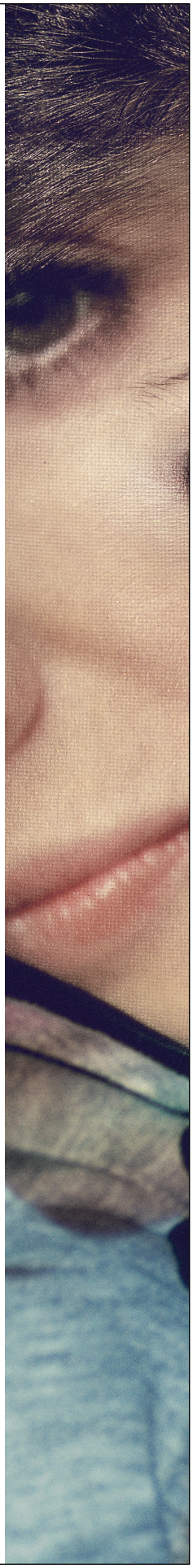
LES VOLEURS D'IDENTITÉ

PAR MARC-ANDRÉ SABOURIN

PHOTO DE CHRISTIAN BLAIS

S'enrichir grâce à vos données personnelles est un jeu d'enfant pour eux. Les témoignages exclusifs d'ex-fraudeurs exposent un système très payant et impossible à contrer.



LE

Le stationnement du centre commercial où Sarah m'a donné rendez-vous est plongé dans le noir, complètement désert. Je coupe le moteur de ma voiture en me demandant une fois de plus si elle va se présenter. Après tout, elle n'a strictement rien à gagner en parlant à un journaliste.

Après quelques minutes d'attente, un VUS s'arrête à côté de mon véhicule. C'est Sarah. Un faux nom, que je lui ai donné afin de la protéger de la justice, mais aussi de ses anciens complices.

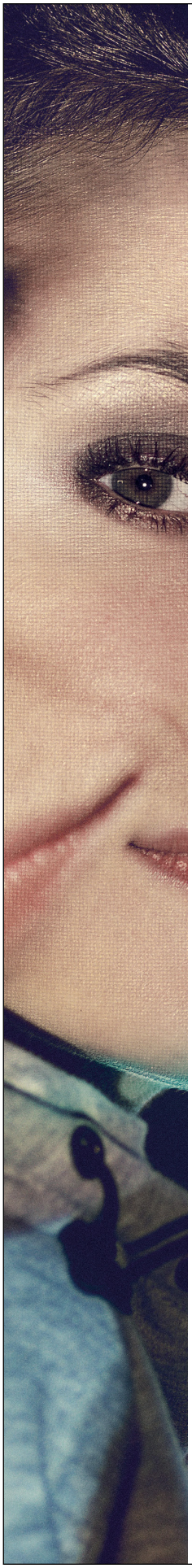
La jeune femme me salue, puis scrute le stationnement vide autour de nous. « Ouin, ça a l'air d'un *deal* de drogue, notre affaire, dit-elle en riant nerveusement. On a vraiment l'air louches. Ça te dérange d'aller ailleurs ? »

Je monte dans son VUS et nous roulons jusqu'à un Tim Hortons. Mais pas question de nous installer à l'intérieur. Nous garons plutôt le véhicule entre ceux des clients, où, dans la noirceur de la nuit, il semble attendre parmi tant d'autres le retour de ses occupants. C'est là, assise dans l'habitacle, que Sarah me raconte son ancienne vie. Celle où elle a usurpé l'identité de centaines de personnes pour commettre des fraudes dépassant le million de dollars.

Quand Desjardins a annoncé en juin 2019 la plus grande fuite de données de son histoire, suivie de peu par Capital One, bien des Québécois ont pris conscience que changer régulièrement leurs mots de passe, c'était loin de suffire à protéger leurs informations personnelles. Et ces données, censées vous identifier, vous et personne d'autre, peuvent se retourner contre vous lorsqu'elles tombent entre les mauvaises mains.

J'y avais moi-même goûté des mois plus tôt, en février 2019. Une enquêtrice de la banque RBC m'avait appelé pour vérifier si j'avais bel et bien fait une demande de carte de crédit auprès de cette institution financière — ce n'était pas le cas. « Vous êtes victime d'un vol d'identité, monsieur », m'avait calmement annoncé la voix au bout du fil.

J'ai été chanceux. La tentative de fraude a été détectée rapidement, ce qui m'a permis de découvrir que des comptes avaient été ouverts à mon nom dans une autre banque. Tout a été fermé, je n'ai subi aucune perte financière, et faire le ménage de mon dossier de crédit — contacter le service d'enquête des institutions où les fraudeurs avaient frappé, consigner les évé-



nements par écrit, faire le suivi avec les agences de crédit pour qu'elles effacent ces transactions de mon dossier — a nécessité moins d'un mois.

Problème réglé ? Non. Car quelqu'un, quelque part, connaît désormais mon adresse, ma date de naissance, mon numéro de téléphone et, surtout, mon numéro d'assurance sociale. Bref, tout ce qu'il faut pour semer le bordel à nouveau dans ma vie. Et je suis loin d'être le seul dans cette situation.

Selon les données compilées par le Centre antifraude du Canada (CAC), il y a eu 9 735 vols d'identité et 9 074 cas de fraude à l'identité — qui consiste à utiliser des données volées pour commettre une fraude — au pays en 2019. Mieux vaut toutefois ne pas trop se fier à ces chiffres, explique Jeff Thomson, analyste au CAC. « Cela inclut uniquement les cas qui nous ont été signalés par les citoyens ou par la police. » Or, de nombreuses personnes, dont moi, ne pensent pas à contacter le CAC ou à porter plainte à la police puisqu'elles n'ont pas subi de pertes financières. Hélas ! lorsqu'un crime est sous-déclaré, « il risque moins d'être une priorité pour les corps policiers », rappelle l'analyste.

