contrast

La perquisition débute toujours à l'aube, mais elle est aujourd'hui numérique. Le digital dawn raid.

Imaginez...

Vous êtes le CEO d'une entreprise qui conçoit et installe des systèmes professionnels de sonorisation et d'éclairage pour les festivals de musique et les événements en direct. Au printemps, tout s'accélère. Les contrats sont signés, les équipes sont programmées, l'équipement est testé. Après des mois de préparation, la saison des festivals est sur le point de commencer.

Tout va bien... et puis un matin, alors que votre journée vient à peine de commencer, votre réceptionniste vous demande de vous présenter immédiatement à la réception.

Des agents de police sont là, ainsi que des fonctionnaires d'une autorité de concurrence. Ils vous remettent un mandat de perquisition et vous expliquent qu'ils procèdent à une inspection inopinée dans le cadre d'une enquête de concurrence.

Vous commencez à parcourir la première page et vous sentez monter une petite panique : ce n'est pas possible. Avant même d'avoir terminé le deuxième paragraphe, les questions fusent : pouvez-vous nous expliquer comment fonctionne votre environnement informatique ? Pouvez-vous nous autoriser à y accéder ? Les employés utilisent-ils des appareils personnels dans le cadre de leurs activités ? Un autre enquêteur fait état d'une obligation de procéder à un obscur 'legal hold'.

Vous tentez d'y voir clair et d'établir une checklist, mais cet exercice ne clarifie guère les choses. Au

contraire, il soulève de nouvelles questions : Qui faut-il appeler en premier ? Qui maitrise notre environnement informatique et qui peut en autoriser l'accès ?

Comment cela fonctionne-t-il exactement et que devez-vous faire maintenant ?

Quelques précisions.

L'une des tâches essentielles de toute autorité de concurrence est de rechercher les cas de non-respect des règles du droit de la concurrence et, le cas échéant, de constater les infractions, d'en ordonner la cessation et d'imposer des sanctions. Le principal outil à la disposition des autorités à cette fin est ce que l'on appelle le "*dawn raid*" : une inspection inopinée (ou perquisition) visant à déterminer si de sérieux soupçons de comportement anticoncurrentiel sont fondés. Ces soupçons découlent souvent de plaintes ou de demandes de clémence. Une autorité peut également ouvrir une enquête de sa propre initiative. Par exemple, l'Autorité Belge de la Concurrence a récemment effectué des perquisitions dans le secteur de la signalisation routière et du mobilier urbain de sa propre initiative, sur la base d'un examen d'informations publiques.

Ce n'est pas seulement la manière dont les perquisitions sont déclenchées qui s'est numérisée, mais aussi la manière dont elles sont menées. Alors qu'autrefois les perquisitions consistaient principalement à fouiller des classeurs, des dossiers physiques et des voitures de fonction, les perquisitions d'aujourd'hui sont essentiellement numériques.

Les inspecteurs peuvent examiner l'ensemble de l'environnement informatique d'une entreprise, y compris les données sur le cloud, celles stockées sur les serveurs, sur les ordinateurs de bureau, les ordinateurs portables, les tablettes et autres appareils mobiles, même lorsqu'il s'agit d'appareils privés utilisés à des fins professionnelles (BYOD). Cela inclut l'accès aux communications professionnelles telles que les courriels, les plateformes de collaboration et de messagerie, ainsi que les chatbots d'IA.

Une recherche numérique n'est pas un exercice superficiel. Les inspecteurs utilisent des outils informatiques de police scientifique pour effectuer des recherches par mots-clés dans de vastes ensembles de données et créer des copies numériques des données électroniques en vue d'un examen ultérieur, souvent dans les locaux de l'autorité.

Les entreprises ont le devoir de coopérer pleinement aux *dawn raids*. Refuser de coopérer, ou ne le faire que partiellement, peut avoir de graves conséquences. Dans la pratique, l'informatique se retrouve souvent au centre de la perquisition. Les équipes informatiques de l'entreprise perquisitionnée peuvent être invitées à expliquer comment les systèmes et les flux de données sont organisés, ou à exécuter des demandes techniques spécifiques, telles que le blocage temporaire de comptes d'utilisateurs individuels, la déconnexion temporaire d'ordinateurs du réseau ou la fourniture d'une assistance en matière de droits d'accès «?administrateur?».

Le message est clair : une perquisition moderne est à la fois une question juridique et une question informatique.

Concrètement

- **La préparation est cruciale**. Assurez-vous d'avoir mis en place un protocole de *dawn raid* actualisé. Incluez-y une section informatique détaillée qui, entre autres, cartographie les systèmes clés et les

emplacements des données (sur site et dans le cloud), identifie les personnes autorisées à accorder des droits d'accès et explique comment fonctionnent les 'legal hold' qui garantissent qu'aucune donnée ne puisse être supprimée ou modifiée) et les exportations de données. Une chose est sûre : vous ne voulez pas vous retrouvez à tenter de résoudre ces problèmes le jour d'un *dawn raid*. Formez votre personnel informatique.

- **Réagissez calmement et immédiatement à l'arrivée des inspecteurs**. Demandez à lire le mandat de perquisition. Vérifiez l'identité des inspecteurs, de même que l'objet précis et la portée de l'enquête. Demandez une assistance juridique et impliquez immédiatement le membre du personnel informatique responsable.
- **Évitez toute obstruction du *dawn raid***. Coopérez pleinement et professionnellement. Vous ne devez en aucun cas déplacer, dissimuler, retirer ou effacer des documents ou des données. Sachez qu'une obstruction peut également résulter de problèmes techniques : l'exécution tardive, incorrecte ou non-coordonnée d'injonctions informatiques formulées durant une perquisition peuvent être qualifiées d'obstruction. La Commission européenne a déjà infligé plus de 2,5 millions d'euros d'amendes à une entreprise perquisitionnée qui s'était abstenue de bloquer une adresse électronique, et avait détourné des emails entrants.
- **Cherchez la clarté et évitez les supputations**. Si une demande n'est pas claire, demandez des éclaircissements. Si vous avez besoin de temps pour exécuter une demande technique en toute sécurité, dites-le.
- **Documentez vous-même le *dawn raid***. Tenez un registre interne des demandes, des systèmes auxquels vous accédez, des recherches que vous effectuez et des données que vous copiez ou examinez.
- **Surveillez les *dawn raids* chez les concurrents, les fournisseurs ou les clients**. Si vos concurrents, fournisseurs ou clients font l'objet d'un *dawn raid* et pas vous, cela ne signifie pas pour autant que vous ne figurez pas sur les radars de l'autorité de concurrence. Les preuves recueillies lors de *dawn raids* effectué au sein d'autres entreprises peuvent également être utilisées contre vous. Il est donc conseillé de surveiller les sites web des autorités de la concurrence afin de repérer les perquisitions qui pourraient vous concerner.

Plus d'infos ?

- Vous souhaitez en savoir plus sur les perquisitions de la Commission européenne? Consultez la Note explicative concernant les inspections menées par la Commission.
- Vous souhaitez en savoir plus sur les recherches effectuées par l'Autorité belge de la concurrence? Consultez les Lignes directrices de l'Autorité belge de la concurrence concernant la conduite des opérations de perquisition.
- contrast organise des ateliers au cours desquels les participants sont guidés pas à pas à travers les différentes étapes d'un *dawn raid* et un plan d'action concret est mis en place. N'hésitez pas à nous contacter pour plus d'informations : compliance@contrast.law
- In the Picture Octobre 2021: Prêt pour une perquisition de l'autorité de concurrence?

Auteurs

Michèle de Clerck