Organisation de Coopération et de Développement Économiques

DAF/COMP/GF(2018)7

Non classifié

Français - Or. Anglais

22 novembre 2018

DIRECTION DES AFFAIRES FINANCIÈRES ET DES ENTREPRISES
COMITÉ DE LA CONCURRENCE

Forum mondial sur la concurrence

LES POUVOIRS D'ENQUÊTE EN PRATIQUE – Sous-session 1: Inspections inopinées à l'ère numérique

- Note de réflexion du Secrétariat -

30 novembre 2018

Ce document rédigé par le Secretariat de l'OCDE est une note de réflextion en vue de la sous-session 1 de la session IV du 17e Forum mondial sur la concurrence tenu les 29 et 30 novembre 2018.

Les opinions et les arguments exprimés ne reflètent pas nécessairement les vues officielles de l'OCDE ou des gouvernements de ses pays membres.

D'autres documents relatifs à cette discussion sont disponibles sur: **oe.cd/pinv**.

Veuillez prendre contact avec Mme. Beyza Erbayat [E-mail: Beyza.Erbayat@oecd.org] et Mme. Lynn Robertson [E-mail: Lynn.Robertson@oecd.org], pour toute question relative à ce document.

JT03440247

Table des matières

Encadrés

Les pouvoirs d'enquête en pratique

Session en sous-groupes n° 1 : Inspections inopinées à l'ère numérique

1. Introduction

1. Les informations sont aujourd'hui produites, stockées et traitées essentiellement sous forme numérique. La communication est de plus en plus facilitée par des technologies numériques comme le courrier électronique et les applications de messagerie instantanée mobile. On estime que le trafic quotidien de courriers électroniques, qui était de 182.9 milliards de messages en 2013[1], augmentera à 281.1 milliards de messages en 2018[2]. Le nombre de comptes de messagerie instantanée (messagerie mobile non comprise) est passé de 3.3[3] à 6.4 milliards[4] au cours des trois dernières années. Ces chiffres englobent les communications privées comme celles entre entreprises. Les entreprises opèrent la transformation numérique de processus comme les paiements, la gestion des stocks et le stockage des données en raison des nombreux avantages qu'elles en tirent en termes d'efficacité, d'innovation et de sécurité.

2. La transformation numérique n'est pas sans effet non plus sur les inspections inopinées effectuées par les autorités de la concurrence. La capacité de mener des inspections sur place est probablement l'outil le plus intéressant dont celles-ci disposent pour réunir des preuves et des informations[5]. À l'ère du numérique, il serait très utile de pouvoir réaliser des perquisitions sur des supports numériques et de recueillir des preuves numériques.

3. La présente note décrit les principaux problèmes relatifs aux perquisitions numériques réalisées lors d'inspections inopinées. La section 2 examine les avantages et les inconvénients de la collecte de preuves numériques. La section 3 s'intéresse aux principes et méthodes suivis pour réaliser des inspections numériques. La section 4 décrit les différentes difficultés auxquelles se trouvent confrontées les autorités de la concurrence lorsqu'elles collectent des preuves numériques. La section 5 est consacrée à la conclusion.

2. Avantages et inconvénients de la collecte de preuves numériques

4. La transformation numérique offre de nombreux avantages aux utilisateurs du monde des entreprises et renforce notamment la sécurité, grâce au cryptage, tout en améliorant l'accessibilité et l'efficacité. Pour les autorités de la concurrence, la transformation numérique des processus d'entreprise présente également une foule d'avantages.

5. Premièrement, la collecte de preuves numériques augmente les sources possibles de preuves. À l'heure actuelle, la quasi-totalité des informations sont créées ou exploitées dans un environnement numérique ou transférées sur un support numérique. Souvent, ces informations n'existent même pas sur support papier (RIC, 2014, p. 7[1]). La perquisition numérique offre donc aux autorités de la concurrence de meilleures chances de découvrir des preuves lors des inspections inopinées.

6. Deuxièmement, il est souvent plus difficile de détruire des preuves numériques que des preuves matérielles. L'environnement numérique permet de récupérer des données supprimées ou endommagées. Un document conservé sur support numérique, même s'il est détruit définitivement, peut être retrouvé sur d'autres supports numériques ou laisser des traces de son existence de sorte que sa destruction peut être détectée plus facilement.

7. Troisièmement, à la différence des preuves matérielles, les informations conservées sur un document numérique ne se limitent pas au contenu. Les informations sur les données mêmes, appelées métadonnées, peuvent aussi être utiles pour une enquête. Les métadonnées peuvent contenir des informations telles que l'origine du document, son auteur, la date à laquelle il a été créé, modifié ou supprimé, la date de la dernière mise à jour, les personnes qui y ont eu accès ou l'identité d'un expéditeur ou d'un destinataire (RIC, 2014, p. 7[1]). Par exemple, l'outil de filtrage des ententes élaboré par l'Autorité britannique de la concurrence et des marchés (*UK Competition and Markets Authority*) utilise entre autres critères des métadonnées sur les auteurs des documents pour détecter les documents de soumission qui pourraient avoir la même origine, ce qui augmente les possibilités de manipulation des offres[6].

8. Enfin, les preuves numériques peuvent se révéler plus utiles dans le cadre des systèmes de gestion des affaires et de perquisition numérique. Les documents examinés dans leur format natif permettront vraisemblablement d'obtenir des résultats de recherche plus complets que les documents papier numérisés (RIC, 2014, p. 8[1]).

9. La transformation numérique des processus d'entreprise peut également soulever des difficultés. Les données numériques peuvent être plus vulnérables que les documents papier. Elles peuvent être modifiées ou détruites par le fonctionnement quotidien des systèmes informatiques ou par les conditions matérielles (par exemple une température élevée et les champs électromagnétiques). Par conséquent, la collecte de preuves numériques demande un soin particulier en termes de sécurité et de préservation des données.

10. La collecte de preuves numériques exige également des compétences, des outils (matériels et logiciels) et des infrastructures (locaux réservés aux activités d'investigation) supplémentaires. Il est plus onéreux de mettre en place et d'entretenir des moyens de collecte de preuves numériques que des moyens de collecte de preuves classiques.

11. Enfin, dans de nombreux pays, le cadre juridique ne contient pas de règles particulières concernant la collecte de preuves numériques et il n'est pas possible d'adapter directement les règles relatives à la collecte de preuves matérielles à celle des preuves numériques. Cette situation réduit la certitude juridique pour les autorités de la concurrence et les autres parties concernées.

