

# Le coronavirus profite-t-il au crime économique?

*“Le crime financier reste inacceptable, même en ces temps de crise comme nous le vivons avec l’épidémie de Covid-19”. Cette déclaration quelque peu lyrique a été faite il y a quelques semaines par l’**Autorité bancaire européenne**, qui avertissait qu’elle n’allait pas cesser sa supervision. Car même si les échanges monétaires sont au ralenti, les flux d’argent illicite, eux, se maintiennent, tant “les criminels sont très flexibles, et développent de nouvelles techniques et de nouveaux canaux de blanchiment d’argent”.*

Le coronavirus va-t-il effectivement susciter de nouvelles vocations criminelles? Comment les institutions et les professionnels de la régulation peuvent-ils continuer leur mandat dans des conditions bousculées? En Suisse, les experts sont inquiets.

## Télétravail et cyber-risques

**Joël Winteregg** est à la tête de la société vaudoise **Netguardians**, qui développe des logiciels de prévention des fraudes à destination des établissements financiers. *“Les banques suisses n’étaient pas du tout habituées au home office avant la crise du coronavirus, explique-t-il, et ce depuis le séisme Falciani, à cause des craintes liées au secret bancaire et au vol de données”.* Mais avec le COVID-19, les établissements bancaires ont dû s’adapter rapidement.

En Suisse, la **Centrale d’enregistrement et d’analyse pour la sûreté de l’information MELANI** a récemment constaté une augmentation des cyber-attaques. Pour Joël Winteregg, il n’y aurait pour l’instant pas eu de tentatives notables de fraudes externes contre des établissements financiers suisses. *“Par contre, la fraude interne est un risque potentiel important, ajoute-t-il. Le Covid-19 crée une fenêtre d’opportunité pour agir pour un employé frustré qui envisagerait ce type de méfait. Avec des contrôles simplifiés en temps de crise et moins de surveillance de la part des collègues, cela laisse plus de latitude pour agir.”*

## Secret professionnel

Le problème se pose aussi du côté des études d'avocats chez qui le télétravail demande la mise en place de règles strictes en matière de respect du secret professionnel, comme en témoigne la jurisprudence sur le sujet - le **Tribunal fédéral (TF)** a en effet rendu un arrêt **très commenté** au sujet du *coworking* l'an dernier. *“Les avocats étaient en général déjà habitués à travailler depuis chez eux le soir explique **Stéphanie Chuffart-Finsterwald**, avocate chez **sigma legal**, mais là, ce qui est nouveau, c'est le télétravail des auxiliaires, des équipes administratives. Une question importante est celle de savoir s'il faut leur donner des accès aux dossiers concernés par le secret professionnel.”*

Pour elle, la situation actuelle est une opportunité pour mettre en place de bonnes pratiques en matière de confidentialité et de protection des données. *“Le cloud par exemple implique presque nécessairement une sous-traitance, ce qui pose d'importantes questions d'ordre réglementaire et pratique, explique-t-elle. Si le prestataire est basé à l'étranger, il faut s'assurer que la couverture du secret y est équivalente à celle de la législation suisse”*. Pour l'avocate, il est également important de *“choisir des plateformes et applications cryptées de bout en bout et qui effectuent une collecte minimale des données, comme par exemple celles offertes par Infomaniak, Wire ou Threema, tous trois sis en Suisse”*. Les vidéos-conférences seraient quant à elles à tenir avec précaution. *“Il faut bien prévenir les clients: la confidentialité ne peut être 100% garantie en utilisant ce type d'outils”*.

Un constat repris par une consultante genevoise en conformité, qui insiste particulièrement sur les risques que posent les applications de visioconférences de type **Zoom** chez les employés des banques ou des gestionnaires d'actifs. *“Lors de réunions d'investissements, des décisions confidentielles d'acheter ou de vendre en masse sont partagées. Si la vidéo est hackée, il y a des risques de délit d'initié”*, estime-t-elle.

