FORUM DE L'OCDE SUR L'ADMINISTRATION FISCALE

Administration fiscale : Risques liés à la pandémie de COVID-19 en matière de protection de la vie privée, de confidentialité des données et de fraude

26 mai 2020

OCDE

DES POLITIQUES MEILLEURES POUR UNE VIE MEILLEURE

Administration fiscale : Risques liés à la pandémie de COVID-19 en matière de protection de la vie privée, de confidentialité des données et de fraude

26 mai 2020

Partout dans le monde, les administrations fiscales ont adopté une série de mesures exceptionnelles afin de soutenir les contribuables et l'économie dans son ensemble, notamment en participant à la mise en œuvre d'aides publiques de plus grande ampleur, tout en faisant en sorte, par le biais d'actions diverses, d'assurer la continuité des activités essentielles et la sécurité du personnel comme des usagers. La rapidité avec laquelle ces mesures sont déployées et les modifications apportées à certaines méthodes de travail et procédures de l'administration fiscale peuvent toutefois entraîner une augmentation significative des risques de fraude mais aussi de défaillances ou de manquements liés aux exigences de confidentialité des données et de protection de la vie privée.

Ce document rend compte de certains de ces risques de haut niveau ainsi que des stratégies d'atténuation envisageables, en mettant plus spécifiquement l'accent sur les problèmes liés au travail à distance. Il a été élaboré par le Secrétariat du Forum de l'OCDE sur l'administration fiscale (FTA), en collaboration avec la communauté

d'intérêt sur la gestion globale des risques (*Enterprise Risk Management*) du FTA. Il tient compte des remarques des administrations fiscales qui ont été recueillies au moyen de réunions virtuelles, d'enquêtes et de discussions bilatérales. Ce document ne contient pas de recommandations invitant à adopter des mesures particulières car les circonstances et les considérations à prendre en compte varient énormément selon les pays. Les administrations fiscales sont invitées à faire part de leurs observations en écrivant au Secrétariat du FTA à l'adresse suivante : FTA@oecd.org.

Table des matières

1 Introduction

1. Dans la période actuelle, les risques de fraude et de défaillances ou de manquements liés aux exigences de confidentialité des données et de protection de la vie privée ont sensiblement augmenté. Cela est principalement dû au développement important du travail à distance, à une évolution rapide et parfois déroutante des procédures, à un accroissement des risques de sécurité et à une multiplication des possibilités d'erreur, de comportements répréhensibles et de fraude.

2. Ce document fait état de certains risques de haut niveau, de mesures d'atténuation, d'expositions et de vulnérabilités identifiés par les administrations fiscales membres de la communauté d'intérêt sur la gestion des risques d'entreprise du Forum de l'OCDE sur l'administration fiscale (FTA). Les éléments qui y figurent visent à alimenter la réflexion et les discussions, et n'ont aucunement vocation à être exhaustifs.

2 Risques liés à la protection de la vie privée et à la confidentialité des données

3. Les risques liées à la protection de la vie privée et à la confidentialité des données se rapportent à une possible perte de contrôle par l'administration fiscale d'informations nominatives, de renseignements fiscaux ou autres données sensibles. La perte du contrôle de telles informations, y compris menant à une divulgation publique potentielle de ces informations, peut avoir des répercussions négatives sur la confiance du public dans le système fiscal et affecter par là même la discipline fiscale de manière générale, mais aussi porter gravement atteinte à la réputation de l'administration compétente. Les risques liés à la protection de la vie privée et à la confidentialité des données présentés dans cette section, ainsi que les possibles stratégies d'atténuation y afférentes, sont classés de la manière suivante :

- ***Risques liés à la fermeture des bureaux et au travail à distance*** (risques découlant de la fermeture des bureaux de l'administration fiscale et de l'augmentation significative du recours au travail à distance) ;
- ***Risques liés aux systèmes informatiques*** (risques découlant de l'utilisation de réseaux potentiellement moins sûrs que ceux dont sont équipés les locaux de bureaux) ;
- ***Risques liés aux ressources humaines*** (risques associés à la gestion des ressources humaines des administrations dans le contexte de la pandémie de COVID-19).

Risques liés à la fermeture des bureaux et au travail à distance

Accès non autorisé aux bureaux administratifs

4. Les administrations ont toujours redouté les intrusions et vols d'informations, et ont donc mis en place différentes mesures de sécurité afin de protéger leurs locaux, parmi lesquelles l'obligation d'isoler les documents et données sensibles ou d'en assurer la sécurité d'une manière spécifique. Bien que les intrusions et les vols soient généralement à craindre la nuit, ils deviennent également un risque non négligeable en journée dans la mesure où un nombre important d'agents travaillent à domicile et que certains bureaux sont fermés ou partiellement ouverts. Dans le cas des bureaux fermés, il peut être suffisant de déployer les mêmes protocoles de sécurité que ceux mis en œuvre en temps normal pendant les heures de fermeture nocturne. Lorsque les bureaux sont ouverts mais qu'ils n'accueillent qu'une partie des agents, voire lorsque le personnel de sécurité est réduit, le risque de visiteurs non autorisés peut être supérieur. Les mesures d'atténuation possibles peuvent ainsi consister à :

