage. Les ventes par cartes de crédit ou de débit étaient rarement la cible de l'écrémage à cause des pistesque laissaient ces types de transactions pour la vérification . Néanmoins, on observe depuis peu aussi des signes de

suppression des ventes réalisées par cartes de crédit ou de débit. Plusieurs pays ont lancé des enquêtes à ce sujet pour déterminer s'il s'agit d'une nouvelle tendance et trouver des parades. Ce travail n'est pas suffisamment avancé pour qu'il soit possible d'en faire état ici.

En ce qui concerne le coût des logiciels Phantomware et Zappers, certaines informations provenant du Canada et des États-Unis montrent qu'il peut soit être inclus dans le coût du système PDV, en particulier dans le cas de Phantomware, soit atteindre environ 1 500 CAD en sus du coût du système PDV, comme dans le cas d'un logiciel Zapper.

Détournement de fonctions des logiciels ECR ou PDV

Les systèmes PDV modernes comprennent de nombreuses options de programmation, dont certaines peuvent être utilisées à des fins de suppression des ventes. Un terminal PDV peut, par exemple, être programmé pour :

- empêcher certains éléments comme les remboursements, les annulations de vente ou d'autres transactions négatives d'apparaître sur le journal ou le relevé ;
- empêcher certains éléments comme les remboursements, les annulations de vente ou d'autres transactions négatives d'être inclus dans les totaux généraux ;
- appliquer le mode formation à l'ensemble du système ou à une seule caisse, afin que les transactions correspondantes ne soient pas enregistrées dans les relevés normaux ;
- remettre les totaux généraux et d'autres compteurs à zéro ou, parfois, les faire repartir d'un chiffre sélectionné ; et
- spécifier que certains produits ne doivent pas apparaître sur le journal ou le relevé.

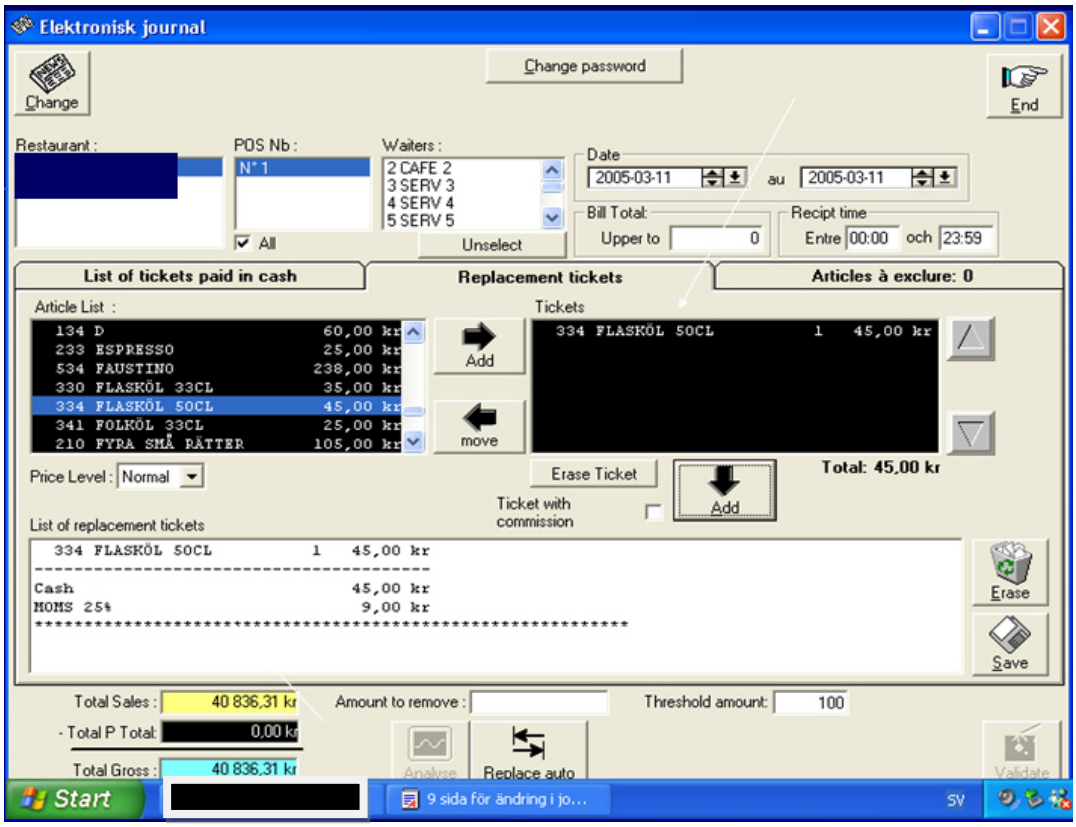
Les options de programmation permettant ces choix ne sont pas dissimulées dans le menu du programme (contrairement à Phantomware) mais sont décrites dans le manuel de programmation ou le manuel des fournisseurs ; ces manuels, cependant, ne sont pas normalement fournis aux acheteurs et sont généralement accessibles uniquement aux revendeurs agréés. Dans la majorité des caisses enregistreuses, la programmation s'effectue à l'aide de codes, ce qui nécessite certaines connaissances techniques de la part du programmeur. La plupart des systèmes PDV informatiques contiennent des options similaires mais le propriétaire de l'entreprise n'a pas besoin d'autant de connaissances techniques pour les utiliser.

Phantomware

Phantomware est un programme logiciel déjà installé ou intégré au logiciel d'application comptable d'une caisse ECR ou d'un système PDV informatisé. Invisible pour les usagers non informés, on peut y accéder en actionnant sur l'écran un bouton dissimulé, en effectuant une série de commandes ou en pressant plusieurs touches à la fois. Cela active un menu d'options permettant de supprimer sélectivement des transactions de vente et/ou d'imprimer des états des ventes où certaines lignes n'apparaissent pas. En cas de suppression de ventes, le dispositif adapte automatiquement les données d'inventaire pour éviter tout décalage apparent ; avec l'option d'effacement de lignes, seul l'état des ventes est modifié. Lorsque des changements comptables sont effectués, le logiciel peut aussi imprimer un journal des transactions supprimées, afin que

le propriétaire de l'entreprise puisse gérer (et suivre) les modifications. Ce mode opératoire est illustré par un programme utilisé dans le secteur de la restauration en Suède afin de recueillir les données du système PDV informatisé et les sauvegarder dans un journal électronique. L'écran du système reproduit ci-dessous montre combien il est facile de déplacer des transactions, nommément à partir des rubriques « List of tickets paid in cash » (Liste des ventes réglées en espèces) et « Replacement tickets » (Tickets de remplacement).

Graphique 2. Exemple de Phantomware



Source : Informations fournies par la Suède

Dans cet exemple de Phantomware, les ventes ne sont en fait pas supprimées mais modifiées en remplaçant des plats plus chers par des plats moins chers. Cette méthode de suppression électronique des ventes est plus sophistiquée parce qu'elle permet d'éviter les écarts qui résultent des suppressions dans la numérotation séquentielle des transactions de ventes. Les contrôleurs doivent savoir qu'avec d'autres versions de Phantomware, il est possible de supprimer des ventes en renumérotant les transactions conservées sans rompre l'ordre séquentiel des numéros de transaction. Par conséquent, l'existence d'une numérotation séquentielle n'exclut pas l'utilisation de techniques de suppression des ventes.

Zappers

Les Zappers (« camoufleurs de ventes ») sont des programmes logiciels externes utilisés pour supprimer des ventes. Ils sont logés sur divers supports électroniques, tels que

clés USB ou CD amovibles, ou peuvent être activés en ligne via un lien Internet. Les Zappers sont conçus, vendus et gérés par des concepteurs de systèmes PDV destinés à différents secteurs d'activité, mais certains acteurs indépendants ont aussi développé des techniques de ce genre. Leur fonctionnement est similaire à celui des logiciels Phantomware mais ils sont plus difficiles à détecter du fait d'une conception plus complexe, et aussi parce que le logiciel fautif n'est pas présent dans la machine pendant l'utilisation normale. Divers types de Zappers ont été détectés au Canada, en particulier dans un grand nombre de restaurants. À chaque fois, une clé USB est utilisée pour activer le Zapper en affichant sur le système PDV un écran spécial qui permet au propriétaire de l'entreprise de commencer à supprimer et/ou modifier les ventes.

Résumé des techniques utilisées

Quel que soit le type de programme utilisé, les éléments recueillis à ce jour semblent indiquer que, dans la plupart des cas, le fournisseur du système PDV l'a programmé de façon à permettre un usage frauduleux. Il peut aussi organiser une formation correspondante ou fournir un mode d'emploi écrit. Ces services sont parfois rendus sans entraîner de frais supplémentaires pour le client.

Dans le cas des logiciels Phantomware et Zappers, l'interface utilisateur est généralement de qualité professionnelle et simple d'emploi. Elle est souvent conçue par un technicien associé à la mise au point du logiciel d'exploitation du système PDV et son format est souvent similaire ; par conséquent, l'aspect et le mode de fonctionnement du logiciel de suppression sont les mêmes que ceux du logiciel commercial légal. La sélection des transactions à modifier est généralement simple à effectuer, le plus souvent en cliquant sur les ventes à supprimer ou à remplacer par une transaction de valeur moindre, ou en indiquant le montant ou le pourcentage des ventes à supprimer. Il existe aussi des filtres permettant à l'utilisateur de camoufler certaines catégories de ventes : un propriétaire d'entreprise qui emploie un personne non déclarée peut ainsi supprimer toutes les ventes de cet employé ou, en cas de vente de produits de contrebande (par exemple des cigarettes), le propriétaire peut faire disparaître les transactions correspondantes et effacer ainsi toute trace de participation à un trafic.

Les fonctions des systèmes de suppression électronique des ventes peuvent être résumées comme suit :

- accès au logiciel caché ;
- affichage du détail des transactions en espèces (mais on a aussi connaissance aujourd'hui de pratiques de suppression des transactions réglées par carte de crédit et de débit) ;
- suppression des ventes sélectionnées et des données d'inventaire correspondantes ;
- remplacement des ventes sélectionnées par des transactions de moindre valeur ;

sélection automatique des transactions à supprimer à hauteur d'un montant fixé à l'avance (pour dissimuler, par exemple, des retraits non déclarés de 1 000 EUR par jour de la caisse de l'entreprise en laissant le logiciel décider des ventes à supprimer) ;

- suppression du journal et d'autres traces des transactions ; et
- archivage des données originelles en un autre lieu.

