Pointages.ca

Mémoire présenté à l'Assemblée Nationale du Québec

Commission parlementaire pour le Projet de loi No 24 Loi protégeant le consommateur contre l'utilisation trompeuse ou frauduleuse de l'identité ou de l'image d'une personne

Sylvain Paquette, Directeur principal, enquêtes et conformité
06/05/2026

Table des matières

1. Introduction

Présentation du contexte du projet de loi 24

Le présent mémoire est soumis dans le cadre de l'étude du projet de loi n° 24 portant sur l'encadrement de l'usurpation d'identité, un phénomène en croissance constante qui constitue aujourd'hui un enjeu majeur de sécurité économique et sociale au Québec.

Ce mémoire est déposé par la société Pointages.ca, entreprise spécialisée dans l'accompagnement des consommateurs en matière de crédit à la consommation, ainsi que dans l'analyse, la détection et la gestion des situations de fraude et d'usurpation d'identité. Par son expertise opérationnelle, Pointages.ca intervient directement auprès de citoyens confrontés aux conséquences concrètes de ces stratagèmes, offrant ainsi une perspective ancrée dans la réalité terrain.

Monsieur Sylvain Paquette, directeur principal – enquête et conformité au sein de l'entreprise, agit à titre d'expert en prévention de la fraude et en usurpation d'identité. À ce titre, il est régulièrement confronté aux mécanismes complexes utilisés par les fraudeurs, ainsi qu'aux lacunes structurelles des systèmes actuels de prévention, de détection et de traitement des cas de fraude.

Pointages.ca accueille favorablement le projet de loi n° 24 et salue l'initiative du législateur visant à renforcer la protection du public face à l'usurpation d'identité. Toutefois, à la lumière de son expérience pratique et des nombreux dossiers traités, l'entreprise estime que certaines bonifications sont nécessaires afin d'assurer une protection réellement efficace des citoyens.

Plus précisément, le présent mémoire vise à :

- Mettre en lumière les mécanismes concrets et structurés de l'usurpation d'identité, tels qu'observés sur le terrain;
- Démontrer les limites des cadres actuels de prévention et de recours;
- Proposer des ajustements législatifs ciblés permettant d'améliorer la protection des consommateurs;
- Et souligner le potentiel de certaines mesures pour générer des retombées économiques positives pour l'État québécois, notamment par une réduction des pertes liées à la fraude et une meilleure responsabilisation des acteurs du marché.

Au-delà de la protection individuelle des victimes, l'usurpation d'identité constitue un phénomène systémique qui fragilise la confiance envers les institutions financières, les plateformes numériques et les mécanismes d'identification. Elle nécessite, en conséquence, une réponse législative structurée, cohérente et adaptée aux réalités technologiques contemporaines.

Le présent mémoire s'inscrit dans cette perspective, en proposant une approche à la fois pragmatique, opérationnelle et juridiquement fondée.

Les constats et recommandations formulés dans le présent mémoire sont directement issus de dossiers réels traités au Québec.

Synthèse des recommandations

Le présent mémoire repose sur trois constats principaux :

- L'usurpation d'identité est aujourd'hui industrialisée et structurée;
- Les mécanismes actuels sont insuffisants et interviennent trop tardivement;
- Les victimes subissent un déséquilibre procédural important.

En réponse à ces constats, trois recommandations prioritaires sont formulées :

1. Immatriculation obligatoire des sites web au Registraire des entreprises du Québec (REQ), afin de réduire l'anonymat numérique et améliorer la traçabilité des acteurs économiques;
2. Mise en place d'un mécanisme de renversement du fardeau de la preuve, par la production d'une déclaration solennelle, permettant de protéger immédiatement les victimes et de rétablir l'équilibre procédural.
3. Encadrement renforcé des plateformes de transfert de fonds, par l'imposition de mécanismes de vérification d'identité accrus et une meilleure traçabilité des transactions.

Ces mesures visent à agir simultanément :

- En amont (protection des données),
- Au cœur du système (flux financiers),
- Et en aval (protection des victimes).

2. Qui sommes-nous

2.1 Présentation de l'entreprise

Pointages.ca est une entreprise québécoise spécialisée dans l'accompagnement des consommateurs en matière de crédit à la consommation, ainsi que dans la détection, l'analyse et la résolution de situations liées à la fraude et à l'usurpation d'identité.

Par son positionnement unique à l'intersection des enjeux financiers, technologiques et juridiques, Pointages.ca intervient directement auprès de citoyens confrontés à des problématiques complexes affectant leur dossier de crédit, leur identité financière et leur réputation économique.

L'entreprise se distingue par une approche opérationnelle fondée sur l'analyse concrète des dossiers, la compréhension des mécanismes de fraude et l'accompagnement personnalisé des victimes dans leurs démarches de régularisation.

2.2 Mission

La mission de Pointages.ca est de sensibiliser, éduquer et accompagner les consommateurs québécois dans la gestion, la compréhension et la restauration de leur identité financière.

À cet égard, l'entreprise poursuit plusieurs objectifs :

- Soutenir les victimes de fraude et d'usurpation d'identité dans leurs démarches administratives et financières;
- Contribuer à l'amélioration de la santé financière des consommateurs;
- Sensibiliser le public aux risques liés à la fraude et aux mécanismes d'usurpation d'identité;
- Agir en tant qu'acteur de prévention en identifiant les failles systémiques exploitées par les fraudeurs;
- Sensibiliser et accompagner les consommateurs dans l'élaboration de budget réaliste tout en prévenant l'endettement.

Cette mission s'inscrit dans une volonté plus large de renforcer la confiance du public envers les institutions financières et les systèmes d'identification.

2.3 Valeurs

Les interventions de Pointages.ca reposent sur des valeurs fondamentales qui guident l'ensemble de ses activités :

Rigueur

Une analyse approfondie et méthodique de chaque dossier, permettant d'identifier avec précision les situations problématiques d'erreur, de fraude et d'anomalies.

Intégrité

Un engagement constant envers la transparence, l'éthique et la protection des intérêts des consommateurs.

Accessibilité

Une volonté de rendre compréhensibles des problématiques souvent complexes, en vulgarisant les enjeux liés au dossier de crédit à la consommation et à l'usurpation d'identité.

Engagement envers le public

Une approche centrée sur la défense des droits des consommateurs et l'amélioration des mécanismes de protection existants.

2.4 Parcours professionnel de l'expert

Monsieur Sylvain Paquette agit à titre de directeur principal – enquête et conformité au sein de Pointages.ca.

Il possède une expertise reconnue en matière de prévention de la fraude, d'usurpation d'identité et de gestion des risques financiers, développée à travers un parcours professionnel riche et diversifié, tant sur le plan opérationnel qu'institutionnel.

À l'échelle professionnelle, Monsieur Paquette est vice-président pour le chapitre du Québec de l'Institut canadien du crédit, une association professionnelle regroupant des directeurs de crédit certifiés à travers le Canada depuis 1928. À ce titre, il contribue activement à l'évolution des pratiques et des standards en matière de gestion du crédit et de prévention des risques.

Il est également l'organisateur du Colloque sur la fraude tenue à Montréal depuis 2018, un événement réunissant des experts issus des milieux financier, juridique, réglementaire et technologique, visant à favoriser le partage de connaissances et l'amélioration des pratiques en matière de lutte contre la fraude.

Au cours de sa carrière, Monsieur Paquette a exercé des fonctions d'enquêteur à la Chambre de la sécurité financière, où il a été impliqué dans l'analyse de dossiers complexes liés à des manquements professionnels et à des situations de fraude.

Il a également été président de l'Académie de formation et de prévention de la fraude, organisme dédié à la formation et à la sensibilisation des acteurs du marché face aux risques émergents en matière de fraude financière.

Par ailleurs, il a agi à titre de dispensateur de formation continue auprès de plusieurs organismes reconnus, notamment l'Autorité des marchés financiers, l'Organisme d'autoréglementation du courtage immobilier du Québec, Professionnels hypothécaires du Canada, le Bureau de la sécurité privé, l'Association professionnelle des notaires du Québec ainsi que le Barreau du Québec.

Dans ce cadre, il a contribué à la formation de nombreux professionnels sur des thématiques telles que :

- La lutte contre la fraude;
- La lutte contre le blanchiment d'argent;
- La fraude immobilière;
- Le vol de titres;
- L'usurpation d'identité;
- La détection de faux documents.

Monsieur Paquette a également réalisé des centaines d'interventions médiatiques afin de commenter l'actualité liée à la fraude, aux vols de données et aux enjeux de cybersécurité, contribuant ainsi à la sensibilisation du grand public.

