crimen
.ch

procédure pénale

Un logiciel *keylogger* est une autre mesure technique de surveillance (art. 280 ss CPP)

Arrêt TF 1B_132/2020 et 1B_184/2020* (d) du 18 juin 2020 (ATF 147 IV 424)

Par Ryan Gauderon, le 2 mars 2022

> L'utilisation d'un logiciel *keylogger* permettant d'enregistrer les frappes sur un clavier d'ordinateur dans le but d'obtenir des mots de passe tombe sous le coup des art. 280 s. CPP et non pas de l'art. 269ter CPP. Le fait qu'il s'agisse d'un logiciel plutôt qu'un keylogger « mécanique » n'y change rien. Seul le critère du mode et du type d'installation est pertinent pour déterminer si le moyen de surveillance doit être qualifié de « moyen technique de surveillance ». Par ailleurs, un tel logiciel ne permet jamais d'intercepter des communications ou d'accéder à un système de traitement de données.

I. En fait

Dans le cadre d'une procédure pénale ouverte d'abord contre « inconnu » puis contre A grâce à certaines mesures de surveillance, le Ministère public II « Cybercrime » de Zurich constate que A est actif comme membre d'un trafic de stupéfiants international (art. 19 ch 2 LStup) et procède également à d'importantes opérations de blanchiment d'argent (art. 305bis ch. 2 CP) durant l'année 2019. Les autorités zurichoises ne parviennent toutefois pas à obtenir des preuves suffisantes car A n'utilise que des moyens de communication cryptés. Il fait également usage d'un système d'exploitation enregistré sur clé USB lui permettant de ne jamais laisser de traces dans l'ordinateur portable qu'il utilise dans un camping-car. Fort de ce constat, le Ministère public ordonne alors la mise en place d'un logiciel *keylogger* sur l'ordinateur de A en février 2020. Ce moyen permet d'enregistrer les touches utilisées sur un clavier d'ordinateur à l'insu de l'utilisateur. Saisi pour approbation du moyen de surveillance, le Tribunal des mesures de contrainte (Tmc) zurichois refuse d'autoriser l'usage du *keylogger*. Le Ministère public interjette recours contre cette décision au Tribunal fédéral (réf. 1B_132/2020).

Fin mars 2020, le Ministère public demande au Tmc la prolongation d'autres mesures de surveillance à l'encontre de A, dont celle relative à l'utilisation du logiciel *keylogger* pourtant non approuvée. Le Tmc accorde la prolongation des autres mesures de surveillance, à l'exception du *keylogger*. Contre cette décision, le Ministère public zurichois forme une nouvelle fois recours au Tribunal fédéral (réf. 1B_184/2020)

II. En droit

S'agissant de la qualité pour recourir du Ministère public zurichois, le Tribunal fédéral rappelle qu'en matière de recours contre les décisions de refus du Tmc, le ministère public

peut se prévaloir d'un préjudice irréparable (art. 93 al. 1 let. a LTF) dès lors que celui-ci s'expose à une destruction et une inexploitabilité absolue des preuves obtenues par une mesure de surveillance non autorisée (*cf.* art. 277 *cum* 281 al. 4 CPP) (c. 1.2).

Notre Haute Cour se penche ensuite sur le régime légal des mesures de surveillance fondées sur le CPP et précise que sous réserve des règles prévues aux art. 280 et 281 CPP, les « autres mesures techniques de surveillance » sont pour le surplus régies par les art. 269 ss CPP, dont l'art. 269ter CPP. Cette nouvelle disposition issue de la modification de la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) entrée en vigueur le 1er mars 2018 permet au ministère public l'introduction dans un système informatique de programmes informatiques spéciaux de surveillance de la correspondance par télécommunication (*GovWare*). Un tel moyen de surveillance ne peut être ordonné qu'aux conditions de l'art. 269 al. 1 et 3 CPP et pour autant que l'infraction poursuivie est cataloguée à l'art. 286 al. 2 CPP. En outre, les mesures de surveillance de la correspondance par poste et télécommunication doivent être restées infructueuses, jugées vaines ou rendraient la surveillance excessivement difficile (art. 269ter al. 1 let. a à c CPP) (c. 2.2).

