Le séquestre de données en entraide pénale internationale : qui peut s'y opposer ?

Célian Hirsch, le 28 février 2021

Seule la société qui dispose de l'accès physique aux *data rooms* est titulaire de la qualité pour recourir en matière d'entraide pénale internationale. Le déposant ou la personne qui détient des droits civils sur les données ne peut pas recourir contre l'ordonnance de clôture.

Arrêt du Tribunal pénal fédéral du 21 juillet 2020 RR.2020.11, RR.2020.12, confirmé par l'arrêt du Tribunal fédéral du 5 août 2020 1C_423/2020.

Le Ministère public de la Confédération ouvre une procédure pénale contre plusieurs personnes physiques et morales (art. 102 al. 2 CP) pour corruption (art. 322^{septies} CP), faux dans les titres (art. 251 CP) et blanchiment d'argent qualifié (art. 305bis al. 2 CP). Dans le cadre de cette procédure, il séquestre des supports de données qui se trouvent dans les locaux de deux sociétés genevoises.

Après avoir reçu des demandes d'entraide pénale internationale visant la transmission de ces données, une société prévenue demande à ce que la qualité de partie lui soit reconnue dans la procédure d'entraide. En effet, les données séquestrées la concerneraient, même si elles n'étaient pas stockées au sein de ses locaux. Elle soutient en particulier qu'elle avait un accès exclusif à distance aux *data rooms* stockées chez les sociétés genevoises puisqu'elle y louait un centre de données. Elle avait ainsi un pouvoir de disposition direct sur les données séquestrées.

Après avoir vu son argumentation rejetée par le MPC, la société saisit le Tribunal pénal fédéral.

Selon l'art. 21 al. 3 EIMP, la personne visée par la procédure pénale étrangère ne peut attaquer une décision que si elle est personnellement et directement touchée par une mesure d'entraide et a un intérêt digne de protection à ce qu'elle soit annulée ou modifiée. L'art. 80*h* let. b EIMP précise que la qualité pour recourir est octroyée à toute personne qui est personnellement et directement touchée par une mesure d'entraide et qui a un intérêt digne de protection à ce qu'elle soit annulée ou modifiée.

Selon la jurisprudence, la qualité pour recourir n'est reconnue qu'aux personnes qui ont une « proximité relationnelle spécifique » avec la décision de clôture (« *spezifische Beziehungsnähe* » ; ATF 137 IV 134 c. 5.2.1). Ainsi, la qualité pour recourir des personnes indirectement touchées, par exemple celles qui ne détiennent pas les documents saisis, doit en principe être refusée.

Le séquestre de documents qui sont en mains de tiers ne peut pas être contesté par une personne qui n'est qu'indirectement concernée par la mesure de contrainte. Cela s'applique également si les documents contiennent des informations sur les activités de la personne indirectement concernée. Ainsi, ni le propriétaire civil ni le déposant ne peuvent recourir contre la décision de clôture visant à transmettre des documents séquestrés auprès d'un dépositaire.

Le Tribunal pénal fédéral considère que ces règles ne s'appliquent pas que pour les documents physiques, mais également pour les données électroniques, ce que le Tribunal fédéral confirmera de façon laconique.

En l'espèce, les supports de données ont été séquestrés au sein de deux sociétés genevoises, avant que les données soient sécurisées et examinées par la police scientifique. Il ressort du rapport de police que l'installation était comparable à un bureau « hors site » par lequel les utilisateurs se connectaient à distance pour y travailler. Les parties étaient en particulier liées par un *Master Service Agreement*.

Cela étant, le Tribunal pénal fédéral considère que l'accès physique aux supports de données est déterminant. Dans une telle constellation, seuls le dépositaire et le propriétaire des dispositifs de stockage électronique de données saisis sont habilités à recourir et non leur déposant, leur propriétaire ou toute autre personne y disposant de droits. Le fait que la société prévenue pouvait accéder à distance aux données en question ne lui confère donc pas un droit de recours.

La société recourante n'est ainsi touchée que de façon indirecte par la mesure de contrainte. Partant, elle ne dispose pas de la qualité de recourir. Seules les sociétés genevoises séquestrées pouvaient donc recourir contre la décision de clôture.

Même si le Tribunal fédéral déclare le recours irrecevable, car il ne s'agit pas d'une question juridique de principe (au sens de l'art. 84*a* LTF), il souligne tout de même qu'il partage pleinement le raisonnement du Tribunal pénal fédéral.

Selon Gotham City et ICIJ, cette affaire concerne les données que Safe Host SA stockait pour Odebrecht, société brésilienne touchée par une affaire de corruption. Ces données permettraient ainsi de découvrir les divers flux d'argent afin de retrouver les personnes potentiellement corrompues.

Au-delà des circonstances particulières de l'affaire concrète, l'absence de qualité pour recourir de la société prévenue démontre, une fois de plus, la possible perte de contrôle des données lorsque celles-ci sont stockées dans un *cloud*. De ce fait, les sociétés qui externalisent la conservation de leurs données doivent désormais être conscientes de ce nouveau risque en matière d'entraide pénale internationale. L'avenir nous dira si les autorités pénales étrangères se montreront de plus en plus intéressées par les nombreuses données hébergées dans des *Data Center* suisses.

Cela étant dit, se pose la question de savoir si l'analogie entre les documents physiques et les données est véritablement convaincante d'un point de vue juridique. Contrairement aux documents déposés auprès d'un dépositaire, la personne qui « dépose » ses données dans un *cloud* peut garder une maîtrise relativement importante de ses données. Non seulement elle y dispose d'un accès instantané à distance, mais elle peut en plus les modifier ou les supprimer à tout moment, en principe sans intervention humaine. Serait-il dès lors opportun de reconnaître aux « titulaires » des données, comme les titulaires de comptes bancaires (art. 9*a* let. b OEIMP), la qualité de partie dans une procédure pénale internationale visant à transmettre leurs données ?

Dans l'attente d'une éventuelle modification de jurisprudence, les sociétés qui recourent au *cloud* devraient expressément prévoir contractuellement une obligation à la charge du prestataire *cloud* d'utiliser toutes les voies de droit possibles afin de défendre les intérêts des clients dont les données ont été séquestrées. L'intégration de clauses contractuelles bien rédigées est ici aussi essentielle, comme il en va d'ailleurs pour diminuer les autres risques du *cloud*.

Proposition de citation : Célian Hirsch, Le séquestre de données en entraide pénale internationale : qui peut s'y opposer ?, 28 février 2021 *in* www.swissprivacy.law/58

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.