Il est par ailleurs l'auteur de l'ouvrage La face cachée des bureaux de crédit, publié en 2011, dans lequel il met en lumière certaines pratiques et enjeux systémiques liés à l'évaluation du crédit. Il a dispensé pendant 5 année, une formation de 12 heures accréditée par le programme de formation continue de l'Autorité des marchés financiers en courtage hypothécaire sur la correction des dossiers de crédit consommateur en conformité avec la Loi sur la protection des renseignements personnels dans le secteur privé.

Son expertise repose également sur une expérience personnelle marquante. En 2006, il a lui-même été victime d'une usurpation d'identité orchestrée par des membres du crime organisé, ayant notamment pour objectif de compromettre ses activités professionnelles et de provoquer la fermeture de son entreprise. Cette situation l'a amené à traverser l'ensemble des étapes complexes, longues et souvent déficientes du processus de reconnaissance et de résolution d'une fraude à l'identité.

À cette occasion, il a dû faire valoir ses droits dans un contexte caractérisé par des obstacles administratifs importants, un accès limité à l'information et une difficulté marquée à faire reconnaître sa qualité de victime. Cette expérience lui confère une compréhension directe et approfondie des réalités vécues par les citoyens confrontés à ce type de situation, notamment en ce qui concerne le renversement de facto du fardeau de la preuve et les délais de traitement souvent incompatibles avec les conséquences subies.

Enfin, il a accompagné de nombreux groupes de victimes dans des dossiers de fraude d'envergure, contribuant non seulement à la récupération de sommes importantes, mais également à la judiciarisation de plusieurs affaires, notamment :

- L'affaire Nil Lapointe;
- L'affaire Denis Francoeur;
- L'affaire Mario Goyette;
- L'affaire Benoit Dicaire;
- L'affaire Lovaganza;
- Et plusieurs autres dossiers significatifs.

Ces expériences confèrent à Monsieur Paquette une compréhension approfondie des mécanismes de fraude, tant du point de vue des fraudeurs que des institutions et des victimes. Elles permettent également d'ancrer les constats et recommandations du présent mémoire dans une réalité empirique, directement issue du terrain, notamment en ce qui concerne les stratagèmes structurés d'usurpation d'identité décrits dans ce mémoire.

3. Constat sur l'usurpation d'identité

Les observations issues du terrain permettent de dégager cinq constats fondamentaux :

1. La fraude à l'identité est aujourd'hui industrialisée;
2. Les données personnelles nécessaires sont déjà largement compromises;
3. Les systèmes actuels d'identification sont contournables;
4. Les mécanismes de détection interviennent trop tardivement;
5. Les victimes sont, en pratique, pénalisées par le système.

L'usurpation d'identité constitue aujourd'hui un phénomène en croissance soutenue, dont la complexité et l'ampleur dépassent largement les représentations traditionnelles de la fraude individuelle.

Contrairement à une perception encore répandue, il ne s'agit plus de gestes isolés commis de manière opportuniste, mais bien de stratagèmes structurés, organisés et souvent industrialisés, reposant sur une chaîne d'interventions spécialisées, exploitant à la fois des failles technologiques, des vulnérabilités humaines et des lacunes réglementaires.

L'expérience terrain de Sylvain Paquette, corroborée par l'analyse détaillée des mécanismes de fraude, permet de dégager plusieurs constats fondamentaux qui doivent être pris en compte dans le cadre du projet de loi n° 24.

3.1 Une industrialisation de la fraude à l'identité à grande échelle

Les stratagèmes contemporains d'usurpation d'identité reposent sur une logique structurée, comparable à une chaîne de production.

Chaque étape du processus est désormais :

- Spécialisée (collecte de données, fabrication de faux documents, exploitation financière);
- Optimisée (automatisation, utilisation d'outils technologiques avancés);
- Et interconnectée (réseaux criminels organisés, parfois transnationaux).

L'accès aux données personnelles constitue aujourd'hui une commodité. Les informations sensibles telles que le nom, la date de naissance, l'adresse ou encore les identifiants financiers sont accessibles à faible coût via des marchés clandestins ou à la suite de fuites de données massives.

Cette réalité transforme profondément la nature du risque : il ne s'agit plus de prévenir un incident ponctuel, mais de faire face à un système organisé de captation et d'exploitation de l'identité.

3.2 Une dépendance excessive aux données statiques

Les systèmes actuels d'identification et de validation reposent encore, dans une large mesure, sur l'utilisation de données dites statiques, telles que la date de naissance, le numéro d'assurance sociale, l'adresse ou encore les informations de crédit. Ces éléments sont traditionnellement considérés comme des indicateurs fiables permettant de confirmer l'identité d'un individu.

Or, il apparaît que ces mêmes données sont aujourd'hui parmi les plus vulnérables. Elles font l'objet de nombreuses fuites, circulent abondamment dans les environnements frauduleux et sont facilement accessibles à des acteurs malveillants. Cette réalité crée un décalage préoccupant entre les mécanismes de sécurité en place et le niveau réel de protection offert.

Il en résulte une vulnérabilité structurelle importante : les systèmes d'authentification continuent de s'appuyer sur des informations qui, dans les faits, ne peuvent plus être considérées comme confidentielles ou sécuritaires. Dès lors, un fraudeur disposant d'un ensemble suffisant de données personnelles peut, sans difficulté majeure, franchir les contrôles d'identification et accéder à des services ou produits au nom d'un tiers.

Par ailleurs, la multiplication des fuites de données au fil des années a contribué à créer une véritable abondance d'informations personnelles. Lorsque ces données sont croisées et regroupées, elles permettent de reconstituer, avec un degré de précision élevé, un profil d'identité complet. Cette capacité de reconstruction renforce considérablement l'efficacité des stratagèmes d'usurpation d'identité et met en évidence les limites des modèles actuels de validation.

3.3 Une chaîne de fraude structurée en plusieurs étapes

L'analyse des dossiers traités met en évidence une séquence récurrente d'actions, révélant le caractère méthodique et organisé des stratagèmes d'usurpation d'identité. Loin de relever d'actes isolés ou opportunistes, ces fraudes s'inscrivent dans une logique structurée, reposant sur une succession d'étapes complémentaires et interdépendantes.

De manière générale, ces stratagèmes débutent par la constitution d'un profil complet de la victime, à partir de données personnelles collectées ou acquises par divers moyens. Les fraudeurs procèdent ensuite au détournement des communications, notamment par l'interception du courrier ou la prise de contrôle des moyens de télécommunication, afin de limiter les risques de détection. Cette étape est suivie par la compromission des mécanismes d'authentification, permettant d'accéder aux services ou comptes de la victime.

Parallèlement, les fraudeurs ont recours à la fabrication ou à la contrefaçon de documents crédibles, destinés à satisfaire aux exigences des processus de vérification. Ces éléments leur permettent d'obtenir, dans des délais très courts, des facilités de crédit ou d'ouvrir des comptes financiers. Enfin, les fonds ainsi obtenus sont rapidement monétisés, souvent par l'achat de biens ou leur transfert vers des circuits difficilement traçables.

Cette séquence démontre que l'usurpation d'identité constitue un processus anticipé, structuré et exécuté selon une logique de rendement économique. Il ne s'agit pas d'une fraude improvisée, mais d'une activité organisée visant une maximisation des profits. À cet égard, les observations terrain indiquent que les fraudeurs expérimentés visent des rendements particulièrement élevés, pouvant atteindre des ratios de l'ordre de 4000 % par rapport au coût d'acquisition initial des données, ce qui illustre à la fois l'efficacité et l'attractivité de ce type de criminalité.

3.4 Des mécanismes de détection et de réaction insuffisants

Malgré la mise en place de divers mécanismes de contrôle au sein des institutions financières et des organismes de crédit, d'importantes limites subsistent quant à leur capacité réelle à détecter et à contrer efficacement les stratagèmes d'usurpation d'identité.

D'une part, ces systèmes reposent largement sur des outils automatisés qui, bien qu'efficaces pour traiter un volume élevé de transactions, demeurent insuffisants pour identifier certaines incohérences plus subtiles ou atypiques. D'autre part, l'absence de corrélation efficace entre les différents signaux de fraude, souvent répartis entre plusieurs institutions ou plateformes, empêche une lecture globale des comportements à risque.

À cela s'ajoute un enjeu majeur de temporalité. Les délais de détection sont fréquemment incompatibles avec la rapidité d'exécution des fraudeurs, lesquels agissent de manière coordonnée et accélérée afin de maximiser leurs gains avant toute intervention. En pratique, les mécanismes actuels interviennent trop tardivement, une fois que les opérations frauduleuses ont déjà produit leurs effets.