12. Cependant, on ne saurait mettre en doute le fait que si l'on veut disposer d'un régime répressif efficace, la collecte de preuves numériques devient de plus en plus indispensable et doit être complémentaire de la collecte de preuves matérielles, laquelle a toujours son importance.

3. Principes et pratiques d'inspection numérique

13. De plus en plus, les autorité de la concurrence prennent en compte les données numériques lorsqu'elles effectuent des inspections pour recueillir des preuves pertinentes. Leurs méthodes et leurs procédures varient largement en fonction des ressources dont elles disposent et du cadre juridique applicable. Certains principes concernant la collecte de

preuves numériques semblent généralement reconnus et peuvent contribuer à façonner la pratique des inspections numériques.

3.1. Principes de criminalistique numérique

14. La criminalistique numérique, qui est une branche de l'investigation judiciaire, englobe l'application de techniques scientifiques pour détecter, préserver, récupérer et analyser des données numériques et présenter des faits et des avis sur celles-ci. La criminalistique numérique respecte les normes juridiques de preuve admissible et les procédures juridiques applicables et est régie par des principes reconnus en matière de collecte de données numériques, et notamment :

- Légalité : toutes les données numériques doivent être recueillies dans le respect de la loi (RIC, 2014, p. 17[1]). Cela signifie que les inspections numériques doivent être juridiquement fondées. En outre, les inspections numériques doivent être menées dans le respect des limites fixées par les décisions d'inspection ou les décisions judiciaires et l'objet de l'affaire en cause.
- Compétence : la collecte de preuves numériques exige compétence et vigilance. « Les personnes qui examinent des preuves numériques doivent avoir la formation appropriée » (US DoJ, 2004[2]). Tous les agents qui prennent part au processus de collecte de preuves numériques devraient connaître les procédures à suivre (RIC, 2014, p. 17[1]).
- Intégrité et sécurité : les mesures prises par les autorités répressives, leurs employés ou leurs agents ne devraient pas avoir pour effet de modifier les données lors de leur obtention, de leur collecte et de leur analyse (US DoJ, 2004[2]) (APCO, 2012[3]). Les données doivent être préservées de telle manière qu'un tiers puisse reproduire les mêmes résultats que ceux présentés devant un tribunal (APCO, 2012, p. 7[3]).
- Obligation pour le personnel chargé de recueillir des preuves d'adopter des mesures de sécurité matérielle et numérique. Par exemple, il convient de travailler sur des copies des preuves originales pour éviter de détruire, d'endommager ou de modifier celles-ci (RIC, 2014, p. 23[1]). La personne qui accède aux données originales « doit être compétente et capable de fournir des preuves expliquant la pertinence et les implications de ses interventions » (APCO, 2012, p. 1[3]).
- Authenticité : l'authenticité des preuves tient à leur provenance et à leur véracité. Pour établir l'authenticité des preuves numériques, il est primordial de disposer d'une chaîne de la preuve[7] et d'une chaîne de conservation[8]. Le compte rendu des opérations relatives à la saisie, à l'examen, au stockage ou au transfert des preuves numériques doit être étayé, préservé et disponible pour faire l'objet d'un examen (US DoJ, 2004[2]). Le compte rendu de l'ensemble des procédures appliquées aux preuves numériques doit être accessible à un tiers indépendant pour lui permettre d'examiner les données originales en suivant les mêmes étapes et de parvenir aux mêmes conclusions (APCO, 2012[3]). Cela signifie que l'intégrité et la sécurité des données originales sont indispensables pour permettre leur reproduction et sont des éléments indissociables de leur authenticité.

15. Bien que ces principes soient énoncés expressément pour les opérations criminalistiques, ils sont fondés sur des règles relatives à l'admissibilité de la preuve et s'appliquent aussi à d'autres pratiques plus élémentaires de collecte de preuves numériques comme la recherche par mots-clés sur un compte de courrier électronique. Ces principes

aident les autorités de la concurrence à concevoir de meilleures pratiques pour leurs activités de collecte de preuves numériques.

3.2. Pratiques et méthodes

16. Les pratiques et méthodes d'inspection varient en fonction des juridictions pour un certain nombre de raisons tenant notamment aux sources disponibles (comme le matériel, les logiciels et le personnel qualifié) ou au cadre juridique. Certaines autorités de la concurrence ne peuvent pas collecter les preuves numériques stockées sur des téléphones portables ou réaliser des images disques (REC, 2013[4]). Dans ce cas, elles effectuent des recherches conceptuelles simples sur les supports qui font l'objet de l'inspection en utilisant des outils de recherche déjà installés. D'autres autorités de la concurrence ont recours à des outils et techniques d'investigation de pointe.

17. Cependant, tous les types d'inspections numériques comportent des étapes comme la planification, l'identification des sources de preuves numériques pertinentes, la collecte de preuves, la préservation des preuves pendant toutes les opérations, l'analyse des données et la présentation des preuves. La collecte, la préservation et l'analyse des informations numériques constituent toutefois les aspects les plus importants des inspections numériques réalisées par les autorités de la concurrence.

3.2.1. *Collecte*

18. La collecte de preuves numériques est au cœur des débats juridiques car il s'agit de l'élément le plus important de la gestion de ce type de preuves (Kasper et Laurits, 2016, p. 197[5]). Une erreur dans le traitement des données à ce stade risque d'entraîner la destruction des preuves ou leur irrecevabilité.

19. Dans le cadre des inspections inopinées, la collecte des données numériques se fait essentiellement suivant deux méthodes. La première méthode consiste en la saisie matérielle des supports de données comme les disques durs et les CD. Une recherche de preuves pertinentes est ensuite effectuée sur les éléments saisis dans les locaux de l'autorité concernée. À cette étape, il est possible d'extraire des données supprimées ou endommagées en ayant recours à des outils d'analyse criminalistique. Pendant le tri des preuves, seules les informations protégées en vertu du secret professionnel sont exclues de la procédure.

20. La deuxième méthode consiste à effectuer des recherches sur les supports de données dans les locaux de l'entreprise visitée et à réaliser des copies de fichiers ou des images disques des données numériques. Certaines autorités analysent aussi des systèmes allumés dans les locaux de l'entreprise[9] afin de pouvoir exploiter des données contenues dans la mémoire volatile auxquelles il n'est pas possible d'accéder lorsque l'appareil est éteint (RIC, 2014, pp. 10, 22[1]).