Si vous croyez que le nombre de vols d'identité signalés en 2019 bondira à plus de six millions à cause de la fuite de données massive chez Desjardins, détrompez-vous. La police a beau enquêter sur ce crime, cela « comptera pour une seule affaire », dit Jeff Thomson, à moins que chaque personne touchée ne communique avec le CAC. En fait, le flou qui entoure le vol d'identité est tel que le Centre antifraude du Canada préfère ne pas chiffrer les dommages économiques causés par ce crime. « Ce serait une donnée erronée. »

Il n'y a pas que les statistiques sur le vol d'identité qui sont incomplètes. L'image que l'on se fait des gens qui commettent ce crime est aussi abstraite. Pour s'en convaincre, il suffit de voir la photo typique du pirate informatique, caché sous un capuchon devant son ordinateur, qui accompagne constamment les articles sur le vol d'identité…

Ces gens dont on ne voit jamais le visage sont les maillons d'un système bien huilé, opaque et surtout très payant, ai-je découvert au cours d'une enquête d'un an et demi, qui a conduit au documentaire *Les voleurs d'identité*. Il a fallu débusquer des fraudeurs, mais aussi les convaincre de rompre l'omerta qui règne dans ce milieu, comme dans tout réseau criminel. Car c'est bien de réseaux qu'il s'agit. Ensemble, leurs témoignages exposent les rouages d'un univers inquiétant et font valser bien des idées reçues sur la protection de nos données personnelles.

Les fraudeurs connaissent certaines de nos informations les plus confidentielles, alors il est plus que temps d'en savoir davantage sur eux.

LES TAUPES

« Un nom, une adresse, une date de naissance. »

J'attends que ma source poursuive son énumération, mais elle se tait. C'est tout ; tout ce qu'il lui faut pour usurper l'identité d'une personne et commettre une fraude.

Cette source, appelons-la Serge, a gravité dans un réseau de fraudeurs pendant plusieurs années. Serge a accepté de m'expliquer d'où provenaient les identités volées utilisées par son groupe, à condition que je ne détaille pas les fraudes auxquelles il a participé.

J'ai pu corroborer les informations de Serge avec une seconde source — appelons celle-ci Anthony —, qui est elle aussi bien rompue au monde du vol d'identité. Les deux hommes ne se connaissent pas, mais les portraits qu'ils dressent sont similaires.

Les pirates informatiques capables d'infiltrer n'importe quel système de haute technologie, « c'est dans les films, ça, rigole Serge. Il n'y a personne comme ça dans la vraie vie ». Si des attaques numériques sont parfois perpétrées pour voler des identités, c'est loin d'être systématique. Car il existe des moyens plus simples et, dans bien des cas, légaux d'obtenir les renseignements dont un fraudeur a besoin. Il y en a même un que vous utilisez peut-être tous les jours : Facebook.

« Sur Facebook, les gens nous donnent leur nom, leur ville de résidence et, la chose la plus importante, leur date de naissance », dit Anthony. Même ceux qui n'affichent pas leur date d'anniversaire sur le réseau social sont souvent compromis par leurs amis qui leur écrivent publiquement « bonne fête »…

Outre Facebook, il y a Pages Jaunes, LinkedIn et les sites de généalogie, notamment, qui fournissent une foule d'informations. Plusieurs bases de données publiques, dont Les Plumitifs (qui permettent de vérifier si quelqu'un a des antécédents judiciaires), le registre des entreprises et le registre foncier du Québec, permettent aussi de dresser un portrait étoffé d'une personne sans jamais lui parler.

Par exemple, dans le cadre de ce reportage, je devais obtenir des renseignements sur une personne dont je n'avais que le nom. En utilisant des ressources accessibles à tous en ligne, j'ai su où elle travaillait, trouvé son adresse et son numéro de téléphone. J'ai découvert qu'elle n'avait plus de contacts avec son père, identifié sa mère, ses frères, ses neveux et nièces. J'ai trouvé sa date de naissance, consulté l'acte de vente de son condo et vu l'ensemble de ses contraventions routières.

Bref, j'en ai appris bien plus sur cette personne que les informations de base dont un fraudeur a besoin.

Pour usurper son identité, je n'aurais eu qu'à me procurer de fausses cartes à son nom. Et ce n'aurait pas été très compliqué, si je me fie à un faussaire. « Il me faut juste ta photo avec les informations que tu veux sur le permis, pis c'est prêt en 48 heures », m'a-t-il affirmé. Le coût : 200 dollars.

Les fraudes les plus complexes — souvent les plus payantes — nécessitent toutefois davantage qu'un nom, une adresse et une date de naissance. L'une des données cruciales qu'un fraudeur doit obtenir devient alors le numéro d'assurance sociale.

« Tu peux acheter ça sur Internet », explique Serge. De nombreux marchés illégaux du Web clandestin — le *dark* Web — vendent en effet des profils complets de personnes venant d'un peu partout sur la planète. « *But there's no honor among thieves*, continue le fraudeur en anglais. Il n'y a pas d'honneur entre les voleurs. » Les données ne sont pas toujours de qualité, et pas moyen de vérifier celle-ci avant de les acheter. Et encore, il arrive qu'elles ne soient jamais livrées.

Afin d'obtenir des informations valides à tout coup, l'idéal est de pouvoir compter sur une « personne à l'intérieur », dit Anthony. À l'intérieur de quoi ? D'une institution financière, par exemple.

C'est ce qui s'est passé chez Desjardins : un employé a utilisé ses accès pour subtiliser des renseignements sur des clients. Ce vol de données est unique pour son ampleur — plus de six millions de personnes touchées —, mais pas pour la méthode employée. Selon Michel Carlos, qui a été directeur des enquêtes à la Banque Nationale après avoir dirigé l'équipe des crimes économiques à la Sûreté du Québec, une « dizaine de taupes » sont attrapées chaque année dans les institutions financières du Québec.

Les taupes n'opèrent pas seulement dans le monde financier. « Il y en a partout où il y a des données personnelles, assure Serge. Ça peut être à ton travail. Ça peut être dans les compagnies de téléphone, les universités. Au gouvernement. Partout. »

« Dans n'importe quelle entreprise qui collecte des données sur les gens, il y a probablement quelqu'un qui les vend, parce que c'est très payant », corrobore Anthony.

J'ai trouvé deux anciens employés de banque qui ont volé des informations pour des réseaux de fraudeurs. Ils ont refusé de m'accorder une entrevue, mais l'un d'eux a tenu à préciser qu'il avait participé à ce stratagème contre son gré. Il avait une dette de drogue et aurait été contraint de la rembourser, sous la menace, en sortant des données.