Par ailleurs, la segmentation des responsabilités entre les différents acteurs, institutions financières, agences de crédit, plateformes technologiques et organismes de régulation contribue à fragmenter les interventions et à ralentir la prise en charge des dossiers.

Dans ce contexte, il n'est pas rare que les situations de fraude ne soient détectées qu'après plusieurs semaines, voire plusieurs mois, souvent au moment où les comptes concernés présentent des défauts de paiement. Cette détection tardive accentue les préjudices subis par les victimes et réduit considérablement les possibilités de récupération des fonds.

3.5 Un renversement de facto du fardeau de la preuve

L'un des constats les plus préoccupants concerne le traitement réservé aux victimes à la suite d'un cas d'usurpation d'identité. En pratique, le fonctionnement actuel du système

tend à inverser les principes fondamentaux de la charge de la preuve, en plaçant implicitement la victime dans une position où elle est présumée responsable jusqu'à démonstration contraire.

Dans ce contexte, la victime se voit contrainte de démontrer qu'elle n'est pas à l'origine des transactions contestées. Elle doit également entreprendre des démarches afin de faire corriger les inscriptions à son dossier de crédit, tout en naviguant dans un environnement administratif complexe impliquant une pluralité d'intervenants. À ces difficultés s'ajoutent des délais souvent importants, notamment en matière d'accès à l'information, qui ralentissent considérablement le traitement des dossiers.

Cette situation est d'autant plus problématique que la victime ne dispose généralement pas des éléments de preuve nécessaires pour soutenir sa contestation. Les informations pertinentes sont majoritairement détenues par les institutions financières et les organismes concernés, auxquels l'accès demeure limité. Par ailleurs, une certaine réticence à reconnaître la fraude peut être observée chez certains acteurs, ce qui contribue à prolonger les démarches et à accentuer le déséquilibre entre les parties. Dans plusieurs cas, cette dynamique mène à une judiciarisation progressive des dossiers, augmentant les coûts et la complexité pour les victimes.

Il en résulte un véritable renversement de facto du fardeau de la preuve, situation incompatible avec les principes d'équité procédurale et particulièrement préjudiciable pour les citoyens. Cette réalité met en lumière la nécessité d'un rééquilibrage du cadre juridique afin de mieux protéger les victimes et d'assurer une répartition plus juste des responsabilités entre les parties.

En pratique, ce fonctionnement revient à présumer implicitement que la victime est responsable jusqu'à preuve du contraire, ce qui constitue une inversion des principes fondamentaux de justice procédurale.

3.6 Des conséquences majeures pour les victimes

Les conséquences de l'usurpation d'identité sont nombreuses et s'inscrivent souvent dans la durée, affectant profondément la situation personnelle, financière et psychologique des victimes.

Sur le plan financier, la détérioration du dossier de crédit constitue l'un des impacts les plus immédiats. Elle entraîne fréquemment des refus d'accès au financement, limitant la capacité des individus à contracter un prêt, à obtenir une carte de crédit ou même à conclure certains engagements contractuels. À cette réalité s'ajoute une atteinte directe à la réputation financière, laquelle peut persister bien au-delà de la résolution du litige.

Par ailleurs, les victimes doivent faire face à un stress psychologique important, découlant à la fois de l'incertitude entourant leur situation et des démarches nécessaires pour rétablir leur identité. Ce processus exige un investissement considérable en temps et en énergie, les obligeant à multiplier les interventions auprès de divers organismes et institutions.

Ces conséquences sont d'autant plus lourdes que les délais de résolution peuvent s'étendre sur plusieurs mois, voire plusieurs années. L'expérience terrain, corroborée par le vécu personnel de l'expert ayant contribué au présent mémoire, démontre que le parcours de rétablissement est généralement complexe, fragmenté et insuffisamment soutenu par les mécanismes existants.

Ainsi, au-delà des pertes financières, l'usurpation d'identité engendre un préjudice global, durable et souvent sous-estimé, qui justifie pleinement une intervention législative adaptée et renforcée.

3.7 Un enjeu systémique nécessitant une réponse législative adaptée

L'ensemble des constats présentés démontre clairement que l'usurpation d'identité ne peut plus être considérée comme un phénomène marginal ou isolé. Elle s'inscrit désormais dans une réalité beaucoup plus large, aux répercussions multiples et interconnectées.

Sur le plan économique, elle engendre des pertes financières considérables, tant pour les citoyens que pour les institutions. Sur le plan social, elle contribue à éroder la confiance du public envers les systèmes financiers, les plateformes numériques et les mécanismes d'identification. À cela s'ajoute une dimension institutionnelle, dans la mesure où la répétition de ces stratagèmes fragilise la crédibilité et l'efficacité des dispositifs actuels de vérification d'identité. Enfin, la présence croissante de réseaux criminels organisés confère à ce phénomène une dimension sécuritaire préoccupante.

Dans ce contexte, l'usurpation d'identité doit être appréhendée comme un enjeu systémique nécessitant une réponse globale, cohérente et adaptée aux réalités contemporaines. Une intervention législative ciblée apparaît non seulement justifiée, mais urgente afin de corriger les lacunes observées et de mieux protéger le public.

Le projet de loi n° 24 constitue, à cet égard, une avancée significative. Il traduit une volonté claire du législateur de s'attaquer à cette problématique. Toutefois, à la lumière des éléments exposés dans le présent mémoire, certaines bonifications apparaissent nécessaires afin d'assurer une protection véritablement efficace et durable des citoyens québécois.

3.8 Une transformation profonde du profil et des modes d'action des fraudeurs

Au cours des trente dernières années, le contexte criminologique dans lequel s'inscrit l'usurpation d'identité a connu une transformation majeure, tant au Québec qu'à l'échelle internationale. Historiquement associée à des individus isolés ou à des réseaux limités, la fraude à l'identité s'inscrit désormais dans un écosystème criminel beaucoup plus vaste, structuré et interconnecté. Les organisations criminelles disposent aujourd'hui de moyen

colossal souvent plus élevé que ce que dispose l'état elle-même pour lutter contre ce phénomène.

3.8.1 Une intégration dans les grandes économies criminelles mondiales

Les activités frauduleuses en ligne, incluant l'usurpation d'identité, doivent désormais être analysées dans une perspective élargie, en tenant compte des principales sources de revenus de la criminalité à l'échelle mondiale. Elles ne constituent plus des phénomènes isolés, mais s'inscrivent dans des dynamiques économiques criminelles globales.

À cet égard, il est généralement reconnu que certaines activités dominent les économies illicites contemporaines, notamment la contrefaçon, le trafic de stupéfiants et le trafic de personnes. Ces secteurs génèrent des flux financiers considérables et structurent en grande partie les réseaux criminels organisés.

Dans ce contexte, la fraude numérique et l'exploitation des données personnelles jouent un rôle de plus en plus central. Elles constituent des leviers complémentaires permettant non seulement de générer des revenus additionnels, mais également de soutenir d'autres activités illicites. Ces mécanismes facilitent notamment le financement des opérations criminelles et contribuent à la circulation et à la dissimulation de capitaux à travers différents canaux.

Ainsi, l'usurpation d'identité ne doit pas être appréhendée comme un phénomène autonome. Elle s'intègre pleinement dans une économie criminelle globale, diversifiée et interconnectée, où les différentes formes de criminalité se renforcent mutuellement.

3.8.2 Une multiplication des acteurs criminels

Le paysage criminel contemporain se caractérise par une diversification et une multiplication des acteurs impliqués, aux profils et aux modes d'organisation variés. Il ne se limite plus à des structures criminelles traditionnelles, mais englobe désormais un ensemble hétérogène d'intervenants, allant des organisations criminelles fortement structurées aux groupes opérant à l'échelle transnationale, en passant par des entités engagées dans des activités de financement illicite, ainsi que des individus agissant de manière autonome, souvent qualifiés de « loups solitaires ».

Cette pluralité d'acteurs s'appuie largement sur les opportunités offertes par le numérique. Les technologies permettent aujourd'hui de mener des opérations de fraude à distance, souvent à partir de juridictions étrangères, ce qui complexifie de manière significative les mécanismes d'intervention, de coopération internationale et de poursuite judiciaire. Cette déterritorialisation du crime contribue à accroître le sentiment d'impunité et à réduire l'efficacité des cadres réglementaires traditionnels.

Par ailleurs, certaines organisations criminelles ont progressivement intégré la fraude en ligne comme une source de financement stratégique. Cette évolution s'explique notamment par un rapport risque-rendement particulièrement avantageux : comparativement à d'autres formes de criminalité, les activités frauduleuses numériques présentent un risque d'interception plus faible, tout en offrant des possibilités de gains élevés et rapides.