21. Les autorités de la concurrence n'ont pas toujours recours à des outils informatiques criminalistiques pour recueillir des preuves numériques. Elles inspectent alors les sources de preuves numériques au moyen d'outils de recherche préinstallés et récupèrent les données supprimées dans les « corbeilles » ou les serveurs de sauvegarde.

22. Au stade de la collecte, les équipes d'inspection peuvent prendre certaines mesures pour veiller à l'intégrité des données et permettre l'authentification. Par exemple, lorsque des images disques sont réalisées, des bloqueurs d'écriture sont utilisés pour assurer l'intégrité du support d'origine. Les valeurs de hachage[10] de toutes les copies de données numériques (fichier/image disque) sont générées pour permettre de vérifier si la copie est

identique aux données numériques originales. Il convient également de garder une trace de chaque mesure effectuée pendant cette procédure.

23. Après avoir recueilli les données numériques, certaines autorités de la concurrence les emportent dans leurs locaux (ou dans ceux de la police ou d'une autorité répressive équivalente) pour poursuivre les recherches. Cette opération est désignée « procédure de prolongation de l'inspection ». Certaines autorités trient les preuves numériques à première vue dans les locaux de l'entreprise visitée et poursuivent l'analyse dans leurs locaux. D'autres effectuent le tri complet des preuves numériques dans les locaux de l'entreprise (REC, 2013, pp. 3-4[4]) (REC, 2012, p. 14[6]). Dans ce cas, seule une sélection d'informations copiées est emportée dans les locaux de l'autorité de la concurrence pour que l'équipe chargée de l'affaire les examine (RIC, 2014, p. 10[1]). Dans certains pays, l'autorité de la concurrence utilise les deux procédures en fonction des particularités de l'affaire.

24. L'ECN (2012[6]) recommande de suivre une procédure de prolongation de l'inspection parce que celle-ci représente un moyen efficace de réunir des preuves numériques. Cette procédure donne plus de temps pour poursuivre la perquisition des données numériques et mieux comprendre l'affaire et, partant, accroît la possibilité de détecter des preuves pertinentes dans un dossier numérique souvent volumineux. Certains estiment toutefois que copier et emporter un volume considérable de données pour les examiner et les trier peut comporter un risque de violation de droits fondamentaux relatifs au respect de la vie privée et au secret professionnel (Michalek, 2015, p. 205[7]).

25. Le tri des données numériques dans les locaux de l'entreprise visitée comporte des avantages et des inconvénients. D'une part, cette procédure permet à l'entreprise d'invoquer immédiatement le droit au secret professionnel en ce qui concerne certaines informations. L'équipe chargée de l'affaire peut accéder aux données sélectionnées pendant un laps de temps relativement court. D'autre part, cette dernière ne peut pas examiner à nouveau le fichier/l'image disque de la source de la preuve numérique et « doit se contenter de la sélection effectuée dans les locaux de l'entreprise même si de nouveaux renseignements apparaissent pendant l'enquête » (RIC, 2014, p. 10[1]).

26. Au terme de la procédure de sélection des données, les informations numériques non pertinentes pour l'enquête sont soit retournées à l'entreprise, soit détruites définitivement (RIC, 2014, p. 21[1]).

3.2.2. *Préservation*

27. La préservation des preuves numériques consiste à en empêcher la suppression ou la destruction pendant leur inspection, leur transfert et leur analyse. Les mesures de préservation consistent à laisser les appareils allumés pour l'analyse sur systèmes allumés, à demander le blocage de l'accès aux boîtes de courrier électronique au niveau du serveur, à débrancher les câbles réseau afin d'empêcher l'accès et à protéger les supports de données de l'électricité statique, des champs magnétiques et des chocs. On l'a vu, l'exploitation des preuves numériques à partir de copies des données numériques est une mesure largement admise pour éviter d'endommager accidentellement les données numériques originales. Le maintien d'une chaîne de conservation solide jusqu'à la clôture de l'affaire est également primordial.

3.2.3. *Analyse*

28. L'analyse est l'étape au cours de laquelle les experts en criminalistique et/ou l'équipe d'enquête effectuent une analyse approfondie des données afin de trouver des éléments de preuve qui permettront d'élucider l'affaire qui fait l'objet de l'enquête.

L'analyse de chacune des données n'est pas un objectif réaliste. Étant donné que les perquisitions numériques peuvent concerner une grande masse de données, il convient de mettre au point une stratégie de perquisition. La recherche par mots-clés est la méthode la plus utilisée (RIC, 2014, p. 24[1]). Les mots-clés proviennent des recherches documentaires, des demandeurs de clémence, ou des explications sollicitées lors de l'inspection sur place. À mesure que progresse l'analyse, de nouveaux mots-clés peuvent s'ajouter à la liste. Un logiciel de recherche criminalistique spécialement mis au point peut identifier les versions incorrectement orthographiées des mots-clés et donner des résultats plus complets, et produire des résultats sur la base d'algorithmes d'auto-apprentissage.

29. D'autres méthodes d'analyse sont la confirmation de l'identité de l'utilisateur, l'examen du gestionnaire d'impression, l'examen des signatures des fichiers pour trouver des signatures erronées, la recherche d'informations cryptées, l'analyse des traces de chat en ligne, de messages web, etc. (RIC, 2014, pp. 24-25[1]). L'application de plusieurs de ces méthodes peut réduire le risque de faux négatifs.

30. L'absence notable de données numériques peut aussi se révéler utile pour l'analyse. Par exemple, la rareté ou l'absence de messages électroniques pendant une certaine période ou émanant d'un salarié donné (RIC, 2014, p. 25[1]) peut également être éclairante.

31. Encore une fois, il est important de garder une trace de toutes les mesures prises pour extraire les preuves de manière à conserver une chaîne de la preuve, afin de permettre à des tiers de reproduire les mêmes résultats.

4. Difficultés liées à la collecte de preuves numériques

32. Les inspections numériques transfèrent le contrôle exercé sur un immense volume de données des entreprises aux autorités de la concurrence et la technologie utilisée par les parties qui font l'objet des inspections et les autorités de la concurrence évoluent sans cesse. Cela crée des difficultés techniques et pratiques pour les autorités de la concurrence, comme on le verra dans la présente section.