On n'a pas encore établi à ce jour que des entreprises utilisent des techniques similaires pour gonfler leurs chiffres de ventes, par exemple pour blanchir des produits du crime. Néanmoins, ce risque existe et les administrations fiscales doivent en être conscientes.

Méthodes de détection

Audit financier

Les bonnes pratiques généralement reconnues en matière de vérification offrent des méthodes utiles pour déterminer si une entreprise pratique la suppression électronique des ventes.

Encadré 1. Méthodes de vérification

- Le **calcul des dépenses de consommation privée** permet de déterminer la quantité d'argent dont dispose un contribuable à des fins d'usage privé, sur la base de ses revenus, de ses dépenses en espèces et de l'évolution de ses actifs. Si la consommation privée apparaît très faible ou même négative, cela veut dire que la personne soupçonnée dépense plus d'argent que ce dont elle déclare disposer. Cela indique qu'elle perçoit sans doute de revenus non déclarés provenant de recettes supprimées. La méthode de l'avoir net et celle des espèces déposées sont également pertinentes à cet égard.
- Un **solde d'espèces négatif** signifie qu'un contribuable soupçonné a dépensé plus d'espèces tirées de la caisse enregistreuse qu'elle n'est censée en contenir. Il ne peut y avoir à cela qu'une explication : une source d'espèces dissimulée et non déclarée.
- La méthode des **bénéfices bruts** est utilisée pour analyser les ventes. Celles-ci sont d'abord évaluées en calculant les bénéfices théoriques sur la base des prix de vente affichés et des achats du contribuable. Les bénéfices bruts sont ensuite calculés à partir des chiffres (achats et ventes) enregistrés dans la comptabilité. Si les bénéfices bruts déclarés sont inférieurs aux bénéfices bruts théoriques, cela indique que toutes les ventes n'ont pas été enregistrées.
- Le **contrôle des quantités** est utilisé pour analyser les flux de marchandises. Il peut indiquer si une entreprise vend plus de marchandises qu'elle n'en a achetées et n'en conserve en stock et, par conséquent, que certaines ventes ne sont pas enregistrées. Cette méthode de contrôle est généralement appliquée en même temps que l'analyse des bénéfices bruts.
- **Flux de trésorerie / ventes nettes** : il s'agit du pourcentage des flux nets de trésorerie d'une entreprise par rapport à ses ventes nettes ou à ses recettes (d'après son compte de résultats). Plus le pourcentage est élevé, mieux cela vaut pour les entreprises où une grande part des transactions sont réglées en espèces ; un taux inférieur à celui que l'on pourrait attendre dans un secteur commercial particulier peut être un signe de minoration. On notera cependant que ce taux varie fortement selon les secteurs et aussi d'une entreprise à l'autre. Dans une affaire concernant le secteur de la restauration, le ratio de liquidités déclaré était conforme à la moyenne statistique nationale, alors qu'en réalité, lorsque les ventes supprimées ont été découvertes, le ratio réel s'est révélé être beaucoup plus élevé, dépassant même le niveau médian supérieur des statistiques publiques.
- Les administrations fiscales peuvent aussi recourir à des **opérations d'infiltration** pour observer le fonctionnement d'une entreprise. De telles opérations peuvent être source pour les contrôleurs des impôts d'informations utiles sur l'utilisation concrète d'un système PDV. Des agents d'une administration fiscale peuvent aussi se faire passer pour des utilisateurs potentiels afin d'acquérir des copies des logiciels pertinents à des fins d'analyse.

- Les **autres systèmes financiers et de gestion d'une entreprise**, comme le contrôle des stocks et la facturation, sont souvent étroitement liés au système de caisses enregistreuses. Lors d'une vérification, l'information obtenue à partir de ces systèmes peut être importante pour évaluer la fiabilité des données conservées dans les caisses enregistreuses.

Les contrôleurs des impôts peuvent apprendre à extraire des informations utiles d'un système PDV. Ils peuvent aussi apprendre à reprogrammer une caisse ECR afin de révéler les ventes et transactions supprimées et d'imprimer des états les faisant apparaître en détail. Cette approche a été adoptée au Royaume-Uni où les contrôleurs des impôts doivent suivre une formation de trois jours. Lors d'une intervention locale, 68 % des entreprises contrôlées ont fait l'objet de rappels d'impôts.

Contrôle numérique spécialisé

Les contrôleurs du commerce électronique ou contrôleurs numériques spécialisés sont également appelés « spécialistes de la vérification du commerce électronique » (SVCE). Les systèmes PDV contiennent souvent des milliers de transactions qu'il est impossible de contrôler sans des outils et techniques de vérification assistée par ordinateur (OTVAO) comme IDEA. Ce type d'outils permet au contrôleur d'importer des données à partir de pratiquement n'importe quel format ou fichier et de les soumettre à de nombreux types d'analyses, ainsi que d'établir des rapports et des graphiques (dont certains sont présentés plus loin). Il peut être utilisé à l'appui des audits internes normaux ou des analyses financières et pour identifier les transactions inhabituelles pouvant être signe de fraude ou de blanchiment d'argent. Les SVCE sont des vérificateurs qui reçoivent une formation spécialisée à l'utilisation des OTVAO. Étant donné le développement des systèmes PDV numériques dans nombre d'entreprises où les règlements se font en espèces, l'intervention des SVCE est nécessaire pour analyser et comprendre les systèmes complexes et recueillir les informations clés pertinentes à examiner à l'aide de logiciels d'audit tels que IDEA, ACL ou SESAM. La sélection des fichiers de données n'est pas une procédure simple, en particulier lorsqu'une entreprise utilise un système ECR ou un système hybride, par opposition aux systèmes PDV basés sur un ordinateur. De plus, les SVCE ont reçu la formation nécessaire pour analyser de manière approfondie les séries de données EPOS volumineuses et complexes et rechercher les indices de suppression électronique des ventes ou d'autres signes de non-respect de la réglementation. Les SVCE peuvent aussi échanger leurs résultats avec les autres membres de l'équipe d'audit et les comparer à d'autres informations recueillies par le contrôleur des impôts.

Expertise légale numérique

Les spécialistes de l'expertise légale numérique utilisent nombre des outils d'expertise dont se servent également les contrôleurs numériques spécialisés. Pour qu'une expertise légale soit valide, il est nécessaire que le système PDV ait été saisi pour analyse dans un laboratoire d'expertise légale ; autrement dit, de même que pour toute autre enquête criminelle, il est essentiel de sécuriser les preuves de l'infraction, y compris les instruments utilisés. Une fois qu'un système a été saisi, généralement sur la base d'un mandat de perquisition, il est reproduit à l'aide d'une procédure fréquemment décrite comme le « clonage » du disque dur d'origine ; les vérifications de l'expertise légale peuvent alors commencer.

Détection d'indices

Une liste détaillée des indices pouvant être identifiés par un contrôleur des impôts, un contrôleur numérique spécialisé ou un spécialiste de l'expertise légale numérique a été établie et est conservée de façon confidentielle par l'OCDE.

Techniques d'enquête criminelle

Dans les affaires de suppression électronique des ventes, le rôle de l'enquêteur criminel, comme dans toute autre forme de fraude fiscale, est de réaliser une investigation criminelle de la situation financière des sociétés et/ou individus soupçonnés de fraude fiscale dans un but de poursuites pénales.

Dans ce type d'affaires, l'enquêteur criminel s'appuie également sur les techniques d'enquête traditionnelles pour recueillir des éléments de preuve, au moyen notamment de mandats de perquisition délivrés par l'autorité judiciaire (pour la saisie des systèmes PDV, des données de sauvegarde PDV, de la correspondance électronique ou d'autres types de données électroniques), d'ordonnances de communication ou d'autres procédures administratives visant à obtenir l'accès à des informations financières, et aussi de l'interrogatoire de témoins potentiels dans les locaux de l'entreprise sous enquête ou de tierces parties comme, par exemple, les fabricants de systèmes PDV.

L'enquêteur criminel peut aussi recourir à des opérations d'infiltration ou réaliser, conjointement avec d'autres organismesrépressifs, des opérations visant les fabricants de systèmes PDV. Les opérations d'infiltration exigent un très haut degré de compétence et de planification. Elles sont parfois le moyen pour l'enquêteur de réunir les preuves directes d'un délit et des motifs raisonnables de requérir un mandat de perquisition. Les chances d'obtenir un aveu sont aussi plus grandes lorsque des preuves obtenues par des moyens discrets sont présentées à l'accusé. Dans une opération visant un concepteur de logiciels menée au Canada, les agents infiltrés se sont présentés comme de riches propriétaires de restaurants étrangers souhaitant ouvrir des restaurants à Vancouver. Dans cette opération, les agents ont négocié avec un concepteur de logiciels l'achat d'un Zapper et les éléments de preuve ainsi recueillis ont permis la délivrance d'un mandat pour la perquisition des locaux du concepteur.

Lorsque les éléments recueillis sont suffisants pour établir la culpabilité hors de tout doute raisonnable, l'affaire est transmise au procureur en vue d'une inculpation pour infraction fiscale et/ou d'autres délits. Le but des poursuites pénales, outre sanctionner les auteurs de l'infraction, est de dissuader d'autres personnes de commettre un délit similaire et de renforcer le respect de la législation en vigueur en faisant savoir que la fraude fiscale est un délit pénal donnant lieu à des poursuites publiques.

Recherche des traces d'utilisation des logiciels fautifs

Dans les cas d'utilisation de logiciels de suppression électronique des ventes, on peut supposer que les mesures prises pour réduire les rentrées en espèces vont aussi rendre difficile ou impossible d'établir les recettes véritables de l'entreprise au moyen d'une vérification des livres et registres comptables. C'est ce qui ressort clairement des enquêtes récentes sur le logiciel Phantomware, la conclusion étant que les enquêteurs sont en grande partie tributaires d'une expertise légale numérique pour établir les faits. Néanmoins, même en l'absence de moyens d'expertise légale numérique, ce qui est souvent le cas, les compétences numériques spécialisées des contrôleurs peuvent leur

permettre de trouver et de copier les fichiers de sauvegarde, ainsi que d'autres fichiers utiles.