Cette réalité est confirmée par les observations des autorités spécialisées. À titre d'exemple, dans son rapport de 2024, le Service canadien de renseignements criminels a identifié environ 2 000 groupes de crime organisé actifs au Canada, incluant des organisations de tailles variables, allant de structures établies à des groupes émergents ou moins formalisés. Cette donnée illustre l'ampleur du phénomène et la complexité du tissu criminel dans lequel s'inscrit désormais la fraude à l'identité.

3.8.3 Une dimension géopolitique et économique accrue

Le développement de la cybercriminalité s'inscrit dans un contexte international en profonde mutation, marqué par des enjeux à la fois économiques, stratégiques et géopolitiques. L'environnement numérique contemporain est caractérisé par la présence de juridictions soumises à des sanctions économiques, par l'émergence de capacités offensives dans le cyberespace, ainsi que par l'utilisation croissante de moyens numériques à des fins d'influence ou de déstabilisation.

Dans ce cadre, certaines activités frauduleuses peuvent s'inscrire, de manière directe ou indirecte, dans des dynamiques d'affaiblissement économique. En ciblant notamment les citoyens et les institutions financières, ces pratiques contribuent à fragiliser les systèmes économiques et à éroder la confiance envers les infrastructures numériques.

Sans qu'il soit nécessaire de généraliser ces phénomènes à l'ensemble des activités frauduleuses, il demeure essentiel de reconnaître que le contexte actuel favorise une déterritorialisation du crime. Les frontières traditionnelles du droit deviennent ainsi moins efficaces face à des acteurs capables d'opérer à distance, à partir de juridictions multiples, souvent hors de portée des mécanismes classiques d'intervention.

Cette évolution impose une adaptation des cadres législatifs et des outils de régulation, afin de mieux répondre à une criminalité désormais transnationale, mobile et technologiquement avancée.

3.8.4 Une montée des fraudes opportunistes et ciblées

Parallèlement aux réseaux criminels structurés, on observe une augmentation notable d'acteurs opérant de manière plus marginale, mais néanmoins efficace. Ces individus ou petits groupes exploitent les outils numériques accessibles pour mettre en œuvre des stratagèmes frauduleux reposant sur des approches plus ciblées et personnalisées.

Ces pratiques prennent notamment la forme de campagnes d'hameçonnage dirigées vers des profils spécifiques, de fraudes de faible envergure en volume mais d'une grande précision dans leur exécution, ainsi que de techniques d'ingénierie sociale adaptées aux caractéristiques particulières des victimes visées. En s'appuyant sur une connaissance fine des comportements et des vulnérabilités individuelles, ces acteurs parviennent à maximiser l'efficacité de leurs interventions malgré des moyens plus limités.

Cette évolution contribue à complexifier davantage la lutte contre la fraude, en combinant deux dynamiques distinctes mais complémentaires. D'une part, des opérations de grande envergure, souvent industrialisées, permettent de toucher un large volume de victimes. D'autre part, des approches ciblées, fondées sur la précision et la personnalisation, augmentent significativement les taux de réussite.

Cette coexistence entre volume et précision rend les stratagèmes frauduleux plus difficiles à détecter, à anticiper et à contrer, en exigeant des réponses à la fois globales et adaptées aux réalités spécifiques des différentes formes de fraude.

3.8.5 Une capacité accrue de blanchiment et d'infiltration de l'économie légale

Les revenus générés par les activités frauduleuses et criminelles ne demeurent pas en marge de l'économie formelle. Ils doivent être intégrés dans des circuits légitimes, ce qui engendre des dynamiques particulièrement préoccupantes pour l'intégrité des marchés et des institutions.

À cette fin, les organisations criminelles mettent en place diverses stratégies leur permettant d'infiltrer l'économie légale. Elles procèdent notamment à des investissements dans des entreprises apparemment légitimes, telles que des établissements du secteur de l'hôtellerie, de la restauration ou des services. Elles acquièrent également des actifs immobiliers, lesquels constituent un vecteur privilégié pour la consolidation et la dissimulation de capitaux d'origine illicite.

Par ailleurs, l'utilisation de structures commerciales permet de masquer l'origine des fonds et de faciliter leur circulation dans l'économie formelle. Ces mécanismes contribuent directement à des opérations de blanchiment d'argent, en complexifiant la traçabilité des flux financiers et en réduisant l'efficacité des contrôles traditionnels.

Ces pratiques ont pour effet de brouiller progressivement la frontière entre économie légale et économie illégale. Elles exercent une pression significative sur l'intégrité des marchés, en introduisant des capitaux d'origine criminelle dans des secteurs économiques légitimes, ce qui peut fausser la concurrence, affaiblir les mécanismes de régulation et miner la confiance envers les institutions.

3.8.6 Des risques pour les institutions et l'État de droit

Au-delà des impacts économiques, les dynamiques associées à la fraude et à l'usurpation d'identité soulèvent des enjeux beaucoup plus larges, qui touchent directement au fonctionnement des institutions et à la stabilité de l'État de droit.

Ces phénomènes comportent notamment des risques accrus de corruption, dans la mesure où les capitaux d'origine criminelle peuvent être utilisés pour influencer certains acteurs ou processus décisionnels. Ils peuvent également donner lieu à des tentatives d'influence dans divers secteurs stratégiques, fragilisant ainsi l'indépendance et l'intégrité de certains mécanismes institutionnels.

Par ailleurs, la répétition et la sophistication de ces stratagèmes contribuent à éroder la confiance du public envers les institutions financières, les organismes de régulation et, plus largement, envers les mécanismes de protection en place. Cette perte de confiance constitue en elle-même un enjeu majeur, puisqu'elle affaiblit la légitimité des systèmes sur lesquels repose l'économie.

Enfin, la complexification croissante des modes opératoires rend le travail des autorités de régulation et des organismes d'application de la loi de plus en plus difficile. Ces derniers doivent composer avec des structures criminelles adaptatives, des technologies en constante évolution et des juridictions multiples, ce qui alourdit les processus d'enquête et limite l'efficacité des interventions.

Dans ce contexte, l'usurpation d'identité apparaît comme une véritable porte d'entrée vers des problématiques systémiques plus vastes, touchant à la sécurité économique, à la stabilité des institutions et à l'intégrité globale du système. Elle ne peut donc être traitée de manière isolée, mais doit être intégrée dans une réflexion plus large sur la protection de l'État de droit à l'ère numérique.

3.8.7 Implications pour le législateur

L'évolution du profil des fraudeurs et de leurs modes d'action impose une adaptation en profondeur du cadre législatif. Les transformations observées, tant sur le plan technologique qu'organisationnel, rendent désormais inadéquates les approches strictement réactives ou centrées sur le traitement de cas individuels.

Dans ce contexte, il devient essentiel de reconnaître pleinement la dimension systémique du phénomène. L'usurpation d'identité et les fraudes connexes ne relèvent plus d'incidents isolés, mais s'inscrivent dans des dynamiques structurées qui nécessitent une réponse globale et coordonnée.

Cette réalité commande également un renforcement de la collaboration entre les différents acteurs impliqués, qu'il s'agisse des institutions financières, des organismes de régulation, des plateformes numériques ou des autorités publiques. Une meilleure coordination apparaît indispensable afin d'assurer une circulation efficace de l'information et une réponse cohérente aux stratagèmes frauduleux.

Par ailleurs, les mécanismes de prévention et de détection doivent être adaptés afin de tenir compte des nouvelles formes de fraude, caractérisées par leur rapidité d'exécution et leur sophistication croissante. Cela implique notamment de repenser les outils existants et d'intégrer des approches plus proactives.

Enfin, une attention particulière doit être portée à l'encadrement des vecteurs utilisés par les fraudeurs, qu'ils soient de nature numérique, financière ou commerciale. Ces canaux constituent des points d'entrée critiques dans la chaîne de fraude et doivent faire l'objet de mesures spécifiques afin de réduire leur exploitation à des fins illicites.

Dans son ensemble, cette évolution appelle à une réponse législative structurée, cohérente et résolument tournée vers l'avenir, capable de s'adapter à un environnement criminel en constante mutation.

3.8.8 Une diversification des motivations et des usages de l'usurpation d'identité

L'analyse des dossiers traités met en lumière une diversification croissante des contextes dans lesquels l'usurpation d'identité est utilisée. Si une proportion importante des cas demeure motivée par un objectif financier direct, certaines situations révèlent des usages plus ciblés et stratégiques.

D'une part, il a été observé que certains cas d'usurpation d'identité sont liés à des contextes personnels, notamment dans des situations impliquant d'anciens conjoints ou conjointes. Dans ces cas, l'usurpation d'identité peut être utilisée comme un outil de représailles, dans une logique de vengeance, visant à causer un préjudice financier ou réputationnel à la victime.