Je n'ai aucun moyen de vérifier ces affirmations. Toutefois, selon Michel Carlos, des problèmes de drogue, d'alcool et de jeu figurent parmi les raisons fréquentes qui poussent quelqu'un à voler des renseignements.

Cela a pris quelques mois, mais la taupe a fini par se faire pincer et a été renvoyée. Son ex-employeur a exigé qu'elle rembourse les dizaines de milliers de dollars que l'institution a dû débourser pour réparer les dégâts causés par la fuite. Autrement, l'entreprise porterait plainte à la police. Par crainte d'avoir un casier judiciaire, la taupe s'est endettée pour payer la banque.

« C'est illégal ! tonne Michel Carlos lorsque je lui rapporte les propos de cette personne. Tu ne peux pas demander de l'argent pour cacher un crime. Ça s'appelle composer avec un acte criminel et tu peux aller en prison pour ça ! Les gestionnaires devraient savoir ça ! »

Encore une fois, impossible de vérifier les affirmations de la taupe, mais un ex-employé du service d'enquête d'une grande banque m'a confirmé, sous le couvert de l'anonymat, avoir été témoin d'une telle pratique dans son institution.

Le vrai problème, souligne Michel Carlos, c'est que même si la taupe a été renvoyée, les bandits qui l'ont recrutée opèrent peut-être encore, sans s'inquiéter. Ils peuvent corrompre d'autres employés, en leur offrant de l'argent ou en les menaçant, et continuer de dérober des identités.

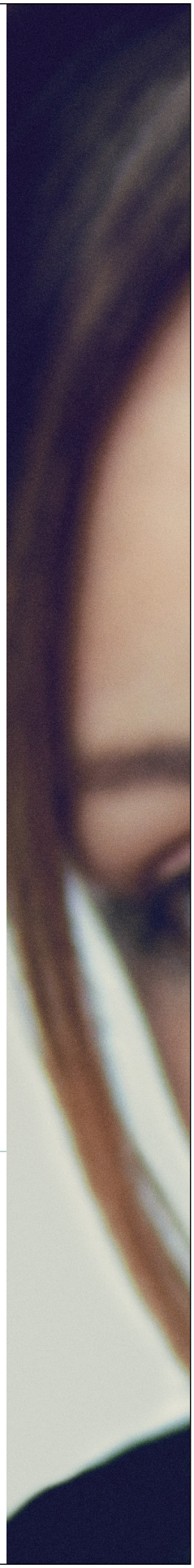
Contactée par *L'actualité*, l'Association des banquiers canadiens n'a pas voulu commenter cet événement en particulier et a affirmé par courriel que, « dans les rares cas où un employé effectue des activités non autorisées, la situation est prise en charge aussitôt découverte [par une banque], en collaboration avec les forces de l'ordre et conformément aux lois en vigueur ».

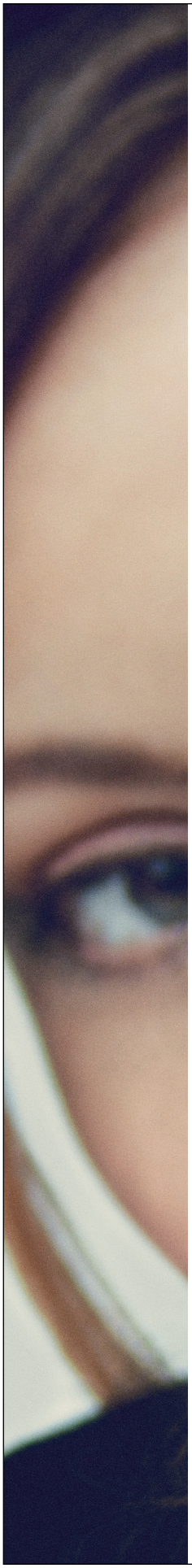
LA COMÉDIENNE

Assise dans son VUS dans le stationnement du Tim Hortons, Sarah me raconte le début d'une vie qui aurait dû être sans histoire. Celle d'une petite fille enjouée, élevée au sein d'une famille de la classe moyenne comblant tous ses besoins, et qui rêvait de devenir actrice. Jusqu'à ce que survienne un drame dans sa famille.

« C'est là que j'ai perdu confiance envers les adultes. Surtout mes parents. Quand t'es un enfant, ils sont censés être tes héros. Mais chez moi, cette idée-là a été détruite. »

Son sens de la famille, c'est à l'adolescence qu'elle l'a retrouvé. Dans la rue, avec des *bums*,





Afin d'obtenir des informations valides à tout coup, l'idéal est de pouvoir compter sur une « personne à l'intérieur », dit Anthony. À l'intérieur de quoi ? D'une institution financière, par exemple.

puis avec des gangs. « On n'avait pas le même sang, on ne venait pas du même milieu, mais on avait le même ressentiment envers le système. »

Avec eux, elle a volé, vendu de la drogue et dansé nue alors qu'elle était encore mineure. « Je n'avais l'air de rien, mais c'était moi la pire de la gang. J'avais perdu le goût de vivre, alors je cherchais toujours la prochaine émotion forte, parce que je ne ressentais rien. »

Un jour qu'elle était mal prise, Sarah a accepté sans remords ni états d'âme l'argent d'un gars qui dirigeait un réseau de fraude, persuadée qu'elle le manipulait… Puis est venu un moment où il lui a demandé de renvoyer l'ascenseur. « Il ne m'a pas dit : "Crache le *cash* ou je te casse les jambes." Les fraudeurs sont charismatiques. C'était plutôt : "Je t'ai aidée, maintenant, c'est à ton tour de m'aider." » Il avait besoin d'une *striker*.

Dans le monde des voleurs d'identité, le *striker* est en quelque sorte un comédien, explique Sarah. Son rôle est de jouer la personne dont les données ont été dérobées. C'est le *striker*, sous cette identité usurpée, qui visitera des commerces pour acheter des produits à crédit, et des banques pour contracter des prêts — qu'il n'a aucune intention de rembourser.