- augmenter les contrôles à l'entrée, affecter un renfort de personnel de sécurité à l'accueil et exiger la présentation d'une pièce d'identité, y compris lorsque l'accès se fait par le biais d'un passe personnel ;

- diffuser auprès du personnel des lignes directrices sur l'augmentation des risques de sécurité (par exemple, sur la nécessité de verrouiller les ordinateurs et de mettre à l'abri tout document sensible lorsque les agents s'éloignent de leurs postes de travail) et demander aux agents de s'enquérir de l'identité des personnes qu'ils ne connaissent pas et de signaler toute activité inhabituelle ;
- fermer à clé les espaces et bureaux inoccupés, et si possible mettre à l'abri tout équipement informatique non utilisé ;
- fouiller les sacs et voitures en sortie des bâtiments.

Violations accidentelles de la vie privée par des téléacteurs de centre d'appels

5. La limitation des interactions en face à face découlant des fermetures complètes ou partielles de bureaux a entraîné une augmentation de la demande pour les centres d'appels. Dans un environnement axé sur les services, cela peut intensifier la pression qui pèse sur les téléacteurs quant au nombre d'appels à effectuer, augmentant ainsi les possibilités d'erreurs pouvant se traduire par des manquements au respect de la vie privée ou de la confidentialité. Ce risque pourrait être aggravé lorsque certains employés sont nouveaux ou n'ont qu'une expérience limitée du travail en centre d'appels (par exemple, lorsqu'il s'agit de personnel d'autres services qui a été réaffecté). On peut également craindre une augmentation du nombre de personnes cherchant à obtenir des informations de manière frauduleuse dans la mesure où les criminels sont prêts à exploiter la moindre vulnérabilité. Les mesures d'atténuation possibles peuvent ainsi consister à :

- permettre une meilleure information du personnel sur les risques et sur l'importance de se conformer aux obligations de vérification et de sécurité des informations ;
- diffuser des conseils sur la manière d'appréhender les appelants en détresse exerçant une pression sur les téléacteurs en vue d'obtenir des informations au mépris des protocoles de sécurité. Dans ce cas, il peut être utile de mettre en place des scripts d'appel, par exemple ;
- instaurer des protocoles clairs à destination du personnel inexpérimenté couvrant le nombre d'appels reçus, le transfert d'appels si la conversation devient confuse ou trop complexe, la gestion des appelants en détresse ou les mesures à prendre si le téléacteur ressent une certaine pression. La mise en place de formations et de rappels pourrait contribuer à renforcer l'efficacité de ces protocoles ;
- préfiltrer les appels afin de permettre un acheminement des cas complexes ou des appelants en détresse vers des téléacteurs plus expérimentés (éventuellement assuré par un système automatique basé sur la sélection d'options par les appelants en début d'appel) ;
- mettre à jour des guides en ligne s'appuyant sur l'expérience des appels reçus, de sorte à ce que le personnel des centres d'appels et les scripts de réponse automatisée répondent de manière fiable et cohérente aux questions les plus souvent posées et permettent de résoudre les nouveaux problèmes.

Conservation du courrier postal

6. Pour de nombreuses administrations fiscales ou leurs activités, le basculement des communications sur papier vers le numérique est impossible sans de profondes modifications, lesquelles peuvent inclure la mise en place de systèmes numériques de contrôle sécurisés[1]. Le volume de

[1] Le rapport de l'OCDE sur l'administration fiscale 2019 (*Tax Administration 2019*) montre que les communications sur papier continuent d'être pour les contribuables un mode d'interaction important avec l'administration fiscale. Le tableau 1.4 du rapport indique que 28 administrations déclarent avoir reçu 66 millions de demandes de service sur papier pour le seul exercice fiscal 2017. Bien que ces chiffres baissent progressivement (−2.9 % par rapport à 2016),

communications reçues par courrier reste donc potentiellement important, dont une partie peut être de nature très générale et une autre partie liée à des versements ou des remboursements, et donc revêtant un caractère d'urgence. (Il s'agira par exemple de cas où seuls des documents sur papier seront acceptés, où des documents d'identification originaux ou autres documents probants doivent être transmis, ou de cas où une signature manuscrite est requise.)

7. Pour certaines administrations fiscales, le courrier postal peut être adressé à des locaux de bureaux en sous-effectif, ce qui risque d'entraîner d'importants retards dans l'ouverture et le traitement ultérieur des documents. Lorsque les bureaux sont tout simplement fermés, le courrier peut être entreposé dans des espaces de stockage temporaires ou gardé dans les bureaux de poste. Outre les risques de graves difficultés découlant du fait que des courriers ne seront ni ouverts, ni traités, l'entreposage de ces courriers peut également augmenter le risque de perte ou de vol, et dans ce second cas, le risque d'une exploitation frauduleuse ou d'une divulgation publique des informations à caractère personnel de contribuables, voire d'usurpations d'identité.