D'autre part, certaines situations analysées démontrent que l'usurpation d'identité peut être utilisée par des acteurs organisés dans un contexte économique ou concurrentiel. Des groupes criminels peuvent ainsi recourir à ce type de stratagème afin de nuire à un compétiteur, notamment en compromettant sa situation financière, en détériorant son accès au crédit ou en perturbant ses opérations.

Dans certains cas, ces pratiques peuvent s'inscrire dans une logique plus large visant à affaiblir une entreprise afin de créer des conditions favorables à son acquisition à moindre coût ou à la prise de contrôle de certains actifs.

Ces observations démontrent que l'usurpation d'identité ne constitue pas uniquement un outil de fraude financière, mais peut également être utilisée comme un levier de déstabilisation personnelle, économique ou concurrentielle.

4. Analyse du phénomène

4.1 La source du problème en amont

L'usurpation d'identité ne prend pas naissance au moment où la fraude est commise, mais bien en amont, dès les phases de collecte, de stockage et de circulation des données personnelles. Le phénomène s'inscrit dans un environnement informationnel où les renseignements permettant d'identifier un individu — tels que le nom, la date de naissance, l'adresse, le numéro d'assurance sociale ou encore les données financières — sont aujourd'hui largement diffusés, souvent sans encadrement suffisant.

Cette situation résulte de plusieurs facteurs convergents. La multiplication des brèches de données au sein d'organisations publiques et privées expose régulièrement des informations sensibles. À cela s'ajoute une tendance à la conservation excessive de ces données, parfois au-delà des besoins opérationnels réels. L'absence de normes uniformes en matière de protection et de gestion des renseignements personnels contribue également à créer des disparités dans les pratiques, accentuant les vulnérabilités.

Par ailleurs, la circulation de données sur des plateformes numériques difficilement contrôlables, combinée à une sensibilisation encore limitée des citoyens quant aux risques liés à la divulgation d'informations personnelles, favorise la dispersion et l'accessibilité de ces renseignements.

Dans un tel contexte, les fraudeurs peuvent, à faible coût et avec une relative facilité, reconstituer des profils complets et exploitables. L'usurpation d'identité ne doit donc pas être perçue comme une anomalie du système, mais plutôt comme une conséquence prévisible d'un environnement où la gestion des données personnelles demeure insuffisamment encadrée

4.2 Les étapes d'une usurpation d'identité (Voir le tableau en annexe)

L'analyse des dossiers traités met en évidence une séquence d'actions structurées, démontrant que l'usurpation d'identité repose sur un processus méthodique et planifié. Ce processus peut être résumé comme suit :

1. Acquisition des données personnelles

Les fraudeurs constituent un profil détaillé de la victime à partir de sources multiples (fuites de données, hameçonnage, ingénierie sociale, sources ouvertes).

2. Détournement des communications

Le contrôle des communications (courrier, téléphone) permet d'intercepter les informations critiques et de retarder la détection.

3. Prise de contrôle des outils d'authentification

L'acquisition ou le détournement d'un numéro de téléphone ou d'une adresse courriel personnelle permet de contourner les mécanismes de sécurité, notamment l'authentification multi facteur. Dans certain cas, les fraudeurs ont souvent recours à des complices dans les boutiques de téléphonie cellulaire. L'adresse courriel personnelle peut également être compromise.

4. Collecte d'informations complémentaires

Des techniques d'ingénierie sociale sont utilisées pour obtenir les données manquantes et renforcer la crédibilité du profil frauduleux.

5. Fabrication de faux documents

Les fraudeurs produisent des documents contrefaits permettant de franchir les étapes de vérification.

6. Demandes de crédit

Des demandes multiples sont soumises auprès de différentes institutions dans un court laps de temps. Les fraudeurs connaissent les failles au niveau des processus d'approbation de certaine institution financière et en tire avantage.

7. Obtention de facilités de crédit

Les contrôles étant souvent insuffisants, les demandes sont acceptées. Les instruments de crédit sont envoyés directement au fraudeur ou ce dernier peut se présenter chez le commerçant pour prendre possession du bien acheté frauduleusement.

8. Monétisation rapide

Les fonds sont convertis en liquidités ou en actifs facilement transférables.

9. Défaut de paiement

Aucun remboursement n'est effectué par le débiteur. Pendant les 120 jours de délinquance qui vont suivre, l'institution financière tente de joindre son débiteur au numéro de téléphone fourni sur la demande de crédit mais sans résultat. Le compte est ensuite transféré en recouvrement pour mauvaise créance.

10. Mauvaise qualification par les institutions

Les dossiers sont initialement traités comme des défauts de paiement plutôt que comme des fraudes. Ils sont ainsi relayés au rang de mauvaises créances.

11. Transfert du fardeau sur la victime

La victime doit démontrer qu'elle n'est pas responsable des transactions. Ce qui s'avère complexe car cette dernière ignore le stratagème utilisé.

Constat clé

Cette séquence démontre que :

- La fraude est anticipée et structurée;
- Les systèmes actuels sont contournables;
- La détection intervient trop tardivement;
- La réponse institutionnelle est inadéquate.

4.3 L'impact sur la vie des victimes

Les conséquences de l'usurpation d'identité dépassent largement les pertes financières immédiates et s'inscrivent souvent dans une dynamique durable, affectant de manière significative la vie personnelle, professionnelle et financière des victimes.

Sur le plan financier, celles-ci subissent fréquemment une détérioration importante de leur dossier de crédit, ce qui compromet leur capacité à accéder à du financement. Cette situation peut également entraîner des refus de location ou même d'emploi, dans la mesure où certaines décisions reposent en partie sur l'évaluation du profil financier des individus. L'atteinte à la réputation financière qui en découle peut persister longtemps, même après la reconnaissance de la fraude.

Au-delà de ces impacts économiques, les victimes font face à un stress psychologique considérable, alimenté par l'incertitude, la perte de contrôle et les conséquences imprévisibles de la fraude. Le processus de rétablissement exige en effet un investissement important en temps et en énergie, les obligeant à entreprendre de multiples démarches auprès de divers intervenants, notamment les institutions financières, les agences d'évaluation du crédit et les autorités réglementaires.

Ce parcours est généralement long, complexe et fragmenté, en raison du manque de coordination entre les acteurs et des délais de traitement souvent importants. Dans certains cas, les conséquences peuvent se prolonger sur plusieurs années, pouvant aller jusqu'à une période de dix à quinze ans avant que la situation ne soit entièrement régularisée.

Ainsi, l'usurpation d'identité engendre un préjudice global, profond et durable, qui justifie pleinement la mise en place de mécanismes de protection plus efficaces et mieux adaptés à la réalité vécue par les victimes.

4.4 Les recours possibles pour les victimes

En théorie, les victimes d'usurpation d'identité disposent de plusieurs recours afin de contester les transactions frauduleuses et de rétablir leur situation. Elles peuvent notamment s'adresser aux institutions financières concernées pour contester les opérations effectuées en leur nom, demander la correction des informations inscrites à leur dossier auprès des agences d'évaluation du crédit, déposer des plaintes auprès des autorités compétentes ou encore exercer des recours auprès de la Commission d'accès à l'information. Dans certains cas, des recours judiciaires peuvent également être envisagés.

Toutefois, l'exercice concret de ces recours révèle d'importantes limites. Les victimes doivent généralement entreprendre seules l'ensemble des démarches, en l'absence d'un accompagnement structuré ou d'un organisme dédié à la prise en charge globale de leur situation. Elles sont confrontées à des délais souvent importants, à une complexité administrative marquée ainsi qu'à un accès restreint à l'information pertinente, laquelle est principalement détenue par les institutions.

À ces difficultés s'ajoute une problématique récurrente liée à la reconnaissance même de la fraude. Les victimes éprouvent fréquemment des obstacles à faire valoir leur situation, ce qui prolonge les démarches et accentue le sentiment d'injustice.

Dans ce contexte, le système actuel tend à laisser les victimes livrées à elles-mêmes, les contraignant à naviguer dans un environnement procédural complexe, fragmenté et peu adapté à la réalité des situations d'usurpation d'identité.

4.5 Le cas Marie-Claude Barette et les personnalités publiques : illustration d'un stratagème structuré d'usurpation d'identité

Dans le cadre de la préparation du présent mémoire, Madame Marie-Claude Barrette a accepté de contribuer en partageant son expérience personnelle en matière d'usurpation d'identité, notamment dans le contexte de l'utilisation frauduleuse de son image sur les plateformes numériques, incluant Facebook.