Certaines affaires ayant eu lieu en Suède et en Norvège illustrent les modifications apportées au mode de fonctionnement des logiciels de suppression électronique des ventes afin de rendre la détection plus difficile. Les premières versions du programme Phantomware laissaient dans le système de gestion de l'entreprise de nombreuses traces des changements effectués, et des fichiers contenant les données originelles sur les ventes restaient présents dans le système. Les administrations fiscales parvenaient ainsi à détecter l'utilisation d'un logiciel de suppression électronique des ventes – mais le fabricant était, lui aussi, informé des résultats de ces enquêtes. Lors d'enquêtes ultérieures, il est apparu que le programme avait été modifié de manière à ne plus laisser de traces. Les versions les plus récentes du programme effacent la plupart des traces des ventes d'origine et sont dotées de fonctions visiblement destinées à empêcher la détection en cas d'examen numérique du système, comme la modification de l'horodatage des fichiers de données.

La compétence juridique et la capacité technique d'accéder au contenu des caisses enregistreuses et des ordinateurs sont décisives pour détecter l'utilisation de Phantomware ou d'un logiciel de suppression électronique des ventes. Même si un logiciel de suppression des ventes est capable de créer des preuves crédibles d'une baisse du chiffre d'affaires et de faire disparaître toute trace du chiffre d'affaires réel, il faut partir du principe que certaines traces électroniques subsistent à des niveaux sous-jacents, par exemple dans les systèmes d'exploitation et les systèmes de fichiers. Ces niveaux ne peuvent dans bien des cas être examinés qu'au moyen d'une expertise légale numérique.

L'utilisation de Zappers peut aussi laisser des traces dans les données des systèmes d'exploitation et des systèmes de fichiers. Contrairement à Phantomware, ces programmes sont retirés du système après utilisation et ne peuvent pas être analysés à partir du matériel auquel on a normalement accès dans une expertise légale numérique. Pour pouvoir analyser un Zapper, il faut le trouver et, le plus souvent, l'autorité juridique de saisir des objets personnels est nécessaire à cette fin.

Une expertise légale numérique s'appuie sur la collecte contrôlée et l'analyse de données. La collecte de données implique la saisie de copies vérifiables de sources de données se rapportant à une entreprise. L'analyse de données englobe les méthodes et mesures d'enquête utilisées pour interpréter l'information numérique saisie.

Saisie des sources numériques

La saisie de données doit viser avant tout le système PDV, mais d'autres sources d'information numérique d'une entreprise peuvent être pertinentes aux fins d'une enquête. Outre le système PDV, certains ordinateurs des systèmes de gestion et certains supports de stockage externes peuvent être impliqués dans l'utilisation de Zappers et de Phantomware. Si la saisie et l'examen de ce type de sources sont légalement autorisés, le défi est d'accéder à l'information afin de pouvoir la copier. En effet, le risque existe d'endommager ou de supprimer des données, ce qui peut avoir des conséquences graves pour l'entreprise visée par une enquête et réduire les chances d'établir son chiffre d'affaires réel. Ce risque peut être évité par la prudence et l'utilisation judicieuse des outils et techniques décrits ci-dessous.

Il existe en effet divers outils, matériels et logiciels permettant de recueillir les données. Il s'agit essentiellement d'outils visant à assurer que l'information numérique de l'entreprise n'est pas modifiée, et que la copie est fidèle à l'original.

Dans les cas où il faut sécuriser le contenu de systèmes propriétaires comme les caisses enregistreuses fonctionnant sur la base d'une mémoire ROM[1], il peut être nécessaire de réaliser des essais préliminaires sur un type de matériel identique avant de recueillir effectivement les données. Cela exige d'être bien renseigné sur les technologies utilisées par l'entreprise avant l'enquête fiscale.

Parmi les programmes permettant de recueillir l'information numérique, on peut citer les systèmes suivants :

- EnCase de Guidance Software, qui peut collecter des données à partir de divers supports de stockage et est fréquemment utilisé en conjonction avec un système hardware de protection d'écriture, afin de protéger l'intégrité des données originelles ;
- Forensic Toolkit Imager d'Access Data, qui peut aussi être utilisé avec un système hardware de protection d'écriture et recueillir des données sur un système opérationnel.

Il s'agit là seulement d'exemples actuels de ce type d'outils car les produits changent, mais leurs principes restent identiques. Dans certains cas, les outils susmentionnés ne sont pas en tant que tels suffisants et les compétences requises pour mener à bien la procédure d'expertise légale sont alors décisives. Le succès dépend donc en grande partie de la documentation existante. Les procédures doivent être appliquées en gardant à l'esprit le fait que chaque tâche doit pouvoir être vérifiée, et ensuite répliquée.

Analyse de l'information numérique

Les procédures d'analyse de l'information recueillie peuvent varier en fonction des besoins de l'affaire, de l'accès à l'expertise, des ressources disponibles et de la législation régissant ce type de travail. Il est donc difficile de donner une description générale de l'analyse à effectuer, mais un bon point de départ consiste sans doute à rechercher et à lire des saisies informatiques relatives aux ventes.

L'expertise légale doit commencer par passer en revue et évaluer la totalité des informations pertinentes aux fins du contrôle fiscal. Il peut s'agir d'informations archivées ou contenues dans le système d'exploitation, les logiciels ou divers autres fichiers. L'analyse doit chercher à établir les preuves de l'utilisation d'un logiciel de suppression électronique des ventes et à identifier le logiciel effectivement utilisé (Phantomware ou Zapper).

Les fichiers d'enregistrement des ventes doivent être confrontés aux données d'horodatage[2] figurant dans le système de stockage et/ou de fichiers. Si les ventes ont été modifiées à une date ou une heure où normalement aucune nouvelle écriture n'aurait dû être ajoutée, cela peut indiquer l'utilisation d'un logiciel de suppression électronique des ventes. Les fichiers journaux peuvent contenir des données supplémentaires confirmant les traces de suppression indiquées. L'information fournie par le système de fichiers est généralement une source fiable pour établir à quel moment un fichier a été créé, modifié ou utilisé pour la dernière fois. Il existe cependant d'autres sources comme le journal des logiciels de sécurité – par exemple les programmes anti-virus – qui peuvent garder trace du nom et de la taille des fichiers. La différence de taille entre les fichiers répertoriés dans

le programme antivirus et les fichiers du système saisi peut être la preuve que leur contenu a été modifié. L'analyse de ces fichiers vise principalement à déterminer si un logiciel de suppression électronique des ventes a été utilisé.

Les outils généralement utilisés pour l'analyse de l'information numérique comprennent notamment :

- EnCase de Guidance Software, un programme adapté à de nombreux systèmes de stockage différents et permettant l'analyse générale des données numériques collectées (*www.guidancesoftware.com/*) ;
- Forensic Toolkit d'Access Data, un programme adapté aux systèmes de stockage les plus courants qui simplifie la procédure de recherche grâce à l'indexation du contenu de l'information numérique recueillie (*www.accessdata.com/*) ;
- IDA de Hex-Rays, un programme s'adaptant à de nombreux systèmes pour décompiler les fichiers d'application (*www.hex-rays.com/idapro/*) ;
- Forensics WinHex de X-Ways Software Technology, un éditeur hexadécimal doté de nombreuses fonctions d'expertise légale (*www.x-ways.com/*).

Lorsque l'analyse numérique vise principalement à détecter la présence d'un logiciel de suppression électronique des ventes, elle doit se focaliser sur les fichiers programme et les entrées du système d'exploitation. Les modalités de ce type d'analyse sont variables et peuvent nécessiter diverses compétences. Une approche fréquemment utilisée et qui donne de bons résultats consiste à isoler et examiner les logiciels d'application des matériels saisis. À cette fin, on peut faire fonctionner le programme sur un autre ordinateur ou sur une *machine virtuelle*. Cette méthode a permis dans plusieurs cas de découvrir une fonctionnalité cachée. C'est aussi un bon moyen de détecter la capacité d'un programme à minorer le chiffre d'affaires (ventes) via l'utilisation d'autres fonctions non cachées. Il existe aussi une méthode plus complexe s'appuyant sur divers modes de décompilation des fichiers programme. Le contenu des fichiers programme, qui se compose principalement d'instructions à l'ordinateur, est alors traduit en un code de programmation lisible par l'enquêteur. Cette manière de procéder, qui demande beaucoup de temps, donne des résultats aléatoires. Une autre méthode parfois efficace consiste à extraire les boîtes de dialogue et les graphiques des fichiers programme. Ces éléments peuvent révéler une fonctionnalité cachée ou garder la trace de fonctions associées à la suppression des données de ventes.

Note

1. La mémoire morte (Read Only Memory, ROM) est la mémoire de l'ordinateur où sont stockées en permanence les données et les applications.
2. L'horodatage indique la date et l'heure effectives d'un événement, par exemple une transaction de vente enregistrée par un ordinateur.

Réponses des pouvoirs publics

Les logiciels de suppression électronique des ventes installés sur les terminaux PDV se développent depuis plusieurs années, et les pouvoirs publics comme les administrations fiscales prennent de plus en plus conscience du problème. Les travaux menés par le Groupe d'action sur les délits à caractère fiscal et autres délits contribuent à mieux sensibiliser les pays et incitent certains d'entre eux à agir. Une présentation effectuée lors du premier Forum sur la fiscalité et la criminalité à Oslo en mars 2011 a permis de porter les risques de nature fiscale à l'attention d'un large public issu d'administrations fiscales et d'autorités répressives.

Le Groupe d'action a recensé les réponses apportées par les pouvoirs publics dans un certain nombre de pays où les informations étaient disponibles. On a ainsi pu analyser l'efficacité de l'éventail des mesures prises afin de remédier au problème de la suppression électronique des ventes et aux risques engendrés par cette pratique.

Ces mesures relèvent des catégories suivantes :

- renforcer la discipline fiscale ;
- améliorer la sensibilisation ;
- détection, contrôle et enquête ;
- renseignements ; et
- caisses enregistreuses sécurisées et systèmes PDV certifiés.