8. Les mesures d'atténuation possibles peuvent ainsi consister à :

- conseiller aux contribuables de communiquer avec les administrations par le biais de moyens électroniques pour les demandes générales ou de routine, et de n'inclure aucune information sensible dans ces échanges ;
- opérer une distinction entre les communications générales et les communications sensibles liées à la fiscalité en conseillant les contribuables et en les invitant à adresser leurs demandes sensibles aux centres qui sont en mesure de les traiter ;
- conseiller aux contribuables et aux agents de renvoyer les documents importants accompagnés des indications appropriées sur les enveloppes, de sorte à que les courriers soient triés et acheminés plus facilement, en veillant à ce qu'aucun élément ne permette d'identifier la nature des contenus, que ce soit par la population générale ou les employés des services postaux ;
- accepter les communications par courrier électronique (copies numérisées) ou par fax, par exemple, en lieu et place des documents originaux ou sur papier. Cela peut nécessiter un assouplissement des règles en vigueur sur les formes de communication et des prescriptions en matière de documentation (par exemple, en acceptant les signatures électroniques). Dans ce cas, il peut être utile d'augmenter le nombre de contrôles nécessaires dans le processus de vérification (par exemple, dans le cas d'un envoi électronique, au moins deux formes d'identification peuvent être demandées ou une question de contrôle peut être posée à partir des informations détenues par l'administration fiscale) ;
- travailler en collaboration avec l'unité chargée de la délinquance fiscale afin d'identifier les signes de fraude à l'identité découlant du détournement de courrier, comme un nombre inhabituel de modifications apportées aux coordonnées (adresses, comptes bancaires, etc.) dans une zone géographique spécifique ;
- conserver les courriers non ouverts dans des locaux sécurisés plutôt que dans de simples installations de stockage.

Procédures d'expédition et de livraison

9. La fermeture des bureaux et le passage aux solutions de travail à distance peuvent entraîner une augmentation significative du transit d'informations fiscales, d'informations nominatives et autres données

---

le nombre de courriers sur papier reste plus élevé que le nombre de messages électroniques (voir OCDE [2019], *Tax Administration 2019: Comparative Information on OECD and other Advanced and Emerging Economies*, Éditions OCDE, Paris, https://doi.org/10.1787/74d162b6-en).

sensibles vers et en provenance de lieux de travail éloignés. Cette possible multiplication du nombre de livraisons augmente les risques, d'autant plus lorsque des procédures « sans contact » sont mises en place (paquets déposés à l'entrée de résidences, par exemple), comme cela est de plus en plus le cas pendant cette période de crise. Les mesures d'atténuation possibles peuvent ainsi consister à :

- diffuser des lignes directrices visant à encourager au maximum le recours à des moyens de communication électronique (ce qui peut nécessiter une modification des exigences en matière de procédures) et donner des instructions claires sur les situations nécessitant ou non l'envoi de courrier ;
- faire uniquement appel à des services de livraison de confiance, garantissant que le courrier ne sera pas laissé à l'extérieur des résidences sans confirmation visuelle que le destinataire est présent et récupère le pli, et mettre en place des procédures pour contrôler ces opérations.

Conduite des salariés et espace de travail à domicile

10. Le simple fait que le personnel travaille à domicile peut entraîner un risque accru de divulgation d'informations fiscales et nominatives auprès de parents, concubins ou visiteurs. L'essor important du travail à distance à l'occasion de la crise actuelle augmente encore davantage les risques, notamment pour les agents qui découvrent le travail à distance. La présence d'autres membres de la famille ou de concubins travaillant également à distance dans le même espace, ou d'enfants au domicile, constitue par ailleurs un facteur aggravant. Le risque principal est que les informations à caractère personnel soient abordées ou traitées, que ce soit physiquement ou en ligne, en présence de personnes qui ne sont pas des agents de l'administration.

11. Nous avons par ailleurs assisté au cours des dernières années à une popularité grandissante des appareils domestiques intelligents, dont les assistants virtuels à commande vocale. Ces assistants qui répondent à la voix des utilisateurs augmentent le risque de divulgation involontaire d'informations sur les contribuables ou sur les activités des administrations, dans la mesure où ils peuvent être activés intentionnellement ou par inadvertance, et sont susceptibles d'enregistrer les conversations.