Son témoignage permet d'illustrer de manière concrète les mécanismes décrits dans cette section, ainsi que les impacts réels de ces stratagèmes, tant sur le plan personnel que sur le plan public.

Nous tenons à souligner sa contribution et à la remercier pour sa collaboration à l'élaboration du présent mémoire.

Dans ce contexte, l'expert Sylvain Paquette a rédigé un rapport d'expertise approfondi portant sur l'analyse du stratagème de fraude dont a été victime Madame Marie-Claude Barrette.

Ce rapport a constitué un élément structurant de la démarche entreprise, en servant notamment de base analytique à l'action collective déposée, laquelle est actuellement en attente d'autorisation.

L'usurpation d'identité impliquant des personnalités publiques constitue aujourd'hui l'une des formes les plus sophistiquées et les plus efficaces de fraude en ligne. Elle repose sur l'exploitation stratégique de la notoriété et de la crédibilité de figures médiatiques afin de renforcer la confiance des victimes potentielles. Le cas de Marie-Claude Barrette illustre de manière particulièrement éclairante un stratagème complexe, structuré et reproductible, tel que documenté dans un rapport d'expertise détaillé.

4.5.1 Une stratégie fondée sur la crédibilité et la confiance

Le stratagème repose avant tout sur un principe fondamental : l'exploitation de la confiance du public envers une personnalité reconnue. Les fraudeurs sélectionnent délibérément des figures publiques présentant un haut niveau de crédibilité, une présence médiatique active, une image d'intégrité et une proximité avec leur auditoire.

Dans ce contexte, Marie-Claude Barrette représentait une cible particulièrement efficace, en raison de sa notoriété et du lien de confiance qu'elle entretient avec le public québécois. L'utilisation de son image permet ainsi de réduire les mécanismes de méfiance chez les victimes et d'augmenter significativement la crédibilité du stratagème.

4.5.2 Une mise en scène frauduleuse sophistiquée

Le stratagème repose ensuite sur la construction d'un narratif entièrement fictif, mais élaboré de manière à paraître plausible et convaincant. Les fraudeurs s'appuient sur des éléments réels issus de l'actualité médiatique afin de renforcer l'illusion de légitimité.

Ils peuvent notamment s'inspirer d'apparitions télévisuelles connues, telles qu'une entrevue à l'émission « Tout le monde en parle », pour créer un scénario fictif reposant sur une prétendue révélation ou une entrevue censurée. Ce récit est ensuite appuyé par la rédaction de faux articles imitant l'apparence de médias reconnus, l'utilisation d'images authentiques sorties de leur contexte et l'intégration d'éléments sensationnalistes destinés à capter l'attention.

Dans le cas analysé, un faux article laissait croire que la personnalité publique aurait dévoilé, lors d'une entrevue, un système permettant de générer des revenus importants grâce aux cryptomonnaies. Ce type de contenu constitue une forme avancée de fausse représentation, renforcée par des techniques de manipulation psychologique, notamment en jouant sur la curiosité, le sentiment d'urgence et la promesse d'un gain financier rapide.

4.5.3 Une instrumentalisation des plateformes numériques

Le stratagème ne se limite pas à la création de contenu frauduleux. Il repose également sur une diffusion massive et ciblée, rendue possible par l'utilisation des plateformes numériques.

Les fraudeurs ont recours à des publicités payantes sur les réseaux sociaux, à des comptes falsifiés ou usurpés, ainsi qu'à des mécanismes algorithmiques permettant de cibler des profils spécifiques, souvent plus vulnérables. Ils exploitent également des techniques d'optimisation de la visibilité afin d'accroître la portée de leurs contenus.

Les utilisateurs sont ainsi redirigés vers de faux articles, puis vers des plateformes transactionnelles frauduleuses conçues pour capter des informations personnelles ou inciter à des investissements.

Le rapport d'expertise réalisé dans le cadre de l'affaire Marie-Claude Barrette met en évidence que ces opérations ne relèvent pas d'initiatives isolées, mais bien de réseaux

organisés disposant de ressources importantes et d'une connaissance approfondie des outils numériques. Cette structuration confirme le caractère industriel et hautement stratégique de ce type de fraude.

4.5.4 Une chaîne de conversion frauduleuse en plusieurs phases

Le stratagème s'inscrit dans une logique de conversion progressive des victimes, structurée en plusieurs étapes :

Étape 1 : Attirer l'attention, par un contenu sensationnaliste utilisant une personnalité publique.

Étape 2 : Générer de la crédibilité, par l'imitation de médias reconnus et l'utilisation d'images authentiques.

Étape 3 : Rediriger vers une plateforme, via des liens intégrés dans les articles ou publicités.

Étape 4 : Collecter les données personnelles (Nom, téléphone, courriel — première étape d'exploitation).

Étape 5 : Établir un contact humain (Appels téléphoniques par de faux conseillers pour renforcer la confiance).

Étape 6 : Inciter à un premier investissement, souvent faible (ex. : quelques centaines de dollars).

Étape 7 : Simuler des gains, par affichage de rendements fictifs pour encourager des investissements plus importants.

Étape 8 : Maximiser l'exploitation financière par pression psychologique pour augmenter les montants investis (technique dite de « pig butchering »).

Étape 9 : Disparaître ou bloquer les retraits, rendant les fonds irrécupérables.

Étape 10 : Réexploiter la victime par des tentatives ultérieures de fraude (faux recouvrement de fonds, frais additionnels).

Étape 11 : Monétiser les données personnelles, revente ou réutilisation des informations collectées.

Ce modèle démontre une logique industrielle de fraude, avec des taux de conversion et des volumes significatifs de victimes.

4.5.5 Une pluralité de victimes

Le stratagème ne vise pas uniquement les consommateurs. Trois catégories principales de victimes sont identifiées :

1. Les personnalités publiques

- Atteinte à la réputation;
- Perte de crédibilité;
- Harcèlement et pression sociale;
- Frais juridiques.

2. Les médias

- Utilisation frauduleuse de leur image;
- Perte de confiance du public;
- Association à des contenus trompeurs.

3. Les citoyens

- Pertes financières;
- Vol de données personnelles;
- Usurpation de comptes;
- Conséquences psychologiques et économiques importantes.

Le rapport estime que ces stratagèmes peuvent toucher des dizaines de milliers de victimes, avec des pertes financières cumulées très importantes.

4.5.6 Un enjeu majeur de responsabilité des plateformes

Le cas analysé met en lumière une problématique centrale liée au rôle et à la responsabilité des plateformes numériques dans la diffusion de contenus frauduleux. Il apparaît que des publicités trompeuses continuent d'être diffusées malgré des signalements répétés, et que les mécanismes de retrait des contenus demeurent souvent insuffisamment rapides pour limiter les préjudices.

Cette situation s'inscrit dans un modèle économique largement fondé sur la publicité, incluant celle émanant d'acteurs malveillants, ce qui soulève des enjeux quant à l'encadrement des pratiques et à la responsabilité des intermédiaires numériques.

Le rapport d'expertise rédigé dans le cadre du dossier de Marie-Claude Barrette met en évidence que ces éléments peuvent engager la responsabilité des plateformes à plusieurs niveaux. Ils soulèvent notamment des questions en matière de responsabilité civile, en raison des dommages causés par la diffusion de contenus frauduleux, ainsi que des enjeux de négligence dans la gestion des signalements et des mécanismes de contrôle. Dans certains cas, ces pratiques pourraient également s'apparenter à une forme d'aveuglement volontaire, dans la mesure où des activités manifestement frauduleuses continuent d'être tolérées malgré leur identification.

Dans ce contexte, la question de la responsabilité des plateformes ne peut être écartée et doit être pleinement intégrée à la réflexion législative, compte tenu de leur rôle central dans la propagation de ces stratagèmes. Cette réalité soulève la nécessité d'un encadrement législatif clair visant à responsabiliser les plateformes quant à la diffusion de contenus manifestement frauduleux.

4.5.7 Portée pour le projet de loi nº 24

L'analyse du cas présenté permet de tirer des enseignements significatifs quant à la nature et à l'ampleur du phénomène d'usurpation d'identité. Elle démontre clairement que celui-ci ne peut plus être appréhendé comme une problématique individuelle, limitée à des situations isolées, mais qu'il s'inscrit désormais dans des dynamiques beaucoup plus larges et structurées.

En effet, les stratagèmes observés reposent sur l'intervention de réseaux organisés, capables d'exploiter de manière systématique des infrastructures numériques légitimes afin de diffuser des contenus frauduleux à grande échelle. Cette réalité confère à l'usurpation d'identité une portée économique et sociale considérable, en raison des pertes financières générées et de l'atteinte à la confiance du public envers les systèmes numériques et les institutions.