Son profil doit *grosso modo* correspondre à celui de la personne à laquelle sont liées les données. Si un fraudeur a mis la main sur les informations concernant Paul Simard, 43 ans, le *striker* doit ressembler à un Paul Simard de 43 ans, et non à un jeune de 20 ans. « Tu ne portes pas une fausse moustache ou un truc de même quand tu fais ça, dit Sarah. C'est ton visage et tu ne peux pas le changer. »

Advenant qu'une enquête soit ouverte, ce visage serait la première chose que les policiers verraient sur les caméras de surveillance. Le *striker* idéal n'a donc pas peur du risque et aime jouer un rôle. Pour Sarah, c'était la façon rêvée de combiner sa quête d'adrénaline et son rêve de devenir comédienne.

Son premier rôle de *striker* consistait à faire le tour des fournisseurs de téléphonie mobile pour s'abonner à des forfaits incluant un cellulaire haut de gamme. Son *boss* revendait les appareils sur le marché noir à l'étranger, tandis que les comptes, impayés, finissaient par être fermés par le fournisseur de service.

Avant chaque coup, Sarah apprenait par cœur le nom, l'adresse et la date de naissance de trois ou quatre profils de victimes, fournis par son *boss*. Il lui remettait aussi des permis de conduire contrefaits, affichant les informations des identités volées et la photo de Sarah. « Ensuite, j'avais juste à entrer dans les magasins, puis à donner les infos pour avoir le plus de téléphones possible au nom de ces personnes-là en une journée. »

Pour éviter les soupçons, la *striker* ne retournait jamais dans la même succursale et inventait une vie à ses personnages. « Je jasais avec les vendeurs, j'expliquais que je voulais faire un cadeau à mes frères et sœurs et que, pour ça, il me fallait quatre lignes. » Sarah n'avait jamais peur de pousser l'audace afin d'obtenir une ligne de plus, persuadée qu'elle ne se ferait jamais prendre, et sortait « 15 téléphones facile avec une seule identité ». Elle touchait une commission pour chaque appareil volé et a déjà gagné jusqu'à 3 000 dollars en une journée.

La *striker* était efficace, trop, même. Son nom a commencé à circuler dans le milieu et d'autres fraudeurs se sont mis à lui proposer des *jobs* plus risqués, mais plus payants. Toujours à la recherche de nouvelles émotions fortes, Sarah disait oui. Et c'est ainsi qu'elle s'est retrouvée à ouvrir des marges de crédit.

Sur papier, le concept est simple : utiliser une identité volée pour demander une marge de crédit dans une institution financière, puis disparaître avec l'argent. Mais sur le terrain, cela requiert du nerf et beaucoup de préparation.

Apprendre un nom et une adresse par cœur ne suffisait plus. Avant de se présenter dans une institution financière, Sarah devait désormais connaître des pans de la vie de la personne dont elle usurpait l'identité. Elle regardait sur Facebook pour savoir si son « personnage » était en couple ou s'il avait des enfants. Elle utilisait LinkedIn pour vérifier quel était son emploi. Elle se servait de tout ce qui pouvait l'aider à être crédible dans son rôle.

Une fois devant le prêteur, Sarah disait qu'elle voulait faire des rénovations ou était enceinte et qu'elle avait besoin d'une marge de crédit, puis improvisait au fil de la conversation. « Il faut que tu te souviennes de la marde que tu racontes, parce que les gens accrochent sur ces détails-là et que tu vas devoir retourner une couple de fois à la banque pour remplir la demande et signer des papiers avant d'avoir l'argent. »

Plus facile à dire qu'à faire, car la *striker* ne frappait pas une seule institution financière à la fois, mais plusieurs. « C'est vraiment du travail ! Je pouvais entrer dans cinq banques différentes par jour pour demander des marges. Et sur les cinq, il y en avait peut-être juste une où ça allait fonctionner, et encore. »

Comme un client normal n'irait pas demander du crédit dans une institution financière à 600 km de chez lui, Sarah se rendait dans la région du Québec ou du Canada où habitait la personne dont elle prenait l'identité. « Souvent, les profils venaient en *batchs*. Si on avait 15 profils du Manitoba, on allait dans une petite ville du Manitoba pour les passer tous en même temps. » Même le voyage se faisait sous une fausse identité.

Sarah n'opérait pas seule. Son patron était avec elle, ainsi que trois ou quatre autres *strikers*, dont l'apparence correspondait à d'autres profils volés. Tous en même temps, ils essayaient d'obtenir des marges de 20 000, 30 000, 50 000 dollars dans différentes institutions financières. Et lorsque l'un deux ressortait avec l'argent dans ses mains, « c'était *insane* ».

« Je ne peux même pas décrire le *high*, dit Sarah. Je n'ai jamais connu une drogue qui pouvait faire ça. C'est comme gagner un million. Après ça, avec la gang, on se pétait la face, on faisait le *party*. Mon *boss* payait tout, mais lui, il riait dans sa barbe. C'est nous qui prenions le risque. »

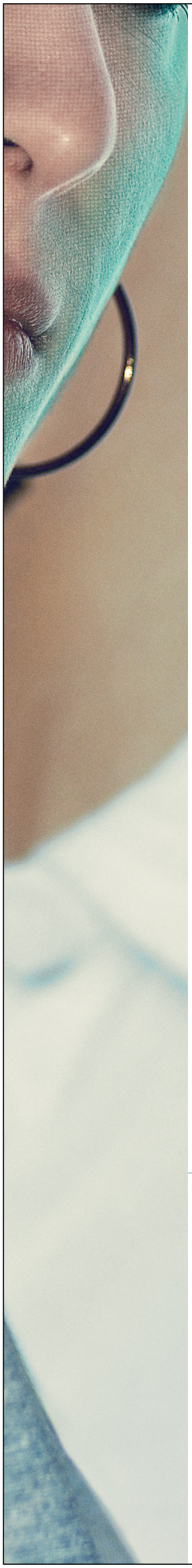
C'est à lui, le patron, que revenait l'argent volé. Les *strikers* touchaient une commission, qui variait selon la somme sortie de la banque. Sur une fraude de 25 000 dollars, Sarah obtenait autour de 7 000 dollars.