La question de la suppression électronique des ventes est complexe et appelle une réponse qui englobe tout ou partie de ces catégories. C'est la raison pour laquelle il faut suivre une approche stratégique afin d'élaborer un ensemble approprié de solutions.

Approche stratégique

Certaines administrations fiscales inscrivent leurs travaux dans ce domaine dans le cadre d'une stratégie plus large visant à s'attaquer au manque à gagner fiscal ou à l'économie souterraine.

Pour élaborer une réponse stratégique à la suppression électronique des ventes, une administration fiscale doit identifier la nature des risques auxquels elle peut être exposée ; pour ce faire, elle peut s'appuyer sur les informations contenues dans ce rapport, ou se procurer des renseignements utiles auprès d'interlocuteurs expérimentés dans d'autres administrations fiscales qui sont plus avancées dans la lutte contre la suppression des ventes.

Les risques peuvent être évalués en menant des contrôles ciblant un éventail d'entreprises, à la fois celles qui présentent un facteur de risque connu et les autres. Cette approche a été suivie dans un certain nombre de pays et a permis de détecter des pratiques de suppression électronique des ventes dans les deux types de cas. La généralisation de ces contrôles peut contribuer à repérer les segments les secteurs de la distribution et des services qui présentent le plus de risques. Dans de nombreux pays, l'accent est mis sur les

restaurants, mais des risques élevés sont également apparus dans les chaînes de supérettes, les pharmacies, les salons de coiffure et d'autres prestataires de services.

Il est également utile de comprendre la nature du marché des terminaux point de vente, qui sont leurs fournisseurs, qu'ils soient à capitaux nationaux ou étrangers, ainsi que leurs parts de marché respectives.

Un certain nombre d'administrations fiscales ont clairement manifesté leur intention de s'attaquer aux logiciels de suppression électronique des ventes par des moyens législatifs. Les procureurs doivent pouvoir s'appuyer sur une législation qui incrimine la fourniture, la possession ou l'utilisation de tels logiciels car elle peut accélérer le processus souvent fastidieux de mise en cause des fournisseurs malhonnêtes et adresser un signal puissant aux fabricants. L'Irlande a récemment introduit une telle législation[1], et certains États américains font de même (dont la Floride, le Maine et New York).

Renforcer la discipline fiscale

Dans son rapport sur le suivi de la discipline fiscale[2], le Forum sur l'administration fiscale indique que « dans un monde idéal, l'ensemble des citoyens et des entreprises honorent leurs obligations fiscales, à savoir s'enregistrer là où cette formalité est prévue, déclarer spontanément leurs bénéfices et payer leur impôt en temps voulu, ceux-ci étant calculés en parfaite conformité avec la législation ». Le respect de ces obligations fondamentales par les contribuables peut aussi être apprécié sous l'angle de son caractère volontaire (*discipline volontaire*) ou contraint par des mesures de vérification/d'exécution prises par l'administration fiscale (*discipline imposée*). Dans le contexte d'une administration fiscale, cette distinction est très pertinente car la « discipline imposée » a un coût, souvent significatif.

Discipline volontaire

La note d'orientation de l'OCDE sur la tenue de registres[3] décrit les avantages de la discipline volontaire en ces termes :

« Imposer le respect de la législation par le biais de contrôles fréquents, de tests de corroboration et de poursuites constitue un moyen onéreux d'assurer le niveau de conformité voulu ; aussi, la plupart des administrations fiscales s'efforcent de promouvoir la discipline volontaire, par laquelle le contribuable est incité à coopérer et à se conformer activement à la réglementation fiscale. Cette stratégie réduit le coût d'administration du système fiscal, mais suppose que les exigences de ce système soient bien comprises, relativement simples à respecter et généralement acceptées par les entreprises ». « La discipline volontaire est favorisée… lorsque les obligations fiscales s'intègrent aux systèmes comptables et de tenue de registres de l'entreprise. À condition que ces systèmes soient fiables, les coûts de la conformité pour les entreprises et les administrations fiscales peuvent probablement être réduits au minimum. »

Dans un effort pour améliorer la « discipline fondée sur la coopération », la note d'orientation du Forum sur l'administration fiscale intitulée « Indications et spécifications relatives à la conformité fiscale des logiciels comptables et commerciaux » formule des recommandations à l'intention des administrations fiscales et des concepteurs de logiciels. Ces recommandations s'appliquent à tous les logiciels comptables et commerciaux, et englobent donc les caisses enregistreuses et les terminaux point de vente. Comme l'indique la note, chaque administration fiscale est confrontée à un environnement différent s'agissant de facteurs tels que le contexte politique, la

législation, les pratiques administratives ou la culture, et ces facteurs doivent être pris en compte dans l'élaboration des réponses.

De nombreuses administrations fiscales cherchent à établir des relations privilégiées basées sur la coopération avec les grandes entreprises. Ces relations supposent confiance mutuelle, transparence et compréhension. La connaissance des réalités de l'entreprise, l'impartialité, la proportionnalité, l'ouverture et la réactivité de la part des administrations fiscales, ainsi que la diffusion d'informations et la transparence de la part des contribuables sous-tendent ces relations. Obtenir des réponses sûres et en temps voulu sur des questions fiscales est l'un des avantages pour les entreprises qui acceptent de s'engager dans ces relations. Lorsqu'elle noue une relation privilégiée avec une grande entreprise, l'administration fiscale examine le cadre de contrôle interne qu'elle a mise en place. Le logiciel comptable (ce qui inclut les caisses enregistreuses électroniques et les terminaux point de vente) fait partie de ce cadre de contrôle interne. S'agissant des petites et moyennes entreprises, l'administration fiscale cherchera souvent à impliquer les secteurs d'activité concernés et leurs organisations représentatives dans les discussions sur la discipline volontaire, et s'efforcera de fournir des réponses sûres et en temps voulu sur des questions fiscales. On peut citer en exemples le Canada et les Pays-Bas, dont les administrations fiscales ont associé le secteur de la restauration aux discussions sur la discipline fiscale.

Les concepteurs de logiciels et fournisseurs de caisses enregistreuses électroniques constituent une catégorie très importante de parties prenantes. Diverses administrations fiscales examinent la possibilité de renforcer leurs relations avec les concepteurs et fournisseurs de terminaux PDV. L'objectif est de créer un environnement dans lequel la grande majorité des caisses seraient exemptes de toute utilisation de technique de suppression des ventes. Les administrations fiscales s'efforcent de nouer des relations de coopération avec ces parties prenantes pour les inciter à renoncer aux logiciels de suppression des ventes. Par conséquent, il importe non seulement d'influencer le comportement des contribuables, mais aussi celui des concepteurs de logiciels et de leurs fournisseurs ; cette approche est probablement plus efficace si elle est collective et proactive et non pas fondée sur des contrôles individuels. Il est important de définir des normes concernant les caisses enregistreuses électroniques et d'obtenir l'engagement des concepteurs et des distributeurs de les respecter.

L'administration fiscale irlandaise a donné un bon exemple de cette approche. Elle a lancé une campagne en faveur de la discipline volontaire concernant l'utilisation des systèmes de caisse enregistreuse, axée sur trois principales parties prenantes : les propriétaires des entreprises (utilisateurs finals), les fournisseurs du matériel et/ou du logiciel ; et leurs organisations représentatives. Toutes ont reçu une lettre accompagnée d'une nouvelle brochure sur le sujet publiée par les autorités fiscales irlandaises. Cette brochure explique clairement ce qui est attendu de la part de chacune des parties prenantes afin de respecter la réglementation sur la TVA de 2008, et notamment en quoi l'obligation de tenue de registres s'applique à l'utilisation de caisses enregistreuses. Ces informations figurent également sur le site Internet de l'administration fiscale irlandaise, à l'adresse : *www.revenue.ie/en/tax/vat/leaflets/cash-registers.html*.

Label de qualité

Dans le cadre d'une approche novatrice de la discipline volontaire menée par l'administration fiscale néerlandaise, un organisme sectoriel a été mis en place, avec pour mission de certifier la qualité des terminaux point de vente commercialisés aux Pays-Bas. Ce système de label de qualité[4], unique en son genre, pourrait toutefois être adapté à

d'autres pays. Une fois le processus entièrement opérationnel, il serait utile d'examiner les possibilités de lui conférer une portée internationale. Il faudrait élaborer des normes spécifiques aux terminaux PDV qui soient applicables à l'échelle internationale, ce qui pourrait procurer des avantages substantiels : réduction considérable du marché des logiciels de suppression électronique des ventes, certitude des administrations fiscales, des concepteurs de logiciels et de leurs utilisateurs quant à la conformité des systèmes PDV, et réduction des coûts de conformité pour tous.

L'administration fiscale néerlandaise et les fabricants participent à ce projet sur une base volontaire. Le projet est désormais opérationnel et bénéficie du soutien de nombreux fabricants ; l'entité chargée de décerner le label de qualité fonctionne en toute indépendance. L'idée est que les systèmes de caisses enregistreuses conformes à la norme obtiennent un label de qualité. L'organisme responsable définit les normes auxquelles un système fiable doit satisfaire et vérifie que les fabricants respectent ces normes (et utilisent correctement le label de qualité).

Graphique 3. Label de qualité mis en place aux Pays-Bas

Source : *www.keurmerkafrekensystemen.nl*

Dans le cadre de son système de gestion des risques, l'administration fiscale néerlandaise tiendra compte du fait que les systèmes bénéficiant du label de qualité présentent un moindre risque de fraude.

Améliorer la sensibilisation

Sensibiliser davantage à l'impact de la suppression électronique des ventes, en suivant une démarche planifiée et progressive, peut procurer des avantages. Parfois, les efforts de sensibilisation peuvent être facilités, voire même initiés, par les médias et par des journalistes d'investigation, comme cela s'est produit au Canada, aux Pays-Bas et en Norvège.

Les administrations fiscales peuvent envisager d'engager un dialogue avec les principales parties prenantes, comme les fabricants, fournisseurs et représentants des entreprises. Par ce dialogue, elles peuvent s'assurer que les parties prenantes comprennent :

- comment la législation s'applique au matériel et au logiciel qu'elles utilisent ;
- le comportement que les pouvoirs publics attendent d'elles en la matière ;
- comment elles peuvent se conformer aux obligations juridiques ; et
- les conséquences possibles en cas d'infraction.