12. Les mesures d'atténuation possibles peuvent ainsi consister à :

- publier des lignes directrices, voire des formations en ligne, sur les risques liés à la sécurité et à la protection de la vie privée. Celles-ci pourraient inclure des exemples simples de la manière dont des informations nominatives peuvent facilement être divulguées dans le contexte du travail à distance (par exemple, si l'on ne verrouille pas son écran lorsqu'on s'éloigne de son ordinateur, si l'on travaille au milieu d'autres personnes, si l'on ne gère pas efficacement les mots de passe, etc.) ;
- mettre en place des rappels réguliers, par exemple au démarrage des ordinateurs ou dans le cadre de notifications générales ;
- demander aux agents de soumettre leur environnement de travail à distance à une évaluation des risques et leur fournir des listes de contrôle à renseigner (avec éventuellement un enregistrement centralisé) afin de vérifier qu'ils respectent les obligations de sécurité. Il pourrait ainsi être demandé aux agents de : programmer un délai de verrouillage de leur écran ; activer le verrouillage de l'écran dès qu'ils ne sont pas à leur poste ; préserver la confidentialité des mots de passe et en changer régulièrement ; installer leur poste de travail de sorte à ce que leurs conversations ne puissent être écoutées et que leur écran ne puisse être vu par d'autres personnes ; conserver sous clé tout document sur papier à caractère sensible ; éviter d'imprimer des informations sensibles ; ou encore verrouiller et sécuriser les ordinateurs portables et de bureau ;
- promouvoir l'utilisation ou fournir au personnel des ordinateurs portables ou des moniteurs disposant de filtres de confidentialité pour bloquer la vision latérale ;

- promouvoir l'utilisation ou fournir au personnel des casques afin que les personnes à proximité ne puissent écouter les appels reçus ou émis ;
- encourager l'adoption de méthodes sécurisées pour la destruction des informations confidentielles (par exemple, en utilisant des ciseaux pour réaliser un déchiquetage transversal, en plongeant les documents dans l'eau pendant 24 heures, etc.) ;
- expliquer au personnel les risques posés par les assistants virtuels et leur conseiller de désactiver ces appareils ou de travailler dans des pièces qui n'en sont pas équipées.

Entreposage des dossiers et équipements informatiques

13. Le travail à distance représente également un risque en ce sens qu'il est possible pour des personnes tierces d'avoir accès aux informations à caractère personnel d'agents, de contribuables ou de bénéficiaires de prestations car les membres du personnel ne disposent pas des installations adéquates pour conserver de manière sécurisée les dossiers fiscaux et les équipements informatiques de l'administration. Bien que le personnel déjà habitué au travail à distance puisse disposer d'armoires de rangement verrouillables et approuvées par l'administration, cela n'est pas nécessairement le cas des agents récemment passés au travail à distance. Les risques sont encore aggravés par le grand nombre de personnes qui ont basculé vers le travail à distance pendant l'épidémie et dont le domicile peut ne pas être aussi sécurisé que les bureaux de l'administration. Les mesures d'atténuation possibles peuvent ainsi consister à :

- diffuser des lignes directrices sur la manière de conserver les dossiers et équipements de manière plus sécurisée à domicile, par exemple dans des pièces ou des armoires fermées à clé, ou dans des lieux inaccessibles à des tiers ;
- lorsque cela n'est pas déjà fait, demander au personnel d'envisager l'achat de cadenas ou de systèmes antivol pour ordinateur ;
- si possible, renforcer la sécurité des disques durs des ordinateurs par l'installation de logiciels de chiffrement.

Risques liés aux systèmes informatiques

Utilisation d'appareils personnels

14. Le travail de l'administration fiscale s'appuie généralement sur des équipements informatiques qui intègrent des contrôles de sécurité susceptibles d'empêcher l'utilisation d'appareils personnels (p. ex., imprimantes ou scanners) pour réaliser certaines tâches dans le cadre du travail à domicile.

15. Les agents peuvent être tentés de contourner ces règles en transmettant des informations sur les contribuables par le biais de canaux non sécurisés afin de faciliter leur travail à domicile, notamment par le biais de messageries électroniques non chiffrées. Dans ce contexte, les appareils personnels pourraient permettre l'introduction de logiciels malveillants dans le système de l'administration ou la divulgation d'informations nominatives à des tiers, comme des parents ou même des pirates informatiques si les appareils personnels sont infectés par un logiciel malveillant et sont par la suite dérobés. Les mesures d'atténuation possibles peuvent ainsi consister à :

- installer sur les ordinateurs de l'administration des logiciels qui détectent et bloquent la connexion d'équipements informatiques non approuvés ;
- installer des logiciels qui empêchent la transmission d'informations sensibles vers des adresses de messagerie non approuvées ou, lorsque cela n'est pas possible, afficher des

invites exigeant des expéditeurs qu'ils confirment que les informations envoyées ne revêtent pas un caractère sensible ;

- lorsque l'impression de documents s'impose, envisager de les faire imprimer par du personnel encore au bureau, puis de les faire envoyer par un service de livraison sécurisé, ou permettre aux agents de réserver des créneaux horaires pour se rendre au bureau et imprimer ou numériser les documents dont ils ont besoin (voire détruire certains documents).