L'argent disparaissait aussi vite qu'il arrivait. « Je n'avais aucun attachement à ce *cash*-là, raconte Sarah. Je le "flaubais" dans des niaiseries. Des vêtements, de la bouffe, de l'alcool, des cadeaux, n'importe quoi. Je connais des fraudeurs qui ont économisé leur argent parce qu'eux, c'était leur plan pour sortir du crime. Moi, ce n'était pas pareil ; je la voulais, cette vie-là. »

Au cours des cinq années où elle a été *striker*, Sarah n'a jamais eu la moindre pensée pour les gens dont elle avait pris l'identité. « Dans ma tête, c'était les banques que je volais. C'est plus tard que j'ai compris l'impact que ça avait sur le monde. » Sur ses centaines de victimes, elle se souvient d'une seule : la dernière.

Sarah avait fait une énième demande de marge de crédit. Il ne lui restait plus, pour obtenir les fonds, qu'à passer à l'institution financière afin de signer les papiers. « Tout de suite en entrant, j'ai eu une *vibe* que je ne devais pas être là, que je devais m'en aller au plus vite. L'air était tendu. En même temps, je me disais : "Non, c'est trop d'argent, je ne veux pas perdre tout le travail que j'ai fait." Puis les policiers sont arrivés. »

Au cours des cinq années où elle a été *striker*, Sarah n'a jamais eu la moindre pensée pour les gens dont elle avait pris l'identité. « Dans ma tête, c'était les banques que je volais. C'est plus tard que j'ai compris l'impact que ça avait sur le monde. »



Elle avait commis une erreur lors de sa rencontre précédente avec l'agent de crédit, croit-elle. « J'ai complètement dévié de mon personnage et j'ai parlé de ma vie à moi. » Un employé de la banque a eu un doute, a appelé au travail de la femme que Sarah prétendait être et a découvert le pot aux roses.

La *striker* a été condamnée à deux ans de prison pour ce crime. Ses autres fraudes à l'identité sont restées sous le radar. Elle n'a pas trahi ses complices, mais son arrestation lui a permis de se rendre compte que, au moment où elle avait le plus besoin d'aide, sa « famille » n'était pas là.

Aujourd'hui, quelques années plus tard, Sarah a réparé les ponts avec sa vraie famille. Elle a un emploi, beaucoup moins payant que le crime, mais qu'elle aime. Et lorsque des fraudeurs la contactent à l'occasion pour l'inviter à participer à un coup, elle refuse sans hésiter. « Je ne veux jamais, jamais, jamais redevenir la personne que j'étais, celle qui n'avait aucun attachement à soi-même. »

Dans l'intimité de sa voiture, Sarah m'a confié le nom de sa dernière victime, à qui elle pense parfois. L'ex-*striker* est maintenant consciente des dommages qu'elle a causés. Du calvaire qu'a probablement enduré cette personne pour faire le ménage de son dossier de crédit. Et surtout, de la souffrance psychologique liée au vol d'identité.

« Je t'ai volé une partie de toi », dit Sarah en passant soudainement au tutoiement, comme si elle s'adressait directement à sa victime. « Je t'ai dénudée de ton identité. Je t'ai violée. Ce n'était pas mon intention, tu ne m'avais rien fait, mais je comprends maintenant que c'est comme ça que tu te sens. Je m'excuse. »

LE FRAPPEUR DE GUICHETS

Armando adore le ronronnement du guichet automatique qui distribue les billets. « Chaque fois, c'est le même *thrill* d'entendre le "brrrrrrrrrr" pis de voir le *cash* sortir. C'est comme si c'était magique. » Surtout lorsque l'argent qui sort appartient à quelqu'un d'autre.

Il y a seulement trois choses que je peux révéler au sujet d'Armando. La première : ce n'est pas son vrai nom. La deuxième : il ne fait plus de fraude. Et la troisième : à l'époque où il fraudait, son « travail » était de « frapper des ATM », des guichets.

« On ne les frappe pas avec un bâton pour faire sortir l'argent », rigole Armando. L'idée est plutôt d'utiliser une carte de débit clonée. Une fois au guichet, le fraudeur entre le NIP correspondant et repart avec l'argent, comme le ferait un client normal. Puis il recommence à un autre guichet, et ainsi de suite.

Armando ne faisait pas cavalier seul. Toute une équipe frappait des guichets avec lui, sous la coordination du *boss*.

Les opérations se déroulaient chaque fois de la même façon. Armando rejoignait son équipe dans une ville, jamais la même, choisie par le patron. « Si tu frappes toujours la même place, je te donne une semaine pis c'est sûr que tu te fais attraper. » Le fraudeur a ainsi voyagé au Québec, au Canada et même ailleurs dans le monde pour réaliser ses coups.

C'est le patron qui apportait les listes numériques de cartes bancaires volées. Celles-ci étaient alors encodées une à une sur des cartes vierges. « Tu peux acheter tout le stock pour faire ça sur Amazon », dit l'ex-fraudeur.

D'où venaient les données volées ? Armando l'ignore et ne veut pas le savoir. « Le moins t'en sais, le mieux c'est pour tout le monde. La plupart du temps, tu ne connais même pas les noms des gars avec qui tu travailles. » Au lieu de poser des questions, il se concentrait sur son rôle.

« Moi, ma *job*, c'était de sortir l'argent. Tu pars sur ta *run* avec tes cartes, tu frappes les ATM, pis tu reviens avec l'argent à la base. Là, y a une autre *batch* de cartes qui t'attend. Tu repars avec, tu frappes, pis c'est ça. »

À force de discuter avec Armando, je comprends que son travail était plus complexe que la description qu'il en fait ne le laisse croire. Pour ne pas attirer l'attention, il évitait d'effectuer plus d'un retrait au même endroit, il s'arrêtait dans des cafés et dans des magasins. Il apprenait les NIP par cœur pour ne pas avoir à consulter un bout de papier devant le guichet. Bref, tout afin d'avoir l'air d'un consommateur normal.

Les sommes retirées dépendaient de l'argent que la personne fraudée possédait dans son compte, ainsi que de la limite de retrait quotidienne imposée par sa banque. Si c'était 500 dollars, c'était 500. Si c'était 1 000, « c'était 1 000 dollars pour nous ».

Armando n'oubliera jamais la sensation de voir l'argent sortir du guichet lors de sa première frappe. « Tu n'arrives pas à croire que cet argent-là, il est à toi. T'as l'impression que t'es plus *smart* que les autres, que t'as réussi à "bypasser" le système. » Mais à la longue, la frappe perd de sa magie.