Si les efforts de sensibilisation visent avant tout l'utilisateur final, le dialogue peut porter sur les points suivants :

- les obligations comptables et juridiques en matière de tenue de livres et de registres ;

- l'utilisation de systèmes de caisse enregistreuse et son respect de la législation ; et
- les avantages de la conformité pour les deux parties (situation gagnant-gagnant) : les entrepreneurs reçoivent des informations à jour sur les questions fiscales et les autorités fiscales connaissent les systèmes utilisés et savent que le contribuable est à « moindre » risque (elles peuvent ainsi axer leurs contrôles en priorité sur les contribuables présentant des risques plus élevés).

Les outils de communication utilisés dans cette approche peuvent être des brochures expliquant l'utilisation des systèmes de caisse enregistreuse, des pages spécifiques sur le site Internet officiel de l'administration fiscale, et des campagnes de sensibilisation plus ciblées.

Si l'accent est mis sur les fournisseurs, la communication peut privilégier les aspects suivants :

- les dispositions juridiques et comptables applicables au développement, à l'installation et à l'utilisation de systèmes de caisse enregistreuse ;
- les obligations particulières auxquelles le système de caisse enregistreuse doit se conformer ; et
- les avantages de la conformité pour toutes les parties concernées (situation gagnant-gagnant) : par exemple, les développeurs/fournisseurs peuvent se livrer concurrence sur un pied d'égalité, tandis que leur comportement vertueux procure à l'administration fiscale une certaine assurance (réduction des risques, affectation des moyens de contrôle aux contribuables présentant des risques plus élevés).

Les principaux outils de communication sont les réunions avec les organes représentatifs et les rencontres individuelles avec les fournisseurs.

Il est aussi possible d'axer les efforts de sensibilisation sur les contribuables en général en utilisant les médias pour faire connaître les condamnations prononcées à l'encontre de fraudeurs, favorisant ainsi la discipline volontaire. Au Canada, la publication dans les médias de poursuites ayant abouti est à la base du succès du Programme d'enquêtes criminelles. Dans certains cas, notamment ceux impliquant un camoufleur de ventes, l'intervention des médias peut être sollicitée au moment de l'exécution du mandat de perquisition et pendant les enquêtes pénales. La divulgation des poursuites et des condamnations fait partie intégrante du système d'autoévaluation et dissuade les fraudeurs potentiels. Le graphique 4 illustre la couverture médiatique dans une affaire de fraude. Le journal télévisé de fin de soirée a rendu compte de cette affaire.

Graphique 4. Camoufleurs de ventes – Couverture médiaque

Source : The Province, « Tax – Cheating software bust – Something's fishy at these restaurants (… and it's not the sushi) », page de couverture, The Province, 11 décembre 2008.

Contrôle et enquête

Les administrations fiscales ne se contentent pas de mener des vérifications individuelles ; elles lancent également des campagnes visant à déceler les cas de suppression électronique des ventes. Différents facteurs interviennent pour sélectionner les cas à examiner. Les logiciels d'analyse des risques (comme le logiciel IDEA décrit plus avant) jouent un rôle important, tout comme la connaissance des entreprises et des secteurs caractérisés par une circulation importante d'espèces. Divers signaux alertant l'administration fiscale peuvent

conduire à la découverte de logiciels et de techniques de suppression électronique des ventes et permettre de démasquer leurs fournisseurs.

En menant des contrôles et des enquêtes visant les fournisseurs de systèmes suspectés d'utiliser des techniques de suppression électronique des ventes, il est possible de se procurer des listes de clients et d'identifier les utilisateurs du logiciel. Ces informations peuvent servir à élaborer des programmes de contrôle portant sur des types spécifiques de caisses enregistreuses électroniques. Elles peuvent également permettre de mieux comprendre les modifications apportées aux systèmes contrôlés.

Les cas les plus graves doivent entraîner des poursuites auxquelles il convient de donner une large publicité afin d'inciter d'autres fraudeurs à s'amender. De nombreuses administrations fiscales se sont dotées de programmes de divulgation volontaire destinés à encourager les contribuables à se faire connaître et à corriger leur déclaration d'impôt.

Toutes les administrations fiscales qui tentent de réprimer les pratiques de suppression électronique des ventes doivent pouvoir s'appuyer sur les compétences des agents de terrain responsables du contrôle de la conformité (contrôleur des impôts, contrôleur numérique spécialisé, spécialiste de l'expertise légale numérique et enquêteur criminel) pour mettre en œuvre la stratégie. Elles devront dégager les ressources et développer les compétences requises pour les fonctions décrites ci-dessous.

Le contrôleur des impôts

Si la lutte contre la suppression électronique des ventes suit « l'approche fondée sur des principes », les administrations fiscales comptent sur les contribuables pour respecter leurs obligations fiscales, tenir des livres et des registres comptables exacts et complets et remettre des rapports fiables. Le contrôleur doit alors rechercher un certain nombre d'indices au cours de sa vérification, en effectuant une visite dans les locaux du contribuable afin de relever des informations sur la présence de terminaux point de vente (nom du fabricant, présence d'anciens systèmes PDV désormais hors service, par exemple), réaliser des entretiens (interroger le contribuable et le personnel sur les différentes fonctions et utilisations du terminal PDV, déterminer les rôles et responsabilités du contribuable et du personnel concernant les processus et contrôles internes de l'entreprise, par exemple), procéder à une vérification indirecte du chiffre d'affaires (test de l'origine et de l'usage des fonds, analyse de la valeur nette, par exemple) et examiner les relevés produits par le système PDV (comparaison des ventes déclarées dans le passé avec celles constatées au moment de la visite du contrôleur, par exemple).

S'agissant en outre de la détection des possibilités de fraude fiscale et de l'information des responsables des enquêtes criminelles au sein de l'administration fiscale ou de l'autorité répressive concernée, le contrôleur doit également être attentif à une utilisation éventuelle d'un logiciel de suppression des ventes, et prendre les dispositions nécessaires pour permettre au contrôleur numérique spécialisé d'examiner le système PDV proprement dit.

Si une « approche fondée sur des règles » (plutôt que sur des principes) est suivie, le contrôleur joue un rôle plus important. Dans cette optique, les pouvoirs publics demandent aux utilisateurs d'employer certains matériels et logiciels « homologués » et de conserver certains registres. Parallèlement aux indices traditionnels mentionnés précédemment, le contrôleur peut être amené à surveiller étroitement les caisses enregistreuses électroniques et les systèmes PDV en vue de détecter d'éventuelles

altérations, et à vérifier les registres générés. Dans certains pays, il peut partager cette fonction avec le contrôleur numérique spécialisé.

Les contrôleurs des impôts transmettent tous les cas probables de fraude fiscale à la section des enquêtes criminelles ou à l'autorité répressive concernée, y compris ceux liés à l'utilisation d'un logiciel de suppression des ventes.

Les contrôleurs numériques spécialisés et spécialistes de l'expertise légale numérique

Les contrôleurs numériques spécialisés jouent un important rôle d'appui aux contrôleurs des impôts dès lors que des contribuables utilisent des systèmes PDV. Ce sont eux qui possèdent les compétences techniques nécessaires pour accéder aux systèmes des contribuables et remettre au contrôleur des impôts un listing des registres électroniques des systèmes PDV.

Toutefois, depuis la découverte du premier logiciel de suppression des ventes dans les années 90, le rôle du contrôleur numérique spécialisé a évolué, passant d'un soutien passif à une fonction active de contrôle. Dans les pays où cette fonction existe, elle a acquis les compétences permettant d'effectuer un traçage informatique sophistiqué (décryptage de mots de passe, mise en évidence de l'utilisation faite des touches de fonction réservées aux responsables, détection des modifications de codes, par exemple). Le contrôleur s'entretient également avec les propriétaires des entreprises et leurs collaborateurs concernant l'utilisation des systèmes PDV. Ses conclusions sont généralement transmises aux contrôleurs des impôts qui en tiennent compte dans leurs vérifications.

Dans les cas de fraude grave, le dossier peut donner lieu à une enquête criminelle et le rôle du spécialiste de l'expertise légale numérique passe au premier plan. Ces spécialistes, à l'instar des contrôleurs numériques spécialisés, ont acquis des compétences scientifiques pour la saisie et l'analyse de données électroniques. Ils ont accès aux systèmes PDV et aux ordinateurs du contribuable et utilisent différents éléments scientifiques (analyse des horodateurs, des totaux de contrôle et des comptages, clonage des systèmes à des fins de test, recherche de courriels suspects et récupération de courriels, fichiers et données effacés, etc.) pour aider les enquêteurs criminels à établir l'intention délictueuse ou l'élément intentionnel généralement requis pour entamer des poursuites pénales. Là encore, leurs conclusions sont habituellement transmises à l'enquêteur criminel qui en tiendra compte dans son enquête.

Quelle que soit l'approche adoptée par les administrations fiscales, les contrôleurs numériques spécialisés et les spécialistes de l'expertise légale numérique jouent un rôle essentiel pour remporter la lutte contre les utilisateurs de logiciel de suppression électronique des ventes. Il est également important que les contrôleurs et spécialistes coopèrent efficacement, à la fois entre eux et avec l'administration fiscale.

Enquête criminelle

La menace d'une enquête et de poursuites pénales constitue le principal élément dissuasif que la plupart des administrations fiscales peuvent employer à l'encontre des contribuables qui commettent des fraudes fiscales graves, y compris celles qui impliquent l'utilisation de techniques de suppression des ventes. Comme pour d'autres autorités répressives, il faut réunir des éléments qui corroborent l'existence d'une intention délictueuse et le calcul des recettes non déclarées.