Tentatives d'hameçonnage

16. L'augmentation du nombre de messages venant de sources différentes (relatifs aux missions de l'administration fiscale, aux mises à jour de situation, aux notifications d'urgence, à l'évolution de la pandémie de COVID-19, etc.) accentue le risque que des messages d'hameçonnage soient considérés par erreur comme des communications officielles et qu'ils soient donc ouverts à la fois par le personnel de l'administration et par des contribuables. Le piratage social est le risque de cybersécurité le plus important car il peut exposer les administrations fiscales à des problèmes de logiciels malveillants ou de compromission d'informations de connexion, et les contribuables à des problèmes d'usurpation d'identité et de fraude au remboursement. Les tentatives d'hameçonnage peuvent être particulièrement courantes dans les pays où les paiements de soutien sont pris en charge par l'administration fiscale ou avec son concours. Les mesures d'atténuation possibles peuvent ainsi consister à :

- diffuser une information publique permettant aux destinataires de courriers électroniques censés venir de l'administration de déterminer si ces messages sont authentiques, et fournir une liste des informations qui ne seront jamais demandées par l'administration fiscale dans une communication par courrier électronique ;
- continuer de communiquer avec le personnel et les contribuables en utilisant toujours la même adresse de messagerie ;
- lorsque l'administration fait appel à des prestataires externes pour réaliser des enquêtes (auprès du personnel ou des contribuables, par exemple), diffuser un message officiel en amont afin d'avertir les parties concernées qu'elles seront bientôt contactées par un prestataire externe. Ce message devrait inclure le nom de ce prestataire et la date à laquelle l'enquête sera envoyée ;
- demander au personnel et aux contribuables de signaler tout message électronique suspect en le transférant à une adresse dédiée de l'administration fiscale ;
- travailler en collaboration avec les fournisseurs d'accès à l'internet pour une meilleure identification des messages indésirables.

Réseaux et applications non sécurisés

17. L'utilisation accrue de réseaux autres que ceux de l'administration publique par le personnel travaillant à distance pose un risque important de violation d'informations. Les réseaux domestiques utilisés par les agents pour connecter leurs équipements aux systèmes informatiques de l'administration fiscale peuvent ne pas disposer du même niveau de sécurité (en termes de pare-feu ou de systèmes de détection d'intrusion) que les réseaux utilisés dans les bureaux de l'administration. Cela pourrait en effet augmenter le risque de compromission d'équipements ou d'accès à des informations sensibles par des personnes non autorisées. Ce risque serait encore renforcé lorsque le personnel souhaite travailler à l'extérieur en utilisant des réseaux publics, par exemple pour éviter de rester dans un logement où résident plusieurs personnes. De la même manière, l'utilisation d'applications non approuvées par l'administration publique (solutions de visioconférence ou services d'hébergement, par exemple) peut présenter des risques d'atteinte à la vie privée puisque des acteurs extérieurs pourraient écouter les conversations ou

assister discrètement à des réunions en ligne. Les mesures d'atténuation possibles peuvent ainsi consister à :

- rappeler au personnel d'éviter de se connecter à des réseaux publics et d'utiliser uniquement des réseaux domestiques sécurisés (tout en veillant à mettre régulièrement à jour les logiciels de sécurité) ;
- diffuser des conseils auprès du personnel sur la protection des réseaux domestiques, y compris sur les applications dont l'utilisation est sûre ;
- améliorer les procédures de contrôle pour les transactions financières, la réinitialisation de l'accès aux comptes, la gestion des informations de connexion et le partage d'informations à caractère personnel ;
- demander au personnel de renforcer les mots de passe et, le cas échéant, de passer à une authentification à deux étapes ;
- envisager une possible installation à distance de systèmes de détection d'intrusion, éventuellement en collaboration avec les fournisseurs d'accès à l'internet ;
- diffuser des lignes directrices sur les sujets à ne pas aborder à l'oral ou à l'écrit en cas d'utilisation d'applications non approuvées par l'administration publique (logiciels de visioconférence, notamment) ;
- vérifier les appareils rapportés afin de détecter une éventuelle infection par un logiciel malveillant.

Risques liés aux ressources humaines

Départ de personnel

18. Même en période de pandémie, certains membres du personnel quittent les administrations fiscales, que ce soit dans le cadre d'un départ à la retraite ou pour d'autres raisons. Bien que des procédures standard existent normalement pour le retour des badges et des équipements confiés aux agents, ces opérations peuvent s'avérer plus difficiles à organiser lorsque le personnel travaille à distance et que les bureaux sont fermés. L'approche naturelle serait de renvoyer ces éléments par courrier ou transporteur au bureau ou à l'adresse d'un responsable désigné. Cela poserait toutefois des risques supplémentaires liés à la récupération des équipements des agents sortants, de leurs dossiers sur papier, de leurs badges d'identification, etc., dans la mesure où des colis peuvent être égarés. Une vigilance renforcée peut donc être nécessaire dans l'expédition de tout équipement ou document au bureau ou au responsable désigné afin d'éviter toute perte éventuelle. Les mesures d'atténuation possibles peuvent ainsi consister à :