4.1. Pouvoir et capacité de réunir des preuves numériques

33. La collecte de preuves numériques doit avoir un fondement juridique. Lorsque les critères juridiques sont satisfaits, les autorités de la concurrence doivent également avoir la capacité technique d'effectuer des inspections numériques.

4.1.1. *Légalité*

34. Les autorités de la concurrence ne peuvent pas collecter des preuves numériques sans fondement juridique. À l'heure actuelle, le pouvoir de collecter des preuves numériques conféré à la quasi-totalité des autorités de la concurrence découle de celui, déjà existant, d'examiner tous les livres et documents de l'entreprise visitée (RIC, 2014, p. 26[1]). L'interprétation habituelle est qu'indépendamment de leur forme, toutes les informations qui se trouvent dans les locaux de l'entreprise sont sujettes à inspection.

35. La capacité de réaliser des perquisitions numériques n'est pas illimité. Comme l'inspection inopinée de preuves matérielles, une inspection numérique doit être proportionnée et demeurer dans le champ de l'enquête pour être licite. Cependant, les méthodes et procédures appliquées dans le cadre des perquisitions numériques peuvent soulever des questions particulières s'agissant de l'interprétation de ces limites.

36. La saisie de disques durs en vue d'une perquisition ultérieure ou la copie quasi-intégrale du serveur de l'entreprise peuvent entraîner la saisie imprévue d'informations qui n'entrent pas dans le champ légitime de la décision ou du mandat d'inspection. Dans certains pays, cette pratique peut soulever, s'agissant du principe de proportionnalité, des préoccupations que les autorités de la concurrence cherchent à atténuer en utilisant des outils de recherche et des mots-clés permettant d'assurer que seules seront saisies les données ayant un lien raisonnable avec l'enquête. En effet, il pourrait être considéré que l'autorité de la concurrence va au-delà de ce qui est nécessaire et raisonnable pour atteindre son objectif légitime.

37. La question de la pertinence se pose également lorsqu'un outil de recherche est utilisé pour savoir quelles données seront copiées. Certains estiment que les mots-clés recherchés ne doivent pas être trop généraux afin d'assurer que seuls les résultats entrant dans le champ de l'inspection soient générés (Lang, 2014[8]) (Polley, 2013[9]). Sinon, on pourrait craindre que les inspections se transforment en « pêche aux renseignements ». Une autre préoccupation est que des perquisitions numériques trop intrusives accroissent le risque d'utilisation illicite des informations obtenues par hasard sous prétexte que ces informations ont été traitées seulement comme des « renseignements » et non comme des preuves (Michalek, 2015, p. 205[7]).

38. Des garanties procédurales solides peuvent atténuer les préoccupations relatives à la proportionnalité et à la pertinence. Un contrôle judiciaire qui remplit une authentique fonction de surveillance peut protéger efficacement les droits des parties faisant l'objet d'une inspection. Dans certains pays comme l'Allemagne, les États-Unis et l'Inde, les inspections inopinées donnent lieu à un contrôle judiciaire préalable. Si rigoureux que soit le contrôle judiciaire préalable, le contrôle judiciaire a posteriori est indispensable. Celui-ci peut être réalisé de manière indépendante ou rétroactive, ce qui signifie que les décisions procédurales peuvent être examinées seulement dans le cadre d'une décision définitive concernant l'affaire. L'absence de contrôle judiciaire indépendant des inspections inopinées est critiquée parce que cela pourrait priver la partie qui fait l'objet de l'inspection d'une mesure corrective appropriée (Jalabert-Doury, 2009, p. 8[10]) (Michalek, 2015, p. 208[7]).[11]

39. Un autre problème juridique est souvent soulevé s'agissant du droit du représentant de l'entreprise d'assister aux perquisitions subséquentes des données copiées. Dans certains pays comme l'Autriche, le tri des données contenues dans les copies de fichiers ou les images disques intervient dans les locaux de l'autorité de la concurrence sans que les représentants des parties qui font l'objet de l'inspection ne soient présents. Dans d'autres pays ou juridictions (par exemple le Danemark, les Pays-Bas ou l'UE), les représentants de la partie qui fait l'objet de l'inspection sont invités à assister à l'inspection ultérieure des données contenues dans les copies de fichiers ou les images disques (Jalabert-Doury, 2009[10]). Pour faciliter la surveillance de la prolongation de l'inspection par la partie qui fait l'objet de l'inspection, une liste de mots-clés utilisés lors de l'analyse des données ou encore une copie des preuves sélectionnées peuvent être fournies. Néanmoins, certains auteurs critiquent la procédure de prolongation de l'inspection parce qu'ils estiment que sa surveillance peut imposer un lourd fardeau aux entreprises dont les ressources sont limitées (Simonsson, 2013, pp. 10-11[11]), et préconisent que celles-ci aient réellement le choix du lieu de l'inspection (Michalek, 2015, p. 210[7]).

Encadré 1. Preuves découvertes par hasard

Les preuves découvertes par hasard sont « tout élément de preuve recueilli fortuitement au cours d'une inspection et concernant des violations présumées des règles de concurrence non prises en compte dans la décision d'inspection initiale » (REC, 2013, p. 20[4]). Dans plusieurs pays ou juridictions, l'autorité de la concurrence peut obtenir ou saisir des preuves découvertes par hasard lors d'une inspection tandis que dans d'autres, il lui faut une nouvelle autorisation pour inspecter. Par exemple, la Cour de justice de l'Union européenne a estimé que la Commission européenne ne peut pas saisir ou copier intentionnellement des preuves sortant du champ de l'inspection[12] mais peut « ouvrir une procédure d'enquête [distincte] afin de vérifier l'exactitude ou compléter des informations dont elle aurait eu incidemment connaissance au cours d'une vérification antérieure au cas où ces informations indiqueraient l'existence de comportements contraires aux règles de concurrence (…) »[13]. L'Autorité hongroise de la concurrence (GHV)[14] peut saisir des preuves découvertes par hasard et demander ensuite une autorisation des instances judiciaires. En 2007, le tribunal d'appel de Budapest a maintenu une décision de violation rendue par la GVH et conclu que celle-ci avait « utilisé licitement les preuves qu'elle avait obtenues dans le cadre d'une autre procédure »[15].