Dans ce contexte, le cas analysé met en évidence la nécessité d'une intervention législative renforcée. Il souligne l'importance d'un encadrement accru des plateformes numériques, afin de limiter leur utilisation à des fins frauduleuses, ainsi que la mise en place de mécanismes plus efficaces de détection et de retrait des contenus trompeurs. Il appelle également à une responsabilisation accrue des intermédiaires, dont le rôle dans la diffusion de ces stratagèmes est central, ainsi qu'à un renforcement des mesures de protection offertes aux victimes.

Ces éléments doivent être pleinement pris en compte dans le cadre de l'étude du projet de loi nº 24, afin d'assurer une réponse adaptée à la réalité contemporaine de l'usurpation d'identité.

5. Recommandations législatives

5.1 L'immatriculation obligatoire des sites web auprès du Registraire des entreprises du Québec (REQ)

5.1.1 Constat

L'analyse des stratagèmes de fraude met en évidence une utilisation massive d'outils numériques permettant aux fraudeurs d'opérer dans un environnement largement dématérialisé et difficilement traçable. Ceux-ci ont fréquemment recours à des sites web anonymes, à des noms de domaine multiples et renouvelés, ainsi qu'à des plateformes transactionnelles opérant sans encadrement clair.

Cette absence de traçabilité constitue un obstacle majeur à plusieurs égards. Elle complique considérablement l'identification des auteurs de fraude, limite la capacité d'intervention des autorités et réduit l'efficacité des mécanismes de protection offerts aux consommateurs. En

pratique, elle permet aux fraudeurs de se soustraire aux cadres réglementaires existants et de multiplier les opérations illicites sans risque immédiat de repérage.

5.1.2 Recommandation

Dans ce contexte, il est proposé d'imposer une obligation légale d'immatriculation auprès du Registraire des entreprises du Québec (REQ) pour tout site web accessible aux consommateurs québécois, dès lors qu'il offre des biens, des services ou des opportunités d'investissement, ou qu'il procède à la collecte de données personnelles.

Cette obligation viserait à encadrer l'activité numérique de manière similaire à celle des entreprises opérant dans l'économie traditionnelle. L'immatriculation devrait notamment inclure l'identification du bénéficiaire réel du site, la fourniture d'une adresse physique vérifiable, la désignation d'un représentant légal au Québec ainsi qu'une déclaration attestant de la conformité aux lois applicables.

5.1.3 Justification juridique

Une telle mesure permettrait d'améliorer de manière significative la traçabilité des acteurs économiques opérant dans l'environnement numérique. Elle faciliterait l'exercice des recours civils et pénaux, tout en réduisant l'anonymat actuellement exploité par les fraudeurs.

Cette approche s'inscrit dans une logique cohérente avec les obligations déjà existantes en matière de transparence et d'immatriculation des entreprises. Elle vise à transposer ces principes dans le contexte numérique, afin d'assurer une équité entre les différents modes d'opération économique.

5.1.4 Impact économique pour l'État

Au-delà de ses effets en matière de protection du public, une telle mesure comporte également des retombées économiques positives pour l'État québécois. Elle permettrait notamment d'augmenter les revenus liés à l'immatriculation, de réduire les pertes financières associées à la fraude et de renforcer l'intégrité du marché numérique.

En favorisant un environnement plus transparent et mieux encadré, cette initiative contribuerait à restaurer la confiance des consommateurs et à soutenir le développement d'une économie numérique saine et sécuritaire.

5.2 La surveillance proactive des données par le ministère de la Cybersécurité et du Numérique

5.2.1 Constat

Tel que démontré dans les sections précédentes, l'usurpation d'identité repose principalement sur l'accès à des données personnelles compromises. Ces informations proviennent, dans la majorité des cas, de fuites de données, de brèches de sécurité non

colmatées, de systèmes informatiques vulnérables ou encore d'une négligence organisationnelle dans la gestion des renseignements personnels.

Dans ce contexte, la fraude à l'identité apparaît moins comme un événement isolé que comme la conséquence directe d'un déficit de protection des données en amont. Or, les mécanismes actuellement en place reposent essentiellement sur une logique réactive, intervenant après la survenance des incidents. Cette approche se révèle insuffisante pour prévenir efficacement les atteintes à la sécurité des données et, par conséquent, les stratagèmes d'usurpation d'identité qui en découlent.

5.2.2 Recommandations

Afin de corriger cette lacune structurelle, il est proposé de mettre en place un mécanisme de surveillance proactive et continue des entreprises immatriculées, sous la responsabilité du ministère de la Cybersécurité et du Numérique. Cette approche reposerait sur l'utilisation de solutions technologiques développées par des entreprises québécoises spécialisées, notamment des outils de détection et d'analyse des fuites de données.

Dans cette perspective, les sites web et les entreprises immatriculés auprès du Registraire des entreprises du Québec, conformément à la recommandation formulée à la section 5.1, devraient faire l'objet d'une surveillance automatisée. Celle-ci permettrait d'identifier les vulnérabilités, de détecter les fuites de données en temps réel, de repérer les incidents de sécurité non traités et d'évaluer le niveau de conformité des organisations en matière de protection des renseignements personnels.

5.2.3 Exemple d'application technologique

Certaines entreprises québécoises offrent déjà des solutions technologiques avancées permettant d'opérationnaliser une telle approche. À titre d'exemple, des outils spécialisés permettent la détection de données compromises circulant sur le web et le Dark Web, l'identification de failles de sécurité exploitables, la surveillance des actifs numériques d'une organisation ainsi que le suivi continu des activités sur des forums clandestins. Ces solutions incluent également des capacités d'analyse des comportements à risque, contribuant à une meilleure anticipation des menaces.

L'intégration de ces technologies dans une approche gouvernementale permettrait au ministère de la Cybersécurité et du Numérique d'identifier rapidement les organisations présentant un niveau de risque élevé et d'intervenir en amont, avant que les données compromises ne soient exploitées à des fins frauduleuses.

5.2.4 Articulation avec la Loi 25 et la Commission d'accès à l'information (CAI)

La Loi 25 impose déjà aux organisations des obligations en matière de protection des renseignements personnels, notamment l'obligation de mettre en place des mesures de sécurité appropriées, de gérer les incidents de confidentialité et de notifier les autorités en cas de risque sérieux de préjudice.

Dans ce cadre, la mise en place d'un mécanisme de surveillance proactive viendrait renforcer l'effectivité de ce cadre législatif. Elle permettrait d'identifier plus rapidement les organisations en défaut de conformité, de documenter les manquements et de faciliter l'intervention de la Commission d'accès à l'information.

Ainsi, lorsqu'une entreprise laisse perdurer une brèche de sécurité, omet de corriger une vulnérabilité connue ou néglige ses obligations en matière de protection des données, elle pourrait faire l'objet de sanctions administratives ou pénales, conformément aux dispositions prévues par la Loi 25.

5.2.5 Justification juridique et opérationnelle

L'approche proposée permettrait d'opérer un changement de paradigme, en passant d'un modèle essentiellement déclaratif, fondé sur les signalements, à un modèle proactif et préventif. Elle renforcerait l'application concrète des obligations légales existantes, tout en responsabilisant davantage les organisations quant à la gestion des renseignements personnels.

Elle repose sur un principe fondamental, à savoir que la protection des données constitue la première ligne de défense contre l'usurpation d'identité. En agissant à la source du problème, il devient possible de réduire significativement les risques de fraude.

Ce mécanisme devrait être encadré par des principes stricts de proportionnalité, de nécessité et de protection des renseignements personnels, afin d'éviter toute atteinte excessive aux droits des organisations et des citoyens.

5.2.6 Impact économique et stratégique pour le Québec

La mise en place d'un tel mécanisme générerait des retombées importantes pour le Québec. Elle permettrait notamment de réduire les coûts associés à la fraude, de diminuer les pertes subies par les citoyens et de renforcer la confiance envers l'économie numérique.

Par ailleurs, cette approche contribuerait à stimuler l'innovation québécoise en matière de cybersécurité, à favoriser l'émergence d'un écosystème technologique local et à positionner le Québec comme un leader en matière de protection des données.

5.2.7 Portée systémique

En intervenant en amont, cette mesure permettrait de s'attaquer directement à la cause principale du phénomène, soit la fuite et la mauvaise gestion des données personnelles, plutôt que de se limiter à en traiter les conséquences.

Elle s'inscrit ainsi dans une logique de prévention structurée, essentielle pour répondre efficacement à l'évolution des stratagèmes d'usurpation d'identité.