- mettre à jour les procédures relatives au départ de personnel. L'administration pourrait par exemple demander à ce que l'expédition soit effectuée à partir d'une date fixe et assurée par un transporteur autorisé ou de confiance. Il pourrait également être exigé que tout appareil permettant l'accès aux systèmes internes (jetons d'authentification, par exemple) soit expédié séparément des ordinateurs portables ;
- veiller à ce que les procédures en place permettent une désactivation complète des accès des agents sortants à la fin de leur contrat ou avant la date convenue pour le retour des équipements, badges, etc. (si cette date est antérieure à la date de fin du contrat) ;
- s'assurer que toute tentative d'utilisation des anciennes informations de connexion d'un agent est immédiatement signalée ;
- envisager de limiter l'accès des agents sortants qui travaillent à distance en temps utile avant la fin de leur contrat.

Informations sur la santé du personnel

19. Les agents disposent d'un droit à la confidentialité des informations relatives à leur santé. La crise actuelle soulève toutefois un grand nombre de questions sur la nature des informations qui peuvent et devraient être partagées sur le personnel atteint de COVID-19, dans la mesure où celles-ci relèvent d'un enjeu de sécurité. Bien qu'une partie des agents ne voient aucun inconvénient à ce que ces informations soient partagées, d'autres peuvent les considérer comme privées et préférer ne pas les partager.

20. L'un des problèmes majeurs pour l'administration est de trouver un équilibre entre le droit de ses agents au respect de leur vie privée et la sécurité des contribuables et des autres membres du personnel. Il est ainsi important de bien déterminer les situations dans lesquelles il convient de partager le diagnostic d'un agent ou les lieux où il a travaillé ou voyagé au cours des semaines passées, et le cas échéant dans quelle mesure ces informations seront diffusées. Le fait qu'un agent ait été atteint de COVID-19 peut par exemple n'affecter aucunement la continuité des activités (sauf pour des besoins de désinfection), même si cet agent travaille à un poste critique. Il peut ainsi être suffisant pour les autres parties concernées de simplement être averties que cet agent risque de ne pas être disponible pendant une période prolongée afin qu'elles prennent les mesures nécessaires pour gérer sa charge de travail. Les mesures d'atténuation possibles peuvent ainsi consister à :

- réaliser une évaluation d'impact relative à la protection des données afin de définir des règles claires ou des protocoles précis à suivre en matière de collecte et de communication d'informations sur les questions liées à la pandémie de COVID-19 (comme le diagnostic, avéré ou suspecté, de membres du personnel ou de leurs parents). Ces questions peuvent nécessiter l'implication des représentants du personnel, y compris des syndicats, ainsi que des responsables de la protection des données ;
- diffuser ces règles et protocoles auprès de l'ensemble du personnel et mettre en place des rappels réguliers ;
- collecter uniquement les informations nécessaires aux objectifs recherchés et limiter au maximum le nombre d'agents ayant accès à ces informations (par exemple, à certains membres du service des ressources humaines) ;
- lorsque des informations ont été partagées pour des raisons de sécurité sanitaire (par exemple, auprès de contribuables ou d'autres agents afin qu'ils se fassent tester, se confinent, procèdent à des opérations de désinfection, etc.), veiller à ce que les personnes concernées comprennent l'importance de conserver la confidentialité de ces informations ;
- s'entretenir avec l'agent affecté pour déterminer avec qui les informations sur sa santé peuvent être partagées et à quelles fins. L'agent doit disposer d'un pouvoir décisionnaire sur le partage de toute information personnelle dans le cadre d'activités facultatives non liées à la sécurité (soutien, assistance ou encore condoléances).

3 Risques de fraude

21. En période de pandémie, on s'attend à ce que les risques de fraude augmentent de manière significative, notamment en raison de l'évolution rapide de la situation, des fortes probabilités d'incertitude et de désinformation, des risques accrus liés à la protection de la vie privée et à la confidentialité des données (tel que défini dans le chapitre 2), de la multiplication des possibilités de fraude liées aux versements réalisés par les services publics, d'une éventuelle réduction des contrôles, ou encore d'une baisse des activités normatives et exécutoires.

22. Les risques présentés dans ce chapitre sont organisés en trois catégories, dont les deux premières ont trait à des sources externes à l'administration fiscale et la troisième à des sources internes :

- ***Risques de fraude à l'identité*** (risques que des personnes acquièrent et utilisent indûment les données relatives à des individus, à des entreprises ou à des organismes publics à des fins frauduleuses) ;
- ***Risques de fraude fiscale*** (risques que des personnes ou des entreprises falsifient intentionnellement des informations pour réduire leurs impôts ou bénéficier de remboursements ou autres types de paiements de l'administration fiscale) ;
- ***Risques de fraude interne*** (risques d'actes frauduleux perpétrés par des personnes internes à l'administration, comme le personnel, les prestataires et autres parties de confiance).