Étant donné que les perquisitions numériques permettent d'accéder à une grande quantité d'informations pendant les inspections inopinées, la question des preuves découvertes fortuitement est sans doute appelée à se poser plus souvent. La décision du tribunal de commerce suédois sur les preuves découvertes fortuitement dans le cadre d'inspections numériques en est une illustration. En novembre 2013, l'Autorité suédoise de la concurrence (KKV) a ouvert une enquête d'office sur le comportement de la société ASSA sur le marché suédois des services de serrurerie en gros. La KKV a mené une inspection dans les locaux de deux filiales du groupe ASSA ALBOY (groupe ASSA) et a saisi des copies d'informations numériques avec le consentement de la partie qui faisait l'objet de l'enquête[16] afin d'examiner les données plus en détail dans ses propres locaux.

Au cours de l'analyse, la KKV a pris connaissance par hasard d'une autre infraction possible qui sortait du mandat d'inspection initial et a donc demandé au tribunal de district de Stockholm l'autorisation d'élargir la perquisition aux données déjà recueillies, autorisation que le tribunal lui a accordée en mars 2014. Le groupe ASSA a fait appel auprès du tribunal suédois du commerce en faisant valoir que la demande de la KKV n'était pas étayée par la législation et que le consentement d'ASSA à la saisie des données électroniques était limité au champ initial du mandat.

La KKV a affirmé que le consentement d'ASSA portait simplement sur le lieu où devait se tenir la perquisition et que cela n'affecterait pas le champ de cette dernière. Elle a également fait valoir que les informations découvertes fortuitement pourraient former la base d'une demande de perquisition dans le cadre d'une enquête distincte et qu'il est plus efficace d'examiner des données déjà saisies que de lancer une nouvelle inspection ou d'envoyer une demande de renseignements. La KKV a souligné que les représentants de l'entreprise pourraient assister à la poursuite de l'examen qui se devait se dérouler dans les locaux de la KKV. La KKV a également fait état de la difficulté qu'il y a à recueillir des informations permettant de justifier une prolongation de la perquisition et soutenu que l'entreprise ASSA avait déjà dissimulé des informations cruciales pendant une affaire de fusion en 2013 et que le risque de dissimulation était encore présent dans l'affaire en cours. De ce fait, si une nouvelle inspection devait être menée, il était essentiel que la KKV soit en mesure de recouper les informations avec les données déjà saisies.

En 2015, le tribunal de commerce a estimé que la prolongation de la perquisition des données saisies n'était pas justifiée juridiquement puisque la Loi suédoise sur la concurrence mentionne des inspections « dans les locaux des entreprises » et que le pouvoir de la KKV de transférer des copies de données électroniques dans ses propres locaux n'était pas établi avec certitude. Le tribunal a estimé que le consentement à la saisie des données n'équivalait pas à donner carte blanche à KKV pour perquisitionner à son gré mais était plutôt limité au champ particulier de l'inspection. Aux termes de la Loi suédoise sur la concurrence, une inspection sur place est autorisée lorsque des solutions moins fastidieuses ne sont pas viables et qu'il existe des risques de dissimulation ou de falsification des éléments de preuve.

Le tribunal a également décidé que l'affaire ne satisfaisait pas à ces conditions préalables car le KKV demandait l'autorisation d'examiner plus en détail des preuves numériques qu'elle détenait déjà et sur lesquelles ASSA n'exerçait plus de contrôle.

Sources : Suspected anti-competitive conduct – investigation related to the market for locksmith wholesale services, communiqué de presse de KKV, http://www.konkurrensverket.se/globalassets/english/competition/13-0494-english.pdf.
Setback for Electronic Searching by Swedish Competition Authority, https://www.nordiccompetitionblog.com/?p=494.

4.1.2. *Capacités*

40. La réalisation d'inspections numériques nécessite du personnel spécialisé et des locaux spéciaux pour l'analyse et la préservation des données numériques, ainsi que du matériel technique et des logiciels. Au fil des progrès technologiques, ces capacités doivent constamment être mise à jour et améliorés.

41. Il est recommandé de disposer en interne d'un service ou d'un groupe en mesure de réaliser la collecte de preuves numériques. Les autorités de la concurrence, du fait de leurs ressources limitées ou pour d'autres raisons, peuvent également estimer qu'il est plus simple de sous-traiter la collecte de preuves numériques à d'autres organismes publics ayant déjà développé ces capacités. Dans ce cas, la conclusion entre l'autorité de la concurrence et l'autre organisme public d'un protocole d'accord dans lequel sont décrites l'étendue et la nature de la coopération constitue une bonne pratique (RIC, 2014, pp. 12-14[1]).

42. La création et le maintien d'une capacité de collecte de preuves numériques au cours des inspections inopinées peut exercer une pression considérable sur les ressources humaines et financières des organismes publics. Les coûts élevés représentent parfois le principal obstacle à la création de capacités. Le développement de logiciels *open source* et la coopération entre autorités de la concurrence à des fins de formation peuvent aider celles-ci à surmonter certaines de ces difficultés[17].

4.2. Informations protégées

43. Dans de nombreuses juridictions, la conséquence directe du droit à une défense et à un procès équitable est que certains éléments d'information sont considérés comme protégés et ne peuvent pas être communiqués à des tiers, y compris à des autorités publiques. Le secret professionnel de l'avocat oblige notamment celui-ci à respecter la confidentialité des informations qu'il échange avec son client dans le cadre de son activité de conseil juridique. Le secret professionnel de l'avocat n'est pas seulement une règle de preuve mais protège également les communications confidentielles de la saisie ou du contrôle par des tiers sans l'assentiment du client (OCDE, 2018[12]). Les méthodes d'inspection numérique comme la réalisation d'images disques ou de copies d'un support numérique dans son intégralité, ou la saisie d'une quantité non vérifiée de données numériques originales, pourraient donc constituer une violation des règles relatives au secret professionnel.

44. Au cours des perquisitions physiques réalisées dans le cadre d'inspections inopinées, les représentants de la partie qui fait l'objet de l'inspection peuvent facilement invoquer le secret professionnel et, par conséquent, éviter la copie, la saisie et l'examen du document. Cela est impossible pour des données stockées sur un support saisi ou copié intégralement depuis des serveurs. Même si, au bout d'un certain temps, le secret

professionnel peut être invoqué pour une partie des données, des informations protégées seront temporairement copiées ou saisies.