## **Abus de marché**

En matière de risques, les professionnels du secteur bancaire semblent se focaliser actuellement en priorité sur le trading. La consultante genevoise, qui souhaite garder l'anonymat, recommande ainsi aux experts de faire particulièrement attention aux risques de *“churning”*. *“Quand par exemple le gestionnaire d'un compte reçoit un pourcentage à chaque transaction, il va être tenté de faire tourner les portefeuilles plus que d'habitude, en*

*achetant et vendant alors que ce n'est pas justifié, au prétexte qu'il y a de grosses turbulences sur les marchés."*

Cette dernière conseille de *"prioriser les contrôles. En ce moment, on peut mettre en pause les ouvertures de comptes afin de ne pas avoir à faire les contrôles "Know Your Customer" liés. Il faut à l'inverse porter une attention accrue sur les risques d'abus de marché"*.

Une tendance adoubée par la **FINMA**, qui a récemment **annoncé** vouloir soutenir *"une activité de surveillance flexible"*, en autorisant notamment le report de certains délais. Contacté par *Gotham City*, son porte-parole explique que cela *"signifie une surveillance orientée systématiquement sur les risques et organisée de manière anticyclique. Cela peut notamment signifier que certains rendez-vous, contrôles de routine sur place ou délais peuvent être reportés, voire effectués à distance, ceci afin de permettre aux assujettis de disposer plus librement des ressources dont ils disposent. Cela peut en outre signifier que certains devoirs en lien avec la remise de documentation physique peuvent être assouplis car de nombreux employés travaillent actuellement depuis la maison. Bien entendu, les directives et les dispositions internes resteront en vigueur. Il n'est également pas question pour la FINMA d'assouplir les règles et attentes en matière de compliance."*

Pour **Daniel Weber**, avocat chez **Wenger & Vieli** et ancien de la FINMA, cette dernière *"doit être flexible, mais seulement quand elle peut l'être. Pas lorsqu'il s'agit de réglementations importantes. Ce n'est pas parce qu'il s'agit d'une crise que l'on ne doit pas respecter les règles, notamment en terme de lutte contre le blanchiment"*.

## **Laver moins blanc**

En la matière, les établissements bancaires américains ont commencé à **militer** auprès des régulateurs afin d'obtenir un assouplissement des règles. Notamment en matière d'exigences de demandes d'informations sur les bénéficiaires effectifs, afin de permettre aux PME de bénéficier rapidement des prêts d'urgence prévus dans les plans de sauvetages étatiques de l'économie. Mais ces demandes peuvent poser des problèmes. Le **Financial Times** pointe par exemple celui de l'intégration à distance de nouveaux clients. Les vérifications virtuelles d'identité, autorisées par la **Financial Conduct Authority**, le régulateur

britannique, seraient ainsi *“une aubaine pour les escrocs financiers”*, estime le quotidien.

En Suisse, la question des prêts-relais fournis actuellement par **UBS** ou le **Credit Suisse** aux petites entreprises pose également question. Ainsi le blog **Inside Paradeplatz** s'inquiète de ces *“millions de francs”* qui pourraient bénéficier *in fine* à des sociétés de domiciliation.

Du côté des entreprises, Daniel Weber explique que la situation actuelle inciterait également ces dernières à mettre la compliance de côté. *“Un “déplacement des ressources” est en train de se produire. Les entreprises doivent concentrer leurs ressources sur leur activité principale et la conformité passe au second plan. Par exemple, parce qu’elles doivent se tourner vers de nouveaux fournisseurs qu’elles ne connaissent pas, ou parce qu’elles subissent une pression accrue pour mettre leurs produits sur le marché plus rapidement, indique-t-il. On verra avec le temps si les entreprises ont suffisamment investi, avant la crise, dans des systèmes de conformité et de contrôle opérationnels qui peuvent faire face aux risques d’une telle situation extraordinaire.”*