« C'est vraiment beaucoup de travail. À un moment donné, taper des *numbers* sur un ATM, ce n'est pas la chose la plus stimulante au monde… Moi, il y a des fois où je m'ennuyais du

9 à 5 pis d'écouter la télé le soir. » Pendant ses frappes, les divertissements étaient rares, et Armando habitait avec les gars de l'équipe dans une chambre d'hôtel tant et aussi longtemps qu'il restait des cartes à utiliser. « Une opération peut durer trois jours. Une autre peut durer un mois. »

Un mois ! Cela signifie que les fraudeurs s'en prennent ainsi à des milliers de comptes en banque. Devant mon air éberlué, Armando éclate de rire. « Ben oui. Le monde fait du *cash* ! »

Armando touchait un pourcentage des retraits qu'il effectuait, et le reste allait au patron. Certes, un fraudeur peut glisser quelques billets supplémentaires dans ses poches — après tout, il est seul au guichet —, mais c'est risqué. Car si un membre de l'équipe rapporte systématiquement moins d'argent que les autres, il va éveiller les soupçons. Le chef pourrait le fouiller.

De toute façon, Armando était satisfait de ce qu'il gagnait. En quelques opérations seulement, il a fait « plus de 100 000 *for sure* ». Sauf que cet argent venait avec « une énergie bizarre », affirme l'ancien fraudeur. « N'importe qui sait que voler, c'est mal. Tu sais que ce que tu fais, ce n'est pas *straight*. J'avais moins de plaisir à dépenser mon argent. Pis tu ne peux pas le déclarer, alors c'est difficile à investir. »

Après un moment, Armando en est arrivé à la conclusion que le risque n'en valait plus la chandelle. Il s'est mis à refuser les opérations qu'on lui offrait, puis son patron a cessé de l'appeler. Armando ne s'est jamais fait arrêter pour ses crimes.

L'EX-FRAUDEUR DEVENU RAPPEUR

Moto tire longuement sur sa chicha, puis laisse paresseusement sortir l'épaisse fumée blanche, qui monte le long de son visage. « À 350, c'est bon, je les prends », dit le colosse de 26 ans au téléphone. Il négociait une paire d'espadrilles de collection et vient de s'entendre sur un prix. « Il va les porter deux fois seulement ! » m'affirme un de ses amis.

Nous sommes dans un condo du centre-ville de Montréal, où Moto m'a invité en ce mercredi soir, à 22 h, pour parler. Deux autres membres de son cercle sont présents, mais ils ne veulent pas être nommés. Moto, lui, s'en fout. « Je suis un gars *reckless*. Je n'ai peur de rien. Si quelque chose arrive, j'assume les conséquences. Ça, c'est moi. »

De tous les fraudeurs interviewés pour ce reportage, il est le seul à ne pas avoir exigé l'anonymat. Cela dit, Moto n'est pas le prénom qui apparaît sur son certificat de naissance ; c'est son nom de rappeur, celui sous lequel ses amis et son public l'interpellent.

Moto fait du street rap, un type de musique où les artistes se vantent ouvertement des crimes qu'ils ont commis — vente de drogue, violence, proxénétisme, meurtre. Dans le cas de Moto, c'est la fraude.

Le rappeur n'en parle pas seulement dans ses chansons ; sur Instagram, il n'hésite pas à montrer à ses quelque 11 000 abonnés des photos que d'autres auraient le réflexe de cacher. « *Flashback* [de] quand je mettais les ATM en feu », peut-on lire sous un cliché où il exhibe une pile de billets de 20 dollars faisant au moins 15 cm de haut.

S'il écrit au passé, c'est parce que Moto assure avoir tourné la page sur sa vie de fraudeur. « Ça ne sert à rien de garder un pied en dedans [du crime] et un pied en dehors, dit-il. Je risquerais juste de perdre tout ce que j'ai construit. » Mais il ne reniera jamais son ancienne carrière, qui, jure-t-il, a commencé à l'âge de 12 ans.

Moto reconnaît lui-même que, sur papier, son profil socioéconomique correspond au cliché de la criminalité. Sa mère l'a élevé seule, il habitait avec elle dans un HLM et traînait dans les rues de Montréal. Oh ! et pour en ajouter aux préjugés, il est noir. Mais le stéréotype ne va pas plus loin. Il adorait l'école — il a poursuivi ses études jusqu'à l'université, en finances —, était bien entouré et n'a jamais manqué de quoi que ce soit. « Je n'ai pas eu la vie dure. Je me la suis rendue dure moi-même. »

Tout a commencé avec les rappeurs qu'il voyait à la télévision : les beaux vêtements, les voitures, les belles filles… « Je me disais : "Merde, ils vivent bien !" » Il voulait vivre comme eux, et pour cela, il lui fallait de l'argent.

Ses options étaient limitées, s'il se fiait aux exemples autour de lui. Il aurait pu vendre de la drogue, mais il avait remarqué que le vendeur du coin ne « restait jamais là plus d'un an sans entrer en prison ». Il y avait le vol à l'étalage, mais Moto s'est fait pincer à sa première tentative. Puis quelqu'un lui a parlé de la « F », la fraude. « Ça avait l'air plus technique, ça me ressemblait plus. Le gars m'a juste vendu tellement de rêve que j'ai pris dans le rêve. »

Le rappeur boit une rasade de vodka dans un verre de plastique rouge, puis raconte sa première frappe. « C'est comme ça que j'ai eu mon nom, Moto. » Le Razr, un cellulaire fabriqué par l'entreprise Motorola, venait de sortir, et l'adolescent se procurait des téléphones de ce modèle en utilisant les fausses pièces d'identité ou les cartes de crédit clonées du « gars », puis reven-

Avec le recul, Moto se rend compte qu'il touchait des « pinottes » pour ses frappes. « Le gars qui m'a appris mangeait sur ma tête. » N'empêche, ça lui rapportait plus d'argent qu'il n'en avait jamais eu, et c'était bien assez à ses yeux d'adolescent.

dait les appareils. « Je trouvais le téléphone beau, j'en avais plein et j'ai dit : "Bon, je vais m'appeler Motorola." On l'a coupé à Moto — c'était trop long, y avait trop de syllabes. »

Avec le recul, Moto se rend compte qu'il touchait des « pinottes » pour ses frappes. « Le gars qui m'a appris mangeait sur ma tête. » N'empêche, ça lui rapportait plus d'argent qu'il n'en avait jamais eu, et c'était bien assez à ses yeux d'adolescent.