45. Les informations protégées peuvent être identifiées au moyen des mêmes outils criminalistiques que pour la perquisition des données. Cela permet d'assurer que le logiciel identifie les documents considérés comme « protégés » et que tous les documents électroniques soient ensuite traités comme le seraient des documents papier afin d'établir leurs caractéristiques juridiques. Il est également suggéré que la partie qui fait l'objet de l'inspection puisse fournir des mots-clés à rechercher en regard des données indexées pour détecter les documents protégés (Polley, 2013, p. 22[9]) ou encore que les noms des conseils juridiques soient exclus des mots-clés utilisés par l'équipe d'inspection (Lang, 2014, p. 15[8]).

4.3. Respect de la vie privée et protection des données

46. La collecte de preuves numériques peut aussi avoir pour effet de porter atteinte aux droits au respect de la vie privée des salariés des entreprises visitées ainsi que de tierces parties. On l'a vu, l'exploitation de très grandes quantités de données avec des outils numériques comporte le risque d'inclure des données protégés par la législation relative à la protection de la vie privée. Ce risque est accru par les politiques du type « apportez vos appareils personnels » (*bring your own device* (BYOD)) en vertu desquelles les salariés peuvent utiliser des appareils personnels comme leurs smartphones et leurs tablettes au travail et à des fins professionnelles. Cela peut rendre difficile le repérage des supports numériques qui doivent être ciblés dans le cadre des inspections et, plus encore, le tri entre les données à caractère privé et celles qui se rapportent à l'entreprise.

Encadré 2. Inspection d'appareils mobiles personnels – Affaire intervenue en Espagne

En 2016, l'Autorité nationale des marchés et de la concurrence (CNMC) a imposé des amendes à six fabricants de nougat qui, entre 2011 et 2013, s'étaient mis d'accord pour se partager le marché du nougat blanc en Espagne. Pendant le déroulement de cette affaire, la CNMC a effectué, en 2013, une inspection dans les locaux de Almendra y Miel SA. L'entreprise a fait appel de la décision auprès de la *Audiencia Nacional* au motif notamment qu'il y avait eu atteinte aux droits à la vie privée et à la liberté informatique (*libertad informatica*). L'entreprise faisait valoir que la CNMC avait violé ces droits lorsqu'elle a collecté des informations confidentielles et personnelles stockées sur le téléphone portable de son salarié, M. Claudio. Selon l'entreprise, l'accès à ces données, en particulier aux enregistrements de conversations téléphoniques et aux documents graphiques stockés sur le téléphone portable de ce dernier, n'était ni autorisé ni pertinent pour les besoins de l'enquête de la CNMC.

Le 18 juillet 2016, la *Audiencia Nacional* a décidé que les documents personnels sans rapport avec l'activité de l'entreprise devaient être exclus de l'enquête. Elle a toutefois estimé que la consultation rapide des documents recueillis pour établir s'ils étaient privés ou non n'avait pas porté atteinte au droit à la vie privée. La décision précise que la demande d'enquête permettait aux enquêteurs d'accéder aux agendas papier et électroniques des salariés de l'entreprise, y compris ceux qui se trouvaient sur leurs téléphones portables.

La *Audiencia Nacional* a également estimé que malgré la plainte de M. Claudio concernant la saisie non autorisée de son téléphone et l'examen de son contenu en son absence, l'inspection s'était déroulée correctement. La décision explique que selon le compte rendu de l'inspection, M. Claudio était présent et a demandé d'extraire des documents personnels ou protégés par le secret professionnel des avocats. Une fois ces documents mis de côté, l'inspection des autres documents (y compris du téléphone) a eu lieu dans une autre pièce sans que les salariés de l'entreprise ne soient présents. La décision souligne que l'entreprise avait signé le compte rendu de l'inspection sans protester.

L'inspection des conversations téléphoniques archivées sur le téléphone de M. Claudio n'a pas été considérée comme une atteinte à la liberté informatique. Selon la décision, rien ne prouve que ses données personnelles aient été utilisées à des fins autres que celles, légitimes, qui en justifiaient l'obtention. La décision souligne enfin que les documents contestés n'avaient pas été versés au dossier d'enquête à la fin des procédures.

Sources : Décision de la *Audiencia Nacional* datée du 18 juillet 2016, D. Claudio, Almendra y Miel SA y Confectionary Holding SL v CNMC, No 136/2014, ES:AN:2016:2986.
http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7784395&links=&optimize=20160805&publicinterface=true
Employee's mobile phones not safe from dawn raid scrutiny, Spanish court finds, http://competitionlawblog.kluwercompetitionlaw.com/2016/09/16/employees-mobile-phones-not-safe-from-dawn-raid-scrutiny-spanish-court-finds/

47. Dans certains pays, la collecte et l'exploitation des données personnelles sont régies par les règles relatives à la protection des données. Selon le niveau de protection assuré par la législation et la réglementation, il se peut que les autorités de la concurrence doivent adapter le déroulement des opérations, leurs procédures et les méthodes suivies pour effectuer des inspections inopinées en fonction des règles de protection des données. Par exemple, il se peut que l'autorité de la concurrence soit tenue d'informer le salarié concerné de l'entreprise visitée sur ses droits, l'objectif de l'exploitation des données (par exemple, de l'extraction des données depuis un disque dur ou du blocage de l'accès à une boîte de messagerie) et sur le destinataire des données personnelles. Une autre difficulté à laquelle sont confrontées les autorités de la concurrence est liée par exemple aux droits des personnes concernées aux termes des dispositions applicables à la protection des données, par exemple le droit de demander d'accéder à leurs données à caractère personnel, de faire rectifier ces données ou de s'opposer à leur exploitation (Kuschewsky et Geradin, 2014[13]). Soulignons toutefois que les règles et principes de protection des données ne sont pas totalement inconnus des autorités de la concurrence car en général, les principes de légalité, de proportionnalité et de sécurité auxquels elles souscrivent déjà contribuent dans une large mesure au respect des objectifs de protection des données.

4.4. Lieu de stockage des informations numériques

48. Dans le monde numérique, les données ne sont pas forcément stockées dans les locaux depuis lesquels elles sont accessibles. Au contraire, à mesure que se généralisent de nouveaux services fondés sur le modèle serveur-client ou le nuage, les espaces de stockage ne se trouvent plus au point d'accès. C'est pourquoi les équipes d'inspection détectent et consultent souvent des données stockées dans des serveurs situés (i) dans d'autres locaux appartenant à l'entreprise visitée, à une autre adresse ; (ii) dans les locaux d'une autre partie ; (iii) à l'extérieur du pays dans lequel l'autorité de la concurrence exerce ses compétences (RIC, 2014, p. 28[1]).