Les enquêteurs ont recours à des techniques traditionnelles (recueil de preuves au moyen de mandats de perquisition octroyés par le juge, ordonnances de communication et entretiens avec les principaux collaborateurs au sein de l'établissement du contribuable, de l'établissement du fabricant du logiciel de suppression des ventes, etc.) en vue de réunir des preuves. Toutefois, d'autres techniques peuvent être appropriées, comme l'organisation d'opérations d'infiltration (décrites précédemment) ou d'opérations conjointes avec d'autres autorités répressives et organismes de réglementation, visant à obtenir des preuves essentielles pour démontrer l'utilisation de techniques de suppression des ventes en vue de minorer des recettes. Le deuxième objectif est d'ordre dissuasif, en sensibilisant le public à la menace croissante que fait peser la suppression électronique des ventes et à l'avantage indu qu'elle confère à leurs utilisateurs. La publicité ainsi générée fait savoir à ceux qui s'engagent dans cette forme de fraude ou d'évasion fiscale que l'administration fiscale est informée de ce comportement et ne le tolérera pas. Les fraudeurs s'exposent à de lourdes amendes et sanctions, voire même à des peines d'emprisonnement.

Sources de renseignements

Outre les agents de terrain qui sont en première ligne du combat contre les techniques de suppression des ventes, d'autres agents œuvrent « dans l'ombre » afin d'appuyer leurs efforts. Il s'agit des agents de renseignements qui, à partir d'informations publiques (non protégées) et générées en interne réunies par les contrôleurs et les enquêteurs (listing des clients des fournisseurs par exemple) sur le terrain, établissent des rapports d'information pour éclairer les décisions des dirigeants ; et des formateurs qui possèdent les compétences nécessaires pour dispenser aux quatre catégories d'agents de terrain la formation requise pour mener à bien leurs tâches.

Une connaissance détaillée du fonctionnement des systèmes PDV est nécessaire pour appuyer le travail de détection et d'enquête. Les informations sur les différents systèmes peuvent être :

- réunies et collectées à partir de sources libres ; ou
- réunies de façon clandestine (par l'achat anonyme de manuels techniques).

Le fondement juridique du recueil d'informations relève de la législation nationale. Il existe de nombreux systèmes qui reposent sur les traditions juridiques et sur la compréhension des droits du public. La plupart des pays de l'OCDE établissent une division entre la législation répressive et la législation fiscale. Le flux d'informations entre l'administration fiscale et l'autorité répressive est généralement très réglementé. De plus en plus, des informations sont recueillies et partagées lorsqu'il y a une forte présomption qu'un délit est ou a été commis. Dans les affaires de malversation et de fraude faisant intervenir des systèmes numériques de type PDV, il est indispensable que les autorités publiques et répressives disposent d'une base juridique suffisante pour collecter et analyser l'information. C'est à cette condition qu'il est possible d'élaborer la meilleure parade et d'identifier les systèmes dont il est fait un usage abusif.

Les informations pertinentes réunies par les administrations fiscales peuvent être partagées avec d'autres administrations fiscales en utilisant toute la palette des dispositifs d'échange de renseignements fiscaux disponibles. Le recours à l'échange spontané de renseignements sur les fabricants exerçant des activités internationales s'est avéré particulièrement utile. L'application de la Convention concernant l'assistance administrative mutuelle en matière fiscale pour permettre l'échange de renseignements

entre plusieurs pays simultanément a montré son efficacité dans de récentes affaires. Cette Convention n'est pas encore signée par tous les États membres, mais le nombre de signataires ne cesse de croître.

Collecte de renseignements

La collecte de renseignements offre à l'enquêteur le moyen de délimiter le champ de son travail. Ces renseignements ne servent pas de preuve lors de poursuites, mais aident l'enquêteur à se procurer des éléments probants utiles. Il sait ce qu'il doit rechercher et sous quelle forme ces éléments se présentent.

Les systèmes de suppression électronique des ventes possèdent de nombreux attributs qui en font de bons candidats à la collecte de renseignements. Les méthodes utiles sont les suivantes :

- Opérations d'infiltration – cette méthode est employée par diverses équipes d'enquête criminelle en matière fiscale pour mener des enquêtes secrètes. Elle suppose une planification juridique, technique et opérationnelle soignée. Les résultats obtenus peuvent être partagés, mais les obstacles juridiques tels que les questions de confidentialité peuvent empêcher la production et l'utilisation de ces informations lors de procédures pénales dans certains pays.
- Les méthodes techniques de *recueil* d'informations incluent les dispositifs d'écoute ou d'interception des communications, la géolocalisation de véhicules, la surveillance de locaux et d'autres opérations « techniques passives » (passives en ce sens qu'elles ne supposent pas une infiltration ou une action similaire). Ces techniques permettent d'*obtenir* des informations et peuvent inclure des mesures telles que l'installation de mouchards sur des ordinateurs, le piratage informatique et d'autres mesures plus agressives encore.
- Utilisation de sources confidentielles et d'informateurs.

Bibliothèque d'informations

Plusieurs pays mettent en place une bibliothèque d'informations pertinentes pour faciliter le travail de contrôle et d'enquête concernant les systèmes PDV. À un niveau national, la bibliothèque peut contenir non seulement des informations disponibles publiquement sur les fabricants, les fournisseurs et les systèmes PDV vendus, mais également des données techniques obtenues lors des contrôles et des enquêtes. Cela conduit à s'interroger sur la possibilité de créer une telle bibliothèque à un échelon international et de la mettre à la disposition des administrations fiscales. Cela pourrait poser des problèmes de protection des données et d'échange d'informations. Une autre solution serait de concevoir un modèle pour l'échange de renseignements sur l'utilisation de systèmes PDV à des fins de suppression des ventes qui ferait partie de l'éventail normal des instruments d'échange de renseignements entre pays qui ont géré leur propre bibliothèque.

Caisses enregistreuses sécurisées et systèmes PDV certifiés

Les pouvoirs publics poursuivent différentes approches pour lutter contre l'utilisation abusive des systèmes PDV par les contribuables à des fins de fraude fiscale. La gamme des solutions s'est étendue, passant de la caisse enregistreuse sécurisée italienne (les données sur les ventes sont sauvegardées dans un dispositif

d'enregistrement à la fin de la journée de travail) au logiciel PDV certifié portugais (le système doit générer des données cryptées sur les ventes accompagnées de signatures numériques qui authentifient la transaction). L'une des principales avancées techniques est que les données sont désormais sécurisées à leur création et non plus, comme dans les anciens systèmes, à la fin de la journée de travail. L'annexe contient une description détaillée des caractéristiques des caisses enregistreuses sécurisées et des systèmes PDV certifiés.

Ce rapport ne préconise pas de solution technique en particulier. Il s'efforce de réunir des informations sur l'éventail des solutions mises en œuvre. On semble s'acheminer vers un système qui enregistre les données au moment de leur création et qui intègre de nouvelles techniques telles que le cryptage de données et les signatures numériques.

Notes

1. La législation adoptée en 2011 ajoute à la loi les infractions suivantes :

   « (ba) possède ou utilise sciemment ou volontairement, en vue d'échapper à l'impôt, un programme informatique ou un composant électronique qui modifie, corrige, supprime, annule, dissimule ou altère de toute autre manière un enregistrement stocké ou conservé au moyen d'un dispositif électronique sans préserver les données originales ainsi que leur modification, correction, annulation, dissimulation ou altération ultérieure,

   (bb) procure ou met à disposition, en vue d'échapper à l'impôt, un programme informatique ou un composant électronique qui modifie, corrige, supprime, annule, dissimule ou altère de toute autre manière un enregistrement stocké ou conservé au moyen d'un dispositif électronique sans préserver les données originales ainsi que leur modification, correction, annulation, dissimulation ou altération ultérieure.

   En cas de condamnation à l'issue d'une procédure simplifiée pour une infraction commise le 14 mars 2008 ou après, ces infractions sont sanctionnées par une amende ne dépassant pas 5 000 EUR (3 000 EUR pour les infractions commises avant cette date) – et qui peut être ramenée à un quart de ce montant au minimum – ou, à la discrétion du tribunal, par une peine d'emprisonnement ne dépassant pas 12 mois, ou les deux, et en cas de condamnation après mise en examen, par une amende d'un montant maximum de 126 970 EUR ou, à la discrétion du tribunal, par une peine d'emprisonnement ne dépassant pas 5 ans, ou les deux. »

2. OCDE (2008) *www.oecd.org/dataoecd/51/13/40947920.pdf*.

3. Note d'orientation sur la tenue de registres : *www.oecd.org/dataoecd/29/25/31663144.pdf*.

4. La brochure sur l'utilisation des labels de qualité, également disponible en anglais, peut être consultée à la page *www.belastingdienst.nl/download/1419.html.*

Conclusions

Depuis que le Groupe d'action de l'OCDE sur les délits à caractère fiscal et autres délits a commencé à sensibiliser les administrations fiscales à la question de la suppression électronique des ventes, celles-ci ont multiplié les initiatives visant à identifier les menaces que ces pratiques font peser sur les recettes fiscales et à y remédier. Néanmoins, ces efforts se sont accompagnés d'une sophistication croissante des techniques employées par les fournisseurs de systèmes PDV afin de dissimuler le recours à cette forme de fraude fiscale. Ce rapport formule des conseils à l'intention des administrations fiscales en vue d'élaborer des stratégies pour combattre la suppression électronique des ventes, et réunit des informations qui permettent aux contrôleurs des impôts et aux enquêteurs de détecter, d'analyser et de réprimer cette fraude fiscale.

Il incombe à chaque administration fiscale d'évaluer les risques et de concevoir la stratégie la plus appropriée et efficace pour s'attaquer à ce problème. Cette stratégie doit comporter une série de recommandations d'action présentées ci-après.

Les travaux du groupe d'experts qui se sont réunis pour établir ce rapport ont eu de nombreuses retombées au cours du processus. La confrontation des expériences a mis en lumière de nouveaux domaines de recherche et, dans certains cas, a favorisé une coopération internationale dans la lutte contre la délinquance financière – allant jusqu'aux descentes dans les locaux et à la question des mandats d'arrêt internationaux. Ces initiatives commencent à avoir un impact sur les fournisseurs de logiciels Phantomware et Zapper qui opèrent à une échelle internationale et qui exploitent à leur profit le manque de communication entre pays.

Recommandations

Les administrations fiscales devraient établir une stratégie de lutte contre la suppression électronique des ventes dans le cadre de leur approche générale de la discipline fiscale, afin que celle-ci tienne effectivement compte des risques posés par les systèmes de suppression électronique des ventes et encourage la conformité volontaire, et elles devraient renforcer les mesures de détection et de répression en ce domaine. Dans l'idéal, il convient d'acquérir une connaissance préalable des systèmes des clients avant d'engager une action, afin de cerner les domaines de risque potentiels et de dégager des ressources.