Risques de fraude à l'identité

Usurpation d'identité personnelle ou d'entreprise

23. De nombreux gouvernements ont mis en place des programmes pour soutenir les entreprises et les particuliers affectés par la pandémie de COVID-19 et c'est, dans certains cas, l'administration fiscale qui est chargée de gérer les aides publiques. La manière dont ces aides sont distribuées peut inciter des parties malintentionnées à usurper l'identité d'individus ou d'entreprises dans le but de détourner des paiements vers une adresse ou un compte bancaire qui leur appartient. Ce problème peut toucher aussi bien des personnes vivantes et des entreprises en activité, que des personnes décédées et des entreprises ayant cessé leur activité.

24. Outre les risques liés au détournement d'aides financières, on peut s'attendre à une augmentation du risque que des parties malintentionnées exploitent, d'une part, les restrictions imposées en termes d'interactions en face à face et, d'autre part, l'essor des services électroniques afin d'accéder aux informations des contribuables dans le cadre d'une usurpation de leur identité, éventuellement à des fins de fraude fiscale (remboursement illicites, par exemple) ou de fraude vis-à-vis de tiers (banques, établissements de prêt hypothécaire, établissement de crédit, etc.). Les mesures d'atténuation possibles peuvent ainsi consister à :

- coopérer avec d'autres organismes publics pour vérifier les coordonnées et les informations de compte des contribuables, en fonction par exemple d'un répertoire national des personnes physiques ou des entreprises ;

- imposer une authentification à deux étapes aux particuliers et aux entreprises avant d'accéder aux paiements ;
- réaliser une évaluation des risques afin de déterminer si les options en libre-service (comme la modification de l'adresse ou du compte bancaire) doivent être soumises à des contrôles supplémentaires.

Escroquerie par usurpation de qualité

25. Une variante de l'usurpation d'identité consiste à usurper la qualité d'agent d'organismes publics afin, dans le cas de l'administration fiscale, de commettre une fraude. Selon le canal de communication exploité, ces escroqueries par usurpation de qualité peuvent prendre des formes différentes, dont :

- les escroqueries téléphoniques, par lesquelles les appelants prétendent être des agents de l'administration et demandent des informations personnelles ou des transferts directs d'argent ;
- les escroqueries par courrier électronique, conçues pour faire croire aux contribuables qu'ils reçoivent des messages officiels de l'administration alors que ceux-ci contiennent des liens vers des sites internet malveillants ;
- les escroqueries par démarchage direct, par lesquelles des individus se faisant passer pour des agents de l'administration font du porte à porte afin de récupérer des sommes dues ou demander des informations à caractère personnel.

26. Les programmes d'aide publique mis en place dans le cadre de la pandémie de COVID-19 augmentent les incitations pour les parties malintentionnées à se faire passer pour des agents de l'administration et leur en donnent davantage d'opportunités (par exemple en prétendant devoir « vérifier » les informations bancaires des contribuables. Les mesures d'atténuation possibles peuvent ainsi consister à :

- mettre en place des campagnes en ligne ou par courrier électronique afin d'exhorter les contribuables à la vigilance et leur conseiller de se rendre directement sur le site internet de l'administration fiscale plutôt que de cliquer sur les liens inclus dans des messages électroniques ;
- présenter clairement en quoi consistent les interactions et le communications officielles, y compris les informations qui ne seront jamais demandées par l'administration, ainsi que les signes les plus courants de fraude potentielle ;
- collaborer avec les fournisseurs d'accès à l'internet et les organisations de sécurité à l'échelle nationale pour fermer les sites internet frauduleux.

Risques de fraude fiscale

Accès aux versements d'aide ou aux remboursements

27. Souvent élaborés et exécutés dans l'urgence, les programmes d'aide publique peuvent donner à certains particuliers et entreprises l'occasion de commettre des actes de fraude fiscale dans le but d'augmenter les crédits ou versements dont ils sont bénéficiaires. Le volume important de demandes d'aide ou de restitution, associé à des faiblesses en matière de surveillance et de contrôle découlant potentiellement d'une augmentation du travail à distance, peut limiter de manière significative la fiabilité des vérifications. Ces agissements frauduleux peuvent également inclure la création de nouvelles entreprises afin de bénéficier d'aides directes ou de remboursements de l'administration fiscale. Lorsque les versements d'aide sont corrélés au nombre d'employés d'une entreprise ou aux salaires des employés, la fraude peut également porter sur la déclaration de personnels fictifs.