49. De nombreuses autorités de la concurrence adoptent une approche fondée sur l'accès aux données. Selon cette approche, dans la mesure où l'entreprise a accès aux données, les contrôle et les utilise depuis les locaux inspectés, celles-ci sont considérées comme étant susceptibles de faire l'objet d'une inspection numérique. Dans ce cas, aucun des lieux de stockage mentionnés ci-dessus ne représente un obstacle à la copie et à l'examen des données[18].

50. Il est également possible de retenir une approche fondée sur la localisation selon laquelle l'autorité de la concurrence ne peut perquisitionner que les données numériques stockées sur le territoire relevant de sa compétence ou sur lequel elle y est autorisée. Si l'approche en fonction de la localisation est acceptée, l'autorité de la concurrence doit obtenir une décision d'inspection ou un mandat judiciaire qui englobe les locaux des tiers qui abritent les serveurs ou les données. Lorsque les serveurs sont situés à l'extérieur du territoire du pays concerné, l'autorité de la concurrence doit s'en remettre à la coopération internationale sur une base ponctuelle ou par le biais de conventions d'entraide judiciaire.

51. En ce sens, l'approche fondée sur la localisation place les autorités de la concurrence dans une situation très délicate. Premièrement, il est parfois très difficile de déterminer où se trouvent les serveurs ou les autres espaces de stockage de données au stade de la planification d'une inspection. Si la localisation des serveurs n'est trouvée qu'au cours de l'inspection, de nouveaux documents juridiques doivent être émis immédiatement étant donné que les preuves numériques seront compromises jusqu'à ce que l'équipe d'inspection puisse obtenir les données numériques. En outre, il semble que la coopération internationale et l'entraide judiciaire prévue par des conventions, qui sont lentes à obtenir, soient des solutions peu réalistes étant donné que les inspections inopinées ont généralement pour but de tirer parti de la surprise et que les éléments de preuve peuvent être perdus entretemps. Enfin, en cas de stockage en nuage, les données sont stockées dans des endroits inconnus sur internet. Une approche rigoureusement fondée sur la localisation peut donc avoir pour effet de mettre les données stockées en nuage à l'abri des inspections.

4.5. Transparence

52. Les inspections numériques constituent un phénomène assez nouveau dans le domaine des inspections inopinées. Les outils et les procédures utilisés pour effectuer les perquisitions numériques sont également appelés à être modifiés à mesure que la technologie se développe et que l'expérience s'étoffe. Bien que de plus en plus d'autorités de la concurrence collectent et analysent des données numériques, les entreprises ne savent pas toujours en quoi consistent ces opérations.

53. La transparence profite généralement à toutes les parties aux procédures. Elle revêt une importance particulière pour les autorités de la concurrence car elle est une composante essentielle d'une enquête efficace et efficiente. La transparence améliore la collecte de preuves en encourageant la coopération entre les parties et l'autorité de la concurrence et en accélérant la procédure (OCDE, 2010, p. 9[14]) (RIC, 2013, p. 4[15]).

54. S'agissant des inspections inopinées de données numériques, les autorités de la concurrence doivent évaluer attentivement les avantages et les inconvénients de la transparence ainsi que le niveau recherché de transparence. D'une part, le fait d'informer les parties qui font l'objet d'une inspection sur ce qui est recherché peut faciliter la coopération et assurer que l'inspection numérique soit rapide, précise et approfondie. Un niveau élevé de transparence sur les procédure de collecte de preuves numériques contribue à la cohérence et à l'équité de ces procédures.

55. D'autre part, les autorités de la concurrence peuvent craindre qu'une connaissance trop précise des méthodes et objectifs de collecte de données numériques ne compromette la réussite d'une inspection inopinée en facilitant la destruction des preuves numériques ou en contribuant à en bloquer l'accès. En termes de procédures, la transparence peut priver l'autorité de la concurrence d'une certaine souplesse en matière de collecte de données numériques (RIC, 2014, pp. 30-31[1]). Certaines autorités de la concurrence ont déjà publié

des lignes directrices dans lesquelles elles présentent leur approche en matière de preuves numériques[19], tandis que d'autres souhaitent acquérir un certain niveau d'expérience et attendre les orietentations des tribunaux avant de publier des documents explicatifs.

5. Conclusion

56. La transformation numérique avance à un rythme très rapide. Dans un environnement où les informations sont dans leur quasi-totalité produites, traitées ou stockées sur support numérique, les inspections inopinées ne peuvent pas être efficaces sans collecte de preuves numériques.

57. Il existe des principes fondés sur le droit de la preuve et les règles de l'investigation en ce qui concerne les inspections numériques. Ces principes peuvent être regroupés sous quatre rubriques : légalité, compétence, intégrité et sécurité, et authenticité. C'est sur la base de ces principes que les autorités doivent définir leurs procédures et leurs méthodes.

58. Les pratiques de collecte de preuves numériques varient selon les autorités de la concurrence concernées. Comme ces pratiques sont relativement nouvelles, la jurisprudence et l'expérience ne suffisent pas encore pour répondre à toutes les questions qui pourraient se poser. En outre, la pratique varie considérablement selon les juridictions. Certaines difficultés sont toutefois communes à l'ensemble des autorités de la concurrence : la définition du fondement juridique approprié pour la collecte de preuves numériques ; la mise en place des capacités ; la proportionnalité dans les perquisitions numériques ; la protection des données confidentielles et personnelles ; l'accès aux informations stockées à l'extérieur de la juridiction de l'autorité de la concurrence concernée ; et la question de la transparence.

Notes

[1] https://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf

[2] https://www.radicati.com/wp/wp-content/uploads/2017/12/Email-Statistics-Report-2018-2022-Executive-Summary.pdf

[3] https://www.radicati.com/wp/wp-content/uploads/2015/02/Instant-Messaging-Market-2014-2018-Executive-Summary.pdf

[4] https://www.radicati.com/wp/wp-content/uploads/2017/12/Instant-Messaging-Statistics-Report-2018-2022-Executive-Summary.pdf

[5] Voir OCDE (2013[16]) pour un aperçu des inspections inopinées.

[6] Communication de l'Autorité britannique de la concurrence et des marchés (UK CMA) lors de l'atelier organisé par l'OCDE sur le filtrage des ententes à l'ère numérique le 30 janvier 2018, https://www.slideshare.net/OECD-DAF/cartel-screening-in-the-digital-era-uk-competition-markets-authority-january-2018-oecd-workshop.