En l'espèce, la réalisation des conditions de l'art. 269 al. 1 CPP ne sont pas contestées. En effet, il apparaît que l'usage de caméras et de *keylogger* mécanique ne semblent pas possible dans la mesure où l'intérieur du camping-car du prévenu est trop sombre pour le filmer et l'installation d'un *keylogger* mécanique ne serait pas suffisamment discrète. Ainsi, seule la qualité de « dispositif technique de surveillance » au sens de l'art. 280 CPP est remise en cause (c. 3).

Le Tmc a motivé son refus d'approbation par le fait que l'installation d'un logiciel *keylogger* ne se justifiait pas en application des art. 280 s. CPP et ne pouvait être considéré comme un "dispositif technique de surveillance". Il a estimé qu'il s'agit plutôt d'une possibilité offerte par le nouvel art. 269ter CPP. Se fondant sur la littérature, le Tmc a également rappelé qu'un *keylogger* mécanique, en tant qu'appareil, tombait sous le coup des art. 280 s. CPP, ce qui n'est pas le cas d'un logiciel. Contre cette argumentation, le Ministère public zurichois soutient que ce n'est pas la nature du moyen mais son mode d'installation qui est décisif pour la qualification d' "appareil" au sens des art. 280 s. CPP. Ainsi, puisqu'un logiciel *keylogger* s'actionne de manière identique à sa version mécanique (par clé USB) et remplit le même rôle (enregistre les frappes sur un clavier d'ordinateur sans besoin de "décrypter" des communications), il doit être considéré comme un appareil (c. 4.2).

Le Tribunal fédéral présente les avis doctrinaux en la matière dont les conclusions convergent toutes, à quelques nuances près, à la reconnaissance d'un logiciel *keylogger* comme « appareil technique de surveillance », sans qu'une distinction claire entre la version mécanique et la version numérique soit opérée. Cela étant, le Tribunal fédéral se rallie à l'avis du Ministère public zurichois s'agissant du critère du mode d'installation du moyen utilisé et reconnaît, en accord avec la doctrine, qu'il s'agit bel et bien d'un moyen technique de surveillance. Le fait qu'un logiciel *keylogger* ne soit pas une « machine » à proprement parler n'y change rien. Contrairement aux mesures fondées sur les art. 269 ss CPP, un *keylogger* ne permet jamais d'intercepter des communications mais uniquement de

constater ce qu'une personne saisit sur son clavier, et le logiciel utilisé reste sur une clé USB sans être « introduit » dans un système de traitement de données. En outre, une clé USB ne peut jamais être considérée comme un système de traitement de données. Le Tribunal fédéral relève finalement que le Tmc, même dans l'hypothèse où le *keylogger* devait tomber sous le coup de l'art. 269ter CPP, aurait dû accorder la surveillance, les conditions de cette disposition étant également remplies dans le cas d'espèce (c. 5.1 et 5.2).

Les deux recours sont admis et la mesure de surveillance peut être autorisée, respectivement prolongée, le Ministère public zurichois ayant correctement motivé la nécessité de prolonger la surveillance (c. 5.4). La publication de ces deux arrêts n'a été possible qu'après validation par l'autorité chargée de l'enquête, raison pour laquelle elle est intervenue tardivement (arrêts rendus en juin 2020 et publiés en février 2022 seulement) (c. 6)

III. Commentaire

Ces deux arrêts ont été dévoilés plus de 18 mois après leur date de prononcé afin de permettre aux autorités zurichoises de continuer leur enquête et d'éviter que les mesures de surveillance secrètes soient compromises par une publication officielle. Cette pratique très exceptionnelle mérite d'être relevée et saluée.

Proposition de citation : Ryan GAUDERON, Un logiciel *keylogger* est une autre mesure technique de surveillance (art. 280 ss CPP), in : https://www.crimen.ch/84/ du 2 mars 2022