28. En parallèle à cela, il est possible que les administrations aient assoupli les modalités relatives aux obligations fiscales pour les particuliers et les entreprises, en exemptant par exemple les contribuables de fournir des justificatifs sur la base de documents originaux ou en permettant l'envoi de copies numérisées. Ces facilités peuvent également augmenter le risque de fraude fiscale. La capacité des banques et autres institutions financières à faire office de filtre supplémentaire pour la détection des fraudes est en outre amoindrie en raison de la limitation des interactions et services en face à face. L'augmentation du recours aux versements électroniques peut également limiter la capacité à identifier les activités suspectes ou frauduleuses.

29. Les mesures d'atténuation possibles peuvent ainsi consister à :

- veiller à la traçabilité complète de l'ensemble des paiements électroniques, en accordant une attention particulière aux nouveaux comptes bancaires ;
- définir de nouveaux signaux d'alerte dans les évaluations des risques lorsqu'il est possible de réaliser des vérifications plus poussées. Ceux-ci peuvent inclure : les entreprises nouvellement créées ; les contribuables récemment enregistrés auprès de l'administration ou qui n'avaient auparavant jamais déposé de dossier ; ou les modifications récentes de coordonnées postales ou bancaires (notamment en période de crise où les déménagements sont moins probables) ;
- communiquer avec les banques sur l'importance des contrôles et l'application des normes de lutte anti-blanchiment, ainsi que du signalement de transactions suspectes ;
- renforcer l'information sur les sanctions encourues, y compris les sanctions pénales, en cas de fausse déclaration.

Fraude fiscale liée aux paiements en espèces

30. La crise économique provoquée par la pandémie de COVID-19 et son incidence sur les finances des entreprises peuvent augmenter le risque de fraude fiscale liée aux paiements en espèces. Par exemple, les entreprises qui n'ont pas cessé leurs activités pendant la crise pourraient vendre des biens ou assurer des services en échange de paiements en espèces sans fournir de reçus afin d'éviter toute imposition (TVA, taxes générales sur les ventes et impôts sur les bénéfices). Une autre forme d'escroquerie, réservée aux entreprises ayant des salariés, consiste à les payer en espèces afin d'éviter d'avoir à les déclarer et à s'acquitter des cotisations sociales et impôts correspondants. Les mesures d'atténuation possibles peuvent ainsi consister à :

- alerter les entreprises sur la nécessité de conserver tous leurs justificatifs à des fins d'audit et de conformité suite à la crise, ainsi que pour permettre à l'administration fiscale d'évaluer les risques ;
- rappeler aux entreprises et aux employeurs les sanctions auxquelles ils s'exposent en cas de fausse déclaration ;
- mettre en œuvre des incitations pour les lanceurs d'alerte ;
- procéder à des audits à distance ou, lorsque cela est possible, à des audits physiques si la suspicion de fraude est importante.

Risques de fraude interne

31. Cette période de pandémie de COVID-19 s'avère difficile pour de nombreuses personnes, y compris les agents des administrations fiscales et les employés de leurs prestataires de services. Les mesures de distanciation physique et le travail à distance peuvent avoir des incidences négatives sur le moral des agents, sous-traitants et partenaires de confiance, et augmenter le stress psychologique auquel

ils doivent faire face. La crise peut par ailleurs également exercer une pression financière sur certaines de ces parties prenantes (y compris sur leurs familles).

32. Cette pression financière accrue, associée à l'évolution rapide de la situation et à la mise en œuvre des programmes d'aide, et parfois au manque de supervision lié au travail à distance, peut présenter pour certains agents une opportunité de commettre des actes de fraude en partageant des informations sur des contribuables ou d'autres agents, ou en se rendant coupables de comportements répréhensibles afin de s'approprier des ressources ou biens publics. Même si le risque est faible, les répercussions de ce type de fraude sur la réputation de l'administration fiscale pourraient être extrêmement préjudiciables.

33. Les mesures d'atténuation possibles peuvent ainsi consister à :

- mettre en place et promouvoir régulièrement des programmes de soutien spéciaux pour les agents, et encourager les responsables à faire le point fréquemment avec leurs équipes. Ces programmes pourraient également venir à l'appui des agents subissant une certaine pression financière ;
- réaliser des évaluations du risque de fraude en interne ou déployer des outils d'auto-évaluation des risques de fraude, lesquels pourraient par exemple exiger du personnel qu'il fasse état de certains types d'investissements ;
- renforcer les contrôles requis au-delà de seuils définis pour les versements à destination des contribuables, par exemple en appliquant le « principe du double regard » (par lequel une opération doit être approuvée par au moins deux personnes) pour valider le versement de sommes importantes ;
- conseiller aux responsables d'observer la plus grande prudence, de veiller à ce que soient réalisés des contrôles internes et des vérifications rétrospectives, et de faire en sorte que les résultats des activités à distance soient systématiquement partagés.

Contact

Secrétariat du Forum de l'OCDE sur l'administration fiscale (✉ FTA@oecd.org)

www.oecd.org/tax/forum-on-tax-administration/