[7] La chaîne de la preuve contient des éléments relatifs à la saisie, à l'analyse et aux autres procédures d'obtention de preuves numériques et atteste que les preuves proviennent incontestablement des informations numériques saisies (RIC, 2014, p. 5[1]).

[8] La chaîne de conservation est le registre contenant l'historique de conservation des preuves numériques, et qui atteste leur provenance (RIC, 2014, p. 5[1]).

[9] L'exploitation de systèmes allumés consiste à saisir ou analyser des informations numériques, des contenus de mémoire et/ou des contenus de supports de données se trouvant sur des systèmes allumés (systèmes en fonctionnement). Cette action extrait des informations contenues dans la mémoire vive (ces informations sont perdues lorsque l'appareil ou les systèmes sont éteints). (RIC, 2014, p. 6[1])

[10] Une valeur de hachage est une valeur numérique unique qui identifie des données comme une empreinte digitale numérique. Elle est produite par des algorithmes mathématiques. Les données ne peuvent pas être modifiées sans que soit également modifiée la valeur de hachage correspondante. (RIC, 2014, p. 6[1])

[11] Un contrôle judiciaire indépendant peut également comporter certains inconvénients, comme le fait qu'il ne possède pas la précision accrue d'un contrôle rétrospectif et prolonge la durée totale des procédures (Simonsson, 2013, p. 13[11]).

[12] Arrêt de la Cour de justice de l'Union européenne, Deutsche Bahn AG e.a. contre Commission européenne, affaire 583/13, EU:C:2015:404, par. 61-68, http://curia.europa.eu/juris/document/document.jsf?text=&docid=165109&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1238484

[13] Arrêt de la cour de justice de l'Union européenne, Dow Benelux contre Commission, affaire 85/87, EU:C:1989:379, par. 19, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A61987CJ0085.

[14] Anti-Cartel Enforcement Template – Hungary, p. 21, http://www.gvh.hu/data/cms1032890/HUN_Cartel_Template_with_settlement_2016_02_01_final.pdf

[15] Communiqué de presse de l'Autorité hongroise de la concurrence, http://www.gvh.hu/en/press_room/press_releases/press_releases_2007/4853_en_gvhs_winning_the_motorway_cartel_case_became_final.html

[16] En vertu de la Loi suédoise sur la concurrence, la KKV ne peut emporter des données numériques dans ses locaux pour les examiner que si la partie qui fait l'objet de l'examen y consent.

[17] Selon l'ICN, (2014, p. 14[1]), il est recommandé d'établir un budget annuel spécial et une planification financière pluriannuelle pour l'achat et la maintenance de l'équipement et des logiciels ainsi que pour la formation du personnel.

[18] Voir Polley (2013[9]) pour une critique de l'approche fondée sur l'accès.

[19] Par exemple, l'Autorité néerlandaise de la consommation et des marchés financiers a publié en 2003 le document « AMC Procedure for the inspection of digital data » et l'a mis à jour en 2014. https://www.acm.nl/sites/default/files/old_publication/publicaties/12772_2014-acm-procedure-for-the-inspection-of-digital-data-2014-02-06.pdf

L'UE a publié une note explicative sur l'autorisation d'effectuer une inspection en exécution d'une décision prise en vertu de l'article 20, paragraphe 4, du règlement nº 1/2003 qui fournit également des orientations sur les inspections numériques : http://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf

L'Autorité fédérale autrichienne de la concurrence a publié un document sur les perquisitions à l'aube intitulé « *Guidance on dawnraids* » et qui comprend une section sur la collecte de données électroniques : https://www.bwb.gv.at/fileadmin/user_upload/Downloads/standpunkte/Guidance_on_dawn_raids_final.pdf

References

APCO (2012), *ACPO Good Practice Guide for Digital Evidence*, https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. [3]

Jalabert-Doury, N. (2009), « Digital evidence searches in competition investigations: Best Practices for effective fundametal rights », *Concurrences*, vol. 4, https://www.concurrences.com/en/review/issues/no-4-2009/articles/Digital-evidence-searches-in-29118. [10]

Tanel Kerikmä, A. (dir. pub.) (2016), *Challenges in Collecting Digital Evidence: A Legal Perspective*, Springer. [5]

Kuschewsky, M. et D. Geradin (2014), « Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges », *World Competition*, vol. 37/1, pp. 69-102, https://www.kluwerlawonline.com/abstract.php?area=Journals&id=WOCO2014005. [13]

Lang, J. (2014), « Legal problems of digital evidence », *Journal of Antitrust Enforcement*, vol. 2/1, pp. 1-25, https://doi.org/10.1093/jaenfo/jnt007. [8]

Michalek, M. (2015), *Right to Defence in EU Competition Law: The case of Inspections*, University of Warsaw, Faculty of Management Press. [7]

OCDE (2018), *Treatment of Legally Privileged Information in Compeititon Proceedings*. [12]

OCDE (2013), *Unannounced Inspections in Antirtust Investigations*, https://one.oecd.org/document/DAF/COMP/LACF(2013)6/en/pdf. [16]

OCDE (2010), *Procedural Fairness: Transparency Issues in Civil and Administrative Enforcement Proceedings*, http://www.oecd.org/daf/competition/mergers/48825133.pdf. [14]

Polley, R. (2013), *Digital Evidence Gathering in Dawn Raids - a Risk for the Compay's Rights of Defence and Fundamental Rights*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2355033. [9]

REC (2013), *ECN Recommendation on the Power to Collect Digital Evidence, Including by Forensic Means*, http://ec.europa.eu/competition/ecn/ecn_recommendation_09122013_digital_evidence_en.pdf . [4]

REC (2012), *Investigative Powers Report*, http://ec.europa.eu/competition/ecn/investigative_powers_report_en.pdf. [6]

RIC (2014), *Chapter on Digital Evidence Gathering*, http://www.internationalcompetitionnetwork.org/uploads/library/doc1006.pdf. [1]

RIC (2013), *Competition Agency Transparency Practices*, http://internationalcompetitionnetwork.org/uploads/library/doc902.pdf. [15]

Simonsson, I. (2013), *Digital Evidence Gathering in Dawn raids. Judicial Review: Up-Front or Retrospective*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327122. [11]

US DoJ (2004), *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf. [2]