Il faudrait mettre en place un programme de communication en vue de sensibiliser l'ensemble des parties prenantes au caractère criminel de l'utilisation de méthodes de suppression électronique des ventes et aux graves conséquences qui peuvent en résulter en cas d'enquête et de poursuites.

Les administrations fiscales devraient s'assurer que la législation leur accorde des pouvoirs adéquats aux fins du contrôle et de l'expertise légale des systèmes PDV.

Les administrations fiscales devraient investir en vue d'acquérir les compétences et les outils nécessaires pour mener des contrôles et des enquêtes concernant les systèmes PDV, y compris en créant les fonctions de contrôleur numérique spécialisé et en recrutant, le cas échéant, des spécialistes de l'expertise légale numérique. Elles doivent mettre en place les mécanismes garantissant une coopération efficace entre différents experts dans la lutte contre la suppression électronique des ventes.

Les administrations fiscales devraient envisager de recommander que la législation incrimine l'offre, la possession et l'utilisation d'un logiciel de suppression électronique des ventes.

Annexe : caisses enregistreuses sécurisées et systèmes PDV certifiés

Caisses enregistreuses sécurisées

Les caisses enregistreuses sécurisées ont été introduites par acte législatif dans un certain nombre de pays il y a plus de 25 ans et elles suscitent dernièrement un regain d'intérêt. Fondamentalement, il s'agit de caisses enregistreuses tenues de répondre à certaines prescriptions techniques en vue de sécuriser le stockage de données et de suivre les événements dans le système. Elles ont été introduites pour la première fois en Italie en 1983, lorsque le gouvernement d'alors a instauré l'obligation pour certaines entreprises d'émettre un reçu fiscal au moyen d'une caisse enregistreuse électronique, afin de réduire la taille de l'économie souterraine. Cette approche a également été adoptée par la Grèce et par un certain nombre d'autres pays. Ce sont les autorités de chaque pays qui ont déterminé les informations que le système doit enregistrer, les modalités de stockage des données, ainsi que le type de document (rapports/fichiers et reçus) que le système doit être en mesure de produire, et dans quel format, afin de sécuriser les données en vue de contrôles fiscaux.

Les caisses enregistreuses sécurisées doivent répondre à un certain nombre d'exigences techniques, notamment :

- la conservation électronique des données détaillées des transactions dans le format prescrit, cryptées selon des modalités spécifiques et sur des dispositifs de stockage prédéfinis ;
- des documents détaillés que seul le contrôleur des impôts peut consulter à sa demande ;
- la conservation de pistes complètes pour la vérification et, dans certains cas, le suivi des événements ;
- le système doit être doté d'un module de contrôle sous une forme ou sous une autre ; et
- d'autres mesures techniques destinées à se prémunir contre des altérations ultérieures de manière à garantir l'intégrité des données.

Dans leurs versions initiales, les caisses enregistreuses sécurisées enregistraient les données sur les ventes à la fin de la journée de travail, alors que la logique actuelle consiste plutôt à les enregistrer au moment de leur création.

La mode opératoire est le suivant : à la fin de chaque journée de travail, l'entrepreneur doit générer un rapport financier journalier. Le total des ventes indiqué dans ce rapport est alors inscrit en mémoire protégée, avec actualisation des compteurs en fonction des chiffres de ventes du jour. Dans certains pays, les compteurs ont été par la suite complétés par des compteurs de tickets, des totaux des remboursements et d'autres fonctions.

À l'origine, la mémoire protégée (ROM) était scellée et sécurisée dans l'équipement proprement dit, par sa fixation au châssis à l'aide d'une colle ou d'une résine époxy. Avec la sophistication croissante des caisses enregistreuses et leur intégration dans des systèmes informatiques, l'insertion de la mémoire protégée à l'intérieur du châssis du terminal est devenue facultative, et elle pouvait être logée dans l'imprimante séparée du système (alors appelée imprimante sécurisée).

Le reçu délivré indique spécifiquement s'il s'agit d'un reçu fiscal authentique, représentatif d'une vente enregistrée, ou s'il est émis à des fins de formation, en tant que facture *pro forma*, ou encore d'une copie de ticket. Les reçus fiscaux arborent également une marque dans la partie inférieure, contenant un logo fiscal qui doit répondre à certaines exigences concernant la police de caractère et la disposition typographique.

Graphique 5. Exemples de gauche à droite : Italie, Bulgarie, Grèce et Hongrie.

Source : Informations communiquées par l'Italie, la Bulgarie, la Grèce et la Hongrie.

En fonction du pays, la certification (qui atteste la conformité du système avec la loi) est effectuée par l'administration fiscale ou par des organismes privés.

Différents pays ont adopté des caisses enregistreuses sécurisées, dont l'Argentine, le Brésil, la Bulgarie, la Grèce, la Hongrie, la Lettonie, la Lituanie, Malte, la Pologne, la Russie, la Turquie et le Venezuela. Ces systèmes restent adaptés dans certaines circonstances. Dans certains pays en développement, leur mise en place s'accompagne d'un téléchargement automatique des transactions vers le système informatique de l'administration fiscale.

Systèmes PDV certifiés

Plus récemment, de nombreux pays se sont efforcés d'améliorer la discipline fiscale des contribuables en imposant l'utilisation de caisses enregistreuses « certifiées »,

pour toutes les transactions en espèces ou pour toutes les entreprises de certains secteurs d'activité (comme les restaurants). Cette approche se caractérise par l'utilisation d'un équipement supplémentaire qui ajoute une signature numérique à tout ou partie des données figurant sur un reçu au moyen d'une technologie de cryptage. Il peut s'agir d'un module de contrôle pour le stockage des données des reçus et des signatures et la mise à jour des totaux généraux en mémoire sécurisée.

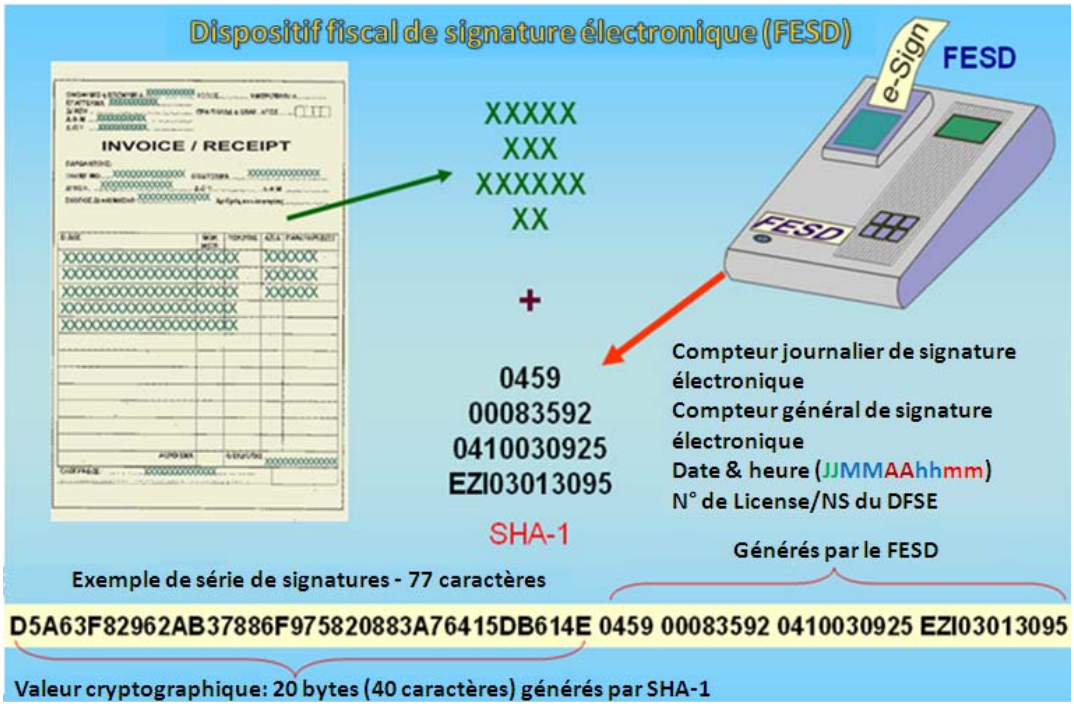
Signature des données sur les reçus et stockage des données pertinentes dans le module de contrôle

Non seulement les solutions techniques de ce type ajoutent une signature numérique à certaines données figurant sur les reçus de transaction, mais elles conservent en outre la trace des données fiscales pertinentes de ces reçus. Parmi les administrations fiscales qui mettent en œuvre ou ont adopté ce type d'approche figurent la Belgique, la Grèce, la province canadienne de Québec et la Suède.

Grèce

Le ministère grec des Finances a été le premier à instaurer la signature numérique[1] des données figurant sur les reçus et les factures. Lorsque cette signature est imprimée sur le reçu ou la facture et enregistrée dans les données d'origine, elle constitue un auxiliaire précieux permettant de vérifier l'intégrité des données du système PDV.

Graphique 6. Le dispositif grec de signature électronique fiscale



Source : Informations communiquées par la Grèce

Québec

Le gouvernement de la province de Québec a conçu un appareil de contrôle, le module d'enregistrement des ventes, qui enregistre les données pertinentes des reçus et génère une signature électronique.[2] La signature est également imprimée sur le reçu du client, dans un code à barres en 2D. La clé publique est conservée par l'administration fiscale (le fournisseur du module d'enregistrement des ventes).