La fraude n'était alors pour lui qu'une façon de s'offrir du bon temps. Mais à 16 ans, après avoir été expulsé de l'équipe de football de son école pour avoir manqué une pratique, il a décidé d'y consacrer tout son nouveau temps libre. « La même tête que j'aurais mise sur un examen, je l'ai mise sur ça. »

Dans la pièce enfumée, je demande à répétition à Moto de m'expliquer à quel type de fraude il s'adonnait. À part pour sa première frappe, je ne reçois que des réponses vagues. « Y a plein de sortes de fraudes. Y en a tellement, je ne peux pas les nommer, ça déborde de la tête. » Ou encore : « Y a plein de types de fraudeurs. Y a celui qui reste chez lui et qui donne du travail aux gens. Y a celui qui apprend aux gens. Y a les affaires plus techniques, comme le *hacking*. »

Il raconte aussi qu'il ne faisait pas ce qu'il considère comme « les affaires de femmes », par exemple aller au magasin en se faisant passer pour quelqu'un d'autre, et qu'il ne fraudait pas les personnes âgées, parce que ça lui « touche le cœur, la conscience ». Mais plus j'essaie d'obtenir de détails sur son passé, plus il se referme.

Si Moto se tait ainsi, c'est en partie pour ne pas s'incriminer, mais surtout pour ne pas « snitcher », c'est-à-dire dénoncer. Je ne lui demande pourtant pas de nommer qui que ce soit. Sauf que, dans le milieu criminel, le simple fait de décrire les techniques employées suffit pour être vu comme un délateur, car cela risque de nuire aux personnes qui les utilisent encore.

Ce dont Moto discute plus volontiers, c'est du fric que la fraude lui a rapporté. « Quand j'ai vu que j'avais tellement d'argent que je ne pouvais plus le tenir dans une main, j'ai dit : "*I made it*, je suis un fraudeur." » Impossible pour lui de préciser combien il a gagné au cours de sa carrière — ce n'est pas comme s'il tenait des livres comptables —, mais il affirme sans hésiter avoir « généré beaucoup plus que la moyenne québécoise ».

Que faisait-il de cet argent ? La même chose que les rappeurs qui le faisaient rêver dans son enfance. « Les beaux vêtements, parler à des belles filles, une voiture, des beaux condos… » Sans oublier les boîtes de nuit. « J'adore les *clubs* ! lance Moto en riant. J'y allais souvent. J'achetais des bouteilles à 200, 300, 400 dollars, et quand il n'y avait plus d'alcool, j'en achetais d'autres. Le lendemain, je mettais les mains dans mes poches et je disais : "*Dude*, j'ai gaspillé tout ça ?" »

Avec le recul, Moto estime que son style de vie était de « l'ignorance totale. Parce que le but du crime, c'est de faire assez d'argent pour en sortir. La plupart des fraudeurs pourraient sortir du crime la première année. Ou même la première semaine ; ça dépend de la frappe. Mais tu deviens victime de l'argent ».

Le rappeur donne l'exemple d'une fraude de 20 000 dollars. « Tu vas dire : "Shit ! j'ai fait 20 000. Je veux 100 000 !" Là, tu fais 100 000, tu veux un demi-million. Tu fais un demi-million, tu veux un million. Ça ne finit jamais, la chaîne. » Jusqu'à ce qu'elle casse.

Le jour où la police a fait irruption chez Moto afin de l'arrêter pour fraude, le colosse n'a pas bronché. « Ils m'ont accusé de plein de choses… »,

dit le rappeur qui, vous l'aurez deviné, refuse de s'étendre sur les détails. Il n'était pas d'accord avec certaines accusations, mais qu'importe, il a « pris [ses] charges. T'as juste à être un homme ».

Lorsqu'il est sorti de prison, Moto était complètement perdu. Le jeune homme est retourné habiter chez sa mère, a recommencé à suivre des cours à l'université. « J'ai réalisé que je n'avais pas envie de vivre une vie de criminel. J'ai pensé à mes plans B, C, D, E, F, G… »

Encore une fois, ce sont les rappeurs qui lui ont montré la voie. Non pas celle de l'argent, mais celle de la musique. Avec l'aide d'amis qui connaissent déjà du succès dans le street rap, Moto s'est lancé. Sa première chanson, « 412 », une collaboration avec le rappeur Le Ice, a été bien reçue par le public et par la critique durant ce printemps pandémique, et il doit lancer un album sous peu. « Je vais l'appeler *Moto Lacroix*. » Une référence au fraudeur Vincent Lacroix, qui a escroqué plus de 100 millions de dollars à 9 200 investisseurs au milieu des années 2000.

CHANGER LE SYSTÈME

Est-il possible de se protéger contre le vol d'identité ? Cette question, je l'ai posée à chacun des fraudeurs interviewés dans ce reportage. La réponse a toujours été la même : impossible.

Certes, vous pouvez compliquer la vie des fraudeurs en évitant de dévoiler des informations personnelles en ligne, en utilisant un gestionnaire de mots de passe, en activant la double authentification de vos comptes en ligne, en installant une boîte de courrier verrouillable, en ne répondant pas aux appels suspects et, pour les plus zélés, en déchiquetant vos documents confidentiels — ce qui, selon le spécialiste en cybersécurité Éric Parent, éviterait à peu près 1 % des fraudes. Mais si un employé d'une entreprise dont vous êtes client laisse filtrer vos informations, tous ces efforts n'auront servi à rien.

