



Cont...tribution du Prof. Dr. Sylvain Métille à l'occasion des cinq ans de LawInside.ch

Pour célébrer les cinq ans de LawInside.ch, nous avons demandé à des personnalités actives dans le monde juridique en Suisse romande et alémanique de commenter un arrêt comme contributeurs externes de LawInside.ch.

Comme premier contributeur, nous avons le plaisir d'accueillir le Professeur Sylvain Métille, avocat associé en l'Étude HDC et Professeur associé à l'Université de Lausanne. Il est un spécialiste reconnu en matière de protection des données et nous présente ici un arrêt du Tribunal fédéral en matière de secret professionnel en lien avec les supports de données chiffrés.

TF 16.12.2019, 1B_459/2019

Lorsqu'un support chiffré contient des données protégées par le secret professionnel, le refus du prévenu de fournir la clé de déchiffrement n'autorise pas la levée des scellés.

Faits

Le Ministère public du canton d'Argovie a saisi des supports informatiques dans le cadre d'une affaire de violation de la loi fédérale sur l'encouragement du sport, de la loi fédérale sur les produits thérapeutiques et de blanchiment d'argent. Le prévenu a demandé leur mise sous scellés, certains supports informatiques contenant de la correspondance avec ses avocats protégée par l'art. 264 al. 1 let. a CPP.

Étant le seul à connaître le contenu des documents scellés, le prévenu doit coopérer à la levée des scellés. Lors de la première audience de tri, le prévenu a indiqué, pour certains des supports de données, dans quels répertoires pouvait se trouver la correspondance échangée avec ses avocats. La plupart des supports de données sont néanmoins chiffrés, ce qui rend une vérification impossible.

Le prévenu a indiqué avoir noté à la main les mots de passe sur un papier qui ne lui a pas été restitué par les autorités de poursuite pénale et ne pas s'en souvenir. Le Tribunal des mesures de contrainte ne croit pas cette version et retient qu'en raison du manque de coopération du plaignant pour déchiffrer les supports de données scellés, il est de fait impossible de séparer la correspondance protégée par l'art. 264 al. 1 let. a CPP. Le Tribunal ordonne alors la levée des scellés sur tous les supports de données qui n'ont pas pu être déchiffrés.

Droit

Dans un arrêt 1B_376/2019 du 12 septembre 2019, le Tribunal fédéral a confirmé qu'en application du principe « *nemo tenetur se ipsum accusare* », personne n'est tenu de contribuer à sa propre accusation dans le cadre d'une procédure pénale et que le prévenu a les mesures techniques de protection sans subir de désavantages en vertu de son droit de refuser de témoigner (art. 14 al. 3 let. g Pacte ONU II de l'ONU, art. 32 Cst., art. 6 al. 1 CEDH, art. 113 al. 1 et art. 158 al. 1 let. b CPP). En particulier, un prévenu ne peut pas être contraint de divulguer le code de verrouillage de l'appareil ou le code PIN ou PUK de la carte SIM.

Il en va de même dans le cadre de la présente affaire. L'obligation de collaboration n'implique pas celle de divulguer un mot de passe. Même si le Tribunal des mesures de

contrainte considérait que l'obligation de coopérer incluait la divulgation des mots de passe, en sanctionnant le refus de coopérer par l'exploitation des documents protégés par le secret professionnel, le Tribunal des mesures de contrainte aurait exercé une pression indirecte excessive sur le plaignant, ce qui violerait le droit de ne pas s'auto-incriminer.

Dans la mesure où il est possible de déchiffrer les supports ou de les exploiter d'une autre manière ne requérant pas la coopération du prévenu, cela doit être fait dans le cadre de la procédure de levée des scellés et sous le contrôle du Tribunal des mesures de contrainte. À cet effet, il peut évidemment faire appel à des experts externes (par exemple des informaticiens) ou à des services de police spécialisés (art. 248 al. 4 CPP).

Note

Cet arrêt confirme la jurisprudence qui reconnaît d'une part le droit du prévenu de ne pas s'auto-incriminer en donnant un code d'accès ou de déchiffrement et d'autre part le droit de l'autorité de poursuite de prendre des mesures pour déjouer les mesures techniques de protection mise en place par le prévenu pour protéger ses données.

Le respect du secret professionnel s'applique donc bien à des données chiffrées, ce qui implique que le processus de déchiffrement doit être mené sous le contrôle du Tribunal des mesures de contrainte et non pas du ministère public. Cela n'exclut pas de recourir à l'aide d'experts techniques, mais il faut alors s'assurer qu'ils agissent sous le contrôle du Tribunal des mesures de contrainte et que l'autorité de poursuite n'ait pas accès aux données.

Proposition de citation : SYLVAIN MÉTILLE, Nemo tenetur, données chiffrées et mise sous scellés, in:

<https://lawinside.ch/879/>