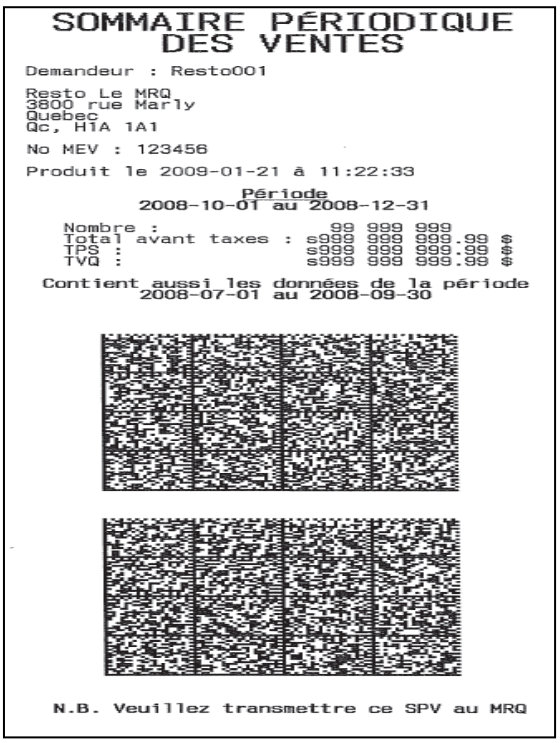
Graphique 7. Le module d'enregistrement des ventes au Québec

Source : Informations communiquées par l'administration fiscale du Québec

La lecture de ce code à barres au moyen d'un lecteur manuel (comportant un logiciel avec clé publique) permet de vérifier très simplement l'authenticité de la signature. Une signature non valide signifie forcément que le contenu du reçu a été falsifié.

En outre, le module d'enregistrement des ventes peut produire un sommaire périodique, également sous la forme d'un code à barres en 2D. Ce sommaire peut être transmis à l'administration fiscale du Québec par courrier normal ou par voie électronique, en le copiant sur une clé USB ou en le téléchargeant sur le site électronique sécurisé de l'administration.

Graphique 8. Exemple de rapport des ventes sous forme de code à barres généré par le module d'enregistrement des ventes québécois



Source : Informations communiquées par le Canada.

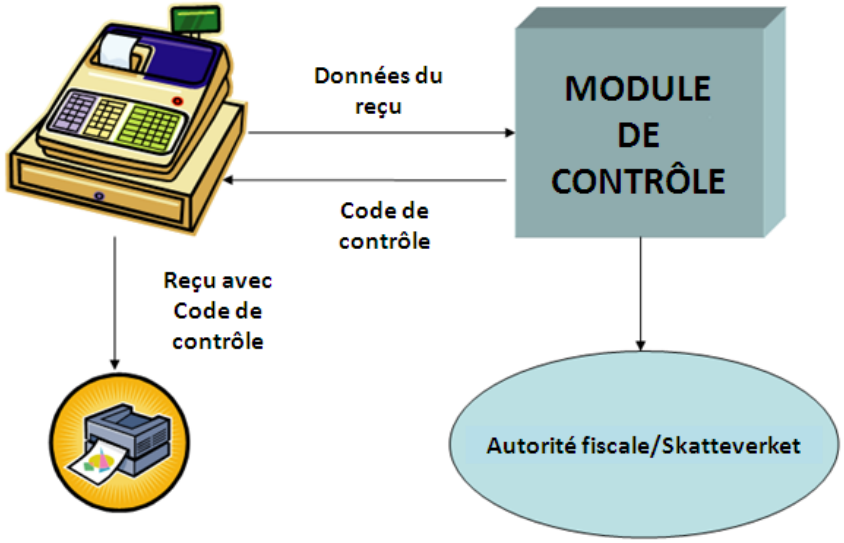
Ce dispositif a été introduit uniquement dans le secteur de la restauration. Des informations complémentaires peuvent être obtenues sur le site Internet[3] de Revenu Québec.

Suède et Belgique

La nouvelle législation suédoise, entrée pleinement en vigueur en 2010, a introduit l'utilisation obligatoire de caisses enregistreuses dans les entreprises caractérisées par une circulation importante d'espèces (avec certaines exemptions, comme les très petites entreprises, les marchés en plein air, les grandes entreprises dotées de contrôles internes rigoureux).

Aux termes de la législation, les systèmes PDV doivent satisfaire à des exigences techniques strictes, qui incluent des fonctions obligatoires et des fonctions prohibées. Le fabricant de la caisse enregistreuse doit la déclarer à l'administration fiscale.

Graphique 9. Le dispositif de contrôle suédois



Source : Informations communiquées par la Suède.

En outre, un module de contrôle doit être relié au système. Il génère une signature numérique[4] basée sur le contenu du reçu. Cette signature (imprimée sur le reçu) simplifie le contrôle de l'intégrité des données figurant sur le reçu. Les données importantes du reçu sont conservées dans une base de données sécurisées contenue dans le module de contrôle, qui héberge également de nombreux compteurs mis à jour à chaque fois qu'un reçu est émis. Une procédure simple de copie permet au contrôleur d'obtenir une copie intégrale de la base de données, ce qui lui permet de mener aisément des vérifications au moyen d'un logiciel spécial.

La Belgique mettra en place un système analogue en 2013. Dans un premier temps, il concernera uniquement les restaurants. Il ciblera les établissements dont au moins 10 % du chiffre d'affaires annuel résulte de la vente de repas consommés sur place.

La principale différence tient au fait que le dispositif de surveillance se compose de deux parties : le module de contrôle comparable au dispositif suédois, et une carte personnalisée (VSC). Le certificat comportant la clé privée, remis par l'administration fiscale, sera inséré dans la carte VSC, qui sera personnalisée en associant le numéro de TVA à la carte, en produisant la paire de clés et en stockant la clé publique dans la base de données de l'administration fiscale. Les fabricants du module de contrôle ne seront pas informés de la clé.

Graphique 10. Le système belge de caisse enregistreuse certifiée

Source : Informations communiquées par la Belgique.

Cette approche privilégie les aspects techniques, mais prévoit également la certification intégrale de chaque composant du système de caisse enregistreuse certifiée, de sorte que chacune des parties prenantes (fabricant, distributeur, utilisateur, administration fiscale) est pleinement informée de ses responsabilités.

Comme en Suède et au Québec, l'émission du reçu (fiscal) est obligatoire, et les systèmes certifiés seront publiés sur le site Internet de l'administration fiscale.

Différentes variantes de ces deux concepts sont à l'étude par d'autres États membres de l'UE, avec notamment l'introduction d'une fonction semi-dématérialisée du module de contrôle.

Signature des données du reçu, stockage des données pertinentes dans l'appareil de contrôle et sécurisation du transfert de données en ligne aux pouvoirs publics

La signature des données du reçu, leur stockage dans un appareil de contrôle et leur mise à disposition pour accès à distance par l'administration fiscale (en utilisant le GRPS par exemple) peuvent être une solution adaptée et économique pour certains États. L'accès à distance peut être automatique, auquel cas une copie intégrale est envoyée à une heure prédéterminée à un serveur central de l'administration fiscale, ou « à la demande », lorsqu'un contrôle est en cours. Un téléchargement automatique peut être considéré comme une déclaration d'impôt officielle.

Signature des données du reçu au moyen d'un logiciel PDV certifié

Le système mis en place au Portugal est l'exemple le plus récent de l'ajout d'une signature numérique au moyen d'un logiciel PDV certifié. Cette approche, qui ne fait pas intervenir d'appareil de contrôle, s'appuie sur un processus de cryptage, qui signe les documents en utilisant une paire asymétrique de clés et un algorithme RSA. Le concepteur du logiciel remet la clé publique à l'administration fiscale et il est le seul à connaître la clé privée. L'administration fiscale vérifie si le logiciel répond aux exigences et, si c'est le cas, le certifie et rend cette certification publique.

Depuis 2008, les systèmes PDV au Portugal doivent obligatoirement utiliser un fichier d'audit standard à des fins fiscales (SAF-T). Cela implique la signature des

champs suivants sur chaque document : date du reçu ; date d'entrée système ; numéro de reçu ; total brut ; et signature du document précédent de la même série.

Par conséquent :

- il est facile de déterminer sur le reçu si un logiciel certifié est ou non utilisé ;
- les chiffres de la signature imprimée doivent correspondre à la signature condensée figurant dans le SAF-T (si le contrôleur le demande) ; et
- sur la base de l'examen de la clé publique, des données du reçu et de la signature sur le reçu, le contrôleur du SAF-T peut déterminer :
  - si le reçu a été falsifié ;
  - si la signature a été générée avec la clé privée correcte ; et
  - si la séquence du reçu a été rompue.

On trouvera des informations complémentaires et une analyse de signature sur le site Internet de l'administration fiscale portugaise (*http://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/news_saf-t_pt.htm*). Y figure également une traduction en anglais de la loi sur la certification des logiciels.

Notes

1. L'algorithme utilisé est un SHA-1 de source libre.
2. Il utilise une infrastructure de clé publique et un algorithme RSA.
3. *http://www.revenuquebec.ca/fr/a-propos/evasion_fiscale/restauration/secteur.aspx*
4. Algorithme RSA, infrastructure de clé publique, clé privée sur certificat dans le module de contrôle.

SUPPRESSION ÉLECTRONIQUE DES VENTES: UNE MENACE POUR LES RECETTES FISCALES

Les techniques de « suppression électronique des ventes » facilitent la fraude fiscale et sont la cause de pertes fiscales très importantes au niveau mondial. Dans le secteur de la vente au détail, les systèmes de terminaux point de vente représentent des outils importants qui doivent contenir des données fiables. En réalité, ces systèmes ne permettent pas seulement l'« écrémage » des recettes en espèces comme un tiroir-caisse manuel, mais, équipés d'un logiciel de suppression électronique des ventes, ils rendent possibles des méthodes de fraude plus complexes. Les administrations fiscales perdent des milliards de dollars à cause des ventes non déclarées et de la dissimulation de recettes à l'aide de ces techniques.

Le présent document examine les fonctions des systèmes PDV, ainsi que les domaines de risque spécifiques. Il décrit en détail les techniques de suppression électronique des ventes qui ont été découvertes par des spécialistes, en particulier « Phantomware » et « Zappers », et montre de quelle façon ces méthodes de fraude peuvent être détectées par les contrôleurs et enquêteurs fiscaux. Le rapport aborde également un nombre de stratégies adoptées dans différents pays afin de lutter contre la fraude liée à la suppression électronique des ventes, et signale certaines pratiques exemplaires. Tout particulièrement, il formule des recommandations destinées aux pays qui souhaitent traiter ce domaine de risque important.

Table des matières:

www.oecd.org/ctp/taxcrimes