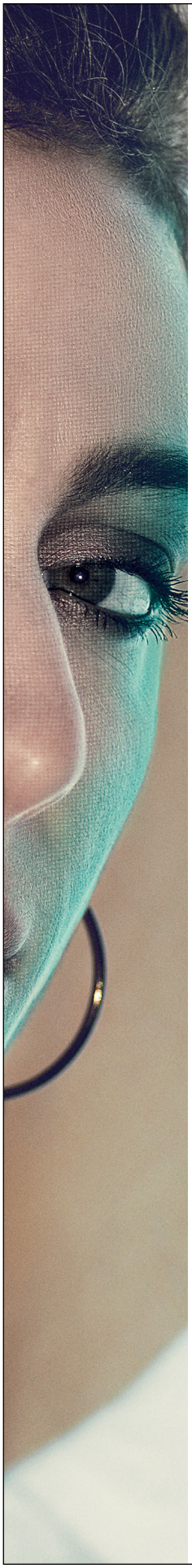
Dans la foulée du scandale de Desjardins, la Coalition Avenir Québec a déposé au cours de l'été 2020 un projet de loi qui donnerait plus de mordant à la Loi sur la protection des renseignements personnels. S'il était adopté, les organisations qui négligent les données de leurs clients — accès non autorisé à des renseignements personnels, perte d'un disque dur contenant des informations, etc. — pourraient se faire imposer des amendes allant jusqu'à 10 millions de dollars, ou 2 % de leur chiffre d'affaires mondial, selon la somme la plus élevée. Et advenant le cas où une entreprise omettrait de divulguer une fuite de données, l'amende pourrait atteindre 25 millions de dollars, ou 4 % du chiffre d'affaires mondial !

Hélas ! pour les gens dont les informations personnelles sont déjà tombées entre les mains de fraudeurs, le projet de loi ne modifiera rien. « Un mot de passe, un numéro de carte de crédit, je peux les changer, dit Éric Parent. Mais le nom de jeune fille de ma mère, ma date de naissance, mon numéro d'assurance sociale, je vais mourir avec. Une fois qu'il y a eu une fuite, c'est terminé. »

Il est possible de se tourner vers les agences de crédit TransUnion et Equifax, qui offrent toutes deux un service payant de surveillance de dossier de crédit. En échange d'une vingtaine de dollars par mois, vous serez automatiquement avisé si une modification est apportée à votre dossier de crédit — les quelque six millions de clients de Desjardins touchés par la fuite ont droit gratuitement au service d'Equifax. Cela

« En 2020, demander à quelqu'un de s'identifier avec des documents falsifiables ou en répondant à des questions dont les réponses se trouvent sur Internet, ça n'a pas de bon sens. »

— Éric Parent, spécialiste en cybersécurité



permet de détecter les fraudes plus rapidement… mais pas de s'en prémunir.

Une autre option, qui a l'avantage d'être gratuite, est de contacter les agences de crédit pour demander l'ajout d'une alerte de fraude à son dossier. Cette alerte indique aux créanciers de redoubler de vigilance avant d'accorder un prêt à votre nom. Le problème, c'est que rien n'oblige lesdits créanciers à respecter cette alerte et à prendre des mesures additionnelles pour vérifier l'identité de l'« emprunteur ».

Pire, les agences de crédit sont souvent utilisées par les criminels eux-mêmes ! Serge m'a ainsi confié que, lorsqu'il recevait des profils d'une taupe, il les filtrait avec Equifax ou TransUnion pour retenir uniquement ceux ayant une bonne cote de crédit. Autrement, son groupe aurait perdu du temps sur des cibles qui n'en valaient pas la peine !

Le meilleur rempart qui pourrait être érigé contre le vol d'identité, croit Éric Parent, serait de revoir notre système d'identification. Car lorsqu'un fraudeur se présente dans un commerce, appelle une banque ou se connecte à un portail gouvernemental, il doit s'identifier afin de se faire passer pour vous. S'il ne parvient pas à le faire, vos données personnelles n'auront plus de valeur à ses yeux.

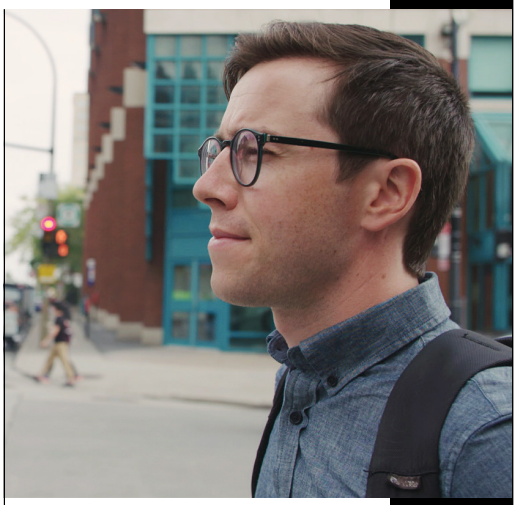
Or, en ce moment, s'identifier est trop simple. « En 2020, demander à quelqu'un de s'identifier avec des documents falsifiables ou en répondant à des questions dont les réponses se trouvent sur Internet, ça n'a pas de bon sens. »

Québec semble d'accord. D'ici 2025, le gouvernement provincial souhaite doter tous les Québécois d'une identité numérique, qui servira à s'identifier autant auprès des autorités que des entreprises privées. Cette identité reposera possiblement sur la chaîne de blocs, la technologie qui sécurise les échanges de cryptomonnaies comme le bitcoin. Près de 42 millions de dollars ont déjà été investis dans le projet, et de nombreux observateurs, dont Éric Parent, craignent que la facture finale atteigne les milliards de dollars.

Mais, peu importe la méthode utilisée, cela n'arrêtera pas les fraudeurs, pense Armando. « Chaque fois qu'il y a un changement, on s'adapte. Eux s'adaptent à nous, pis nous on s'adapte à eux. » Sans fin.

Après deux heures dans le VUS, Sarah a terminé son histoire. Tandis qu'elle me reconduit à ma voiture, dans le stationnement désert du centre commercial, elle me raconte avoir été récemment victime d'une tentative de fraude. « Ça n'a pas fonctionné, dit-elle en riant. J'ai trop un crédit de marde. »

Avoir un mauvais crédit. C'est, à ma connaissance, l'une des rares protections contre la fraude à l'identité qui fonctionne. ◘



LES VOLEURS D'IDENTITÉ À LA TÉLÉ

Suivez la quête de notre journaliste dans le documentaire *Les voleurs d'identité*, réalisé par Christine Chevarie et produit par *L'actualité* et Les Productions Bazzo Bazzo, en collaboration avec Télé-Québec.

Le mercredi 14 octobre, 20 h, à Télé-Québec, puis gratuit en tout temps à telequebec.tv.