5.3 Le renversement encadré du fardeau de la preuve par déclaration solennelle

5.3.1 Constat

Le traitement actuel des dossiers d'usurpation d'identité repose, en pratique, sur une inversion du principe fondamental de la charge de la preuve. Les victimes sont généralement contraintes de démontrer qu'elles ne sont pas à l'origine des transactions contestées, de prouver l'existence même de la fraude et de contester des décisions rendues sur la base d'informations auxquelles elles n'ont pas accès.

Ce fonctionnement crée un déséquilibre procédural significatif, en plaçant la victime dans une position particulièrement défavorable. Il engendre également une complexité excessive pour les citoyens, confrontés à des démarches longues et techniques, ainsi que des délais incompatibles avec les conséquences subies. À cela s'ajoute une détérioration immédiate et parfois durable du dossier de crédit, qui accentue les préjudices déjà causés par la fraude.

5.3.2 Recommandation

Afin de corriger cette situation, il est proposé d'instaurer un mécanisme formel permettant le renversement du fardeau de la preuve, déclenché par la production d'une déclaration solennelle assermentée par la victime.

5.3.3 Mécanisme proposé

Lorsqu'une personne affirme être victime d'une usurpation d'identité, elle pourrait produire une déclaration solennelle rédigée sur un formulaire officiel, administrée sous serment et encadrée par l'Office de la protection du consommateur ou l'Autorité des marchés financiers, selon la nature du litige.

À compter du dépôt de cette déclaration, le fardeau de la preuve serait transféré à l'institution financière, au commerçant ou à l'organisme concerné. Il leur appartiendrait alors de démontrer que la transaction contestée est légitime, que la victime a contribué à la situation par une faute lourde, ou encore que la déclaration produite est fausse.

5.3.4 Effet immédiat sur le dossier de crédit

En complément de ce mécanisme, il est essentiel de prévoir une mesure de protection immédiate pour la victime. Conformément aux règles applicables en matière d'évaluation du crédit, le consommateur dispose du droit de faire inscrire une note explicative à son dossier lorsqu'une information est contestée.

Ainsi, dès la production de la déclaration solennelle d'usurpation d'identité, une mention obligatoire devrait être inscrite au dossier de crédit du consommateur, indiquant que le compte ou la transaction fait l'objet d'une contestation pour cause d'usurpation d'identité. Cette mention devrait être visible par tout prêteur ou utilisateur du dossier, suspendre les effets négatifs associés à l'information contestée, empêcher toute décision défavorable

automatique fondée sur celle-ci et demeurer en place jusqu'à la résolution complète du litige.

5.3.5 Justification de la mesure

Une telle disposition est essentielle afin d'éviter que la victime ne subisse un préjudice additionnel pendant la durée de l'enquête. Elle permet notamment d'empêcher que des refus de crédit soient fondés sur une situation frauduleuse et de protéger la réputation financière du consommateur. Elle reconnaît également que la contestation est crédible dès lors qu'elle est appuyée par une déclaration sous serment.

5.3.6 Fondement juridique de la déclaration solennelle

La déclaration solennelle constitue un acte juridique engageant. À cet égard, les articles 131 à 134 du Code criminel disposent que le fait de faire une fausse déclaration sous serment constitue une infraction pénale.

Ce cadre permet d'assurer un équilibre entre la protection des victimes de bonne foi et la prévention des abus, en dissuadant toute utilisation frauduleuse du mécanisme proposé.

5.3.7 Encadrement institutionnel

L'Office de la protection du consommateur et l'Autorité des marchés financiers pourraient être appelés à jouer un rôle central dans la mise en œuvre de ce mécanisme. Ils pourraient notamment élaborer les formulaires officiels de déclaration, encadrer les modalités d'inscription de la note au dossier de crédit, superviser les délais de traitement et intervenir en cas de litige.

En cas de fausse déclaration, ces organismes pourraient également imposer des sanctions administratives et, le cas échéant, transmettre les dossiers aux autorités compétentes en vue de poursuites pénales.

5.3.8 Justification juridique

La mesure proposée permet de rétablir un principe fondamental selon lequel la charge de la preuve doit incomber à la partie qui détient les moyens de preuve. Elle tient compte de l'asymétrie informationnelle entre les institutions et les consommateurs, reconnaît la vulnérabilité de ces derniers et répond à la nécessité d'adapter les mécanismes procéduraux à la réalité de la fraude moderne.

5.3.9 Effets attendus

La mise en place de ce mécanisme permettrait d'assurer une protection immédiate du dossier de crédit des victimes, de réduire les préjudices secondaires, d'accélérer le traitement des dossiers et de responsabiliser davantage les institutions. Elle contribuerait également à améliorer la confiance du public envers le système de traitement des fraudes.

Le projet de loi n° 24 ne pourra atteindre pleinement ses objectifs sans corriger ce déséquilibre fondamental.

5.4 L'encadrement renforcé des plateformes de transfert de fonds par l'Autorité des marchés financiers (AMF)

5.4.1 Constat

Les stratagèmes d'usurpation d'identité et de fraude en ligne reposent sur un élément central : la capacité des fraudeurs à transférer, convertir et dissimuler rapidement les fonds obtenus. Le véritable « nerf de la guerre » réside ainsi dans les mécanismes de transfert de fonds, qui permettent la concrétisation et la rentabilisation des activités frauduleuses.

Dans la majorité des cas observés, les fraudeurs utilisent divers intermédiaires numériques, notamment les virements électroniques, les services de paiement en ligne et les plateformes de transfert international. Ces outils offrent une combinaison particulièrement avantageuse pour les acteurs malveillants, en permettant des transactions rapides, une certaine forme d'anonymisation et une dispersion des fonds à l'échelle internationale, rendant leur traçabilité plus complexe.

5.4.2 Une asymétrie réglementaire préoccupante

Cette réalité est d'autant plus préoccupante qu'elle s'inscrit dans un contexte d'asymétrie réglementaire marquée. Les institutions financières traditionnelles sont soumises à des obligations strictes en matière de connaissance du client, de lutte contre le blanchiment d'argent, de déclaration des opérations douteuses et de vérification rigoureuse de l'identité.

À l'inverse, certaines plateformes de transfert de fonds appliquent des mécanismes de contrôle moins contraignants, reposant parfois sur des processus d'auto-déclaration et limitant leur responsabilité au moyen de clauses contractuelles. Cette disparité crée une zone de vulnérabilité importante, exploitée par les fraudeurs pour contourner les mécanismes de surveillance plus rigoureux.

5.4.3 Recommandation

Dans ce contexte, il est proposé de renforcer l'encadrement des plateformes de transfert de fonds en leur imposant des obligations accrues en matière de vérification d'identité et de traçabilité des transactions, sous la supervision de l'Autorité des marchés financiers.

5.4.4 Mesure proposée : authentification biométrique des transactions

Il est recommandé d'imposer aux plateformes de transfert de fonds l'obligation d'exiger une capture d'image avec reconnaissance faciale au moment de la transaction, tant pour l'émetteur que pour le destinataire des fonds. Cette exigence devrait s'appliquer lors de l'envoi des fonds, au moment de leur réception ou de leur encaissement, ainsi que dans le cadre de toute opération jugée à risque.

5.4.5 Données à collecter et à conserver

Afin d'assurer l'efficacité de ce mécanisme, les plateformes devraient être tenues de conserver un ensemble de données permettant une traçabilité complète des transactions. Cela inclurait les images captées à des fins de biométrie faciale, les métadonnées associées

telles que l'horodatage et les informations relatives à l'appareil utilisé, les données de géolocalisation ainsi que les informations techniques propres à chaque transaction.

Ces données devraient être sécurisées, conservées pour une période déterminée et rendues accessibles aux autorités compétentes dans le cadre d'enquêtes, conformément aux règles applicables en matière de protection des renseignements personnels.

5.4.6 Objectifs de la mesure

L'objectif principal de cette approche est de réduire significativement l'anonymat dont bénéficient actuellement les fraudeurs. Elle vise également à dissuader les activités criminelles, à faciliter l'identification des auteurs, à améliorer l'efficacité des enquêtes et à renforcer la traçabilité des flux financiers.

5.4.7 Portée de la mesure

Il convient de préciser que cette obligation viserait exclusivement les plateformes de transfert de fonds et ne s'appliquerait pas aux paiements effectués par carte de crédit. Elle serait particulièrement orientée vers les transactions à risque ou ne bénéficiant pas des mécanismes de protection traditionnels.

5.4.8 Justification juridique et opérationnelle

Cette mesure s'inscrit dans la continuité des obligations existantes en matière de lutte contre le blanchiment d'argent, le financement d'activités illicites et la fraude financière. Elle repose sur un principe fondamental selon lequel le niveau de vérification doit être proportionnel au niveau de risque associé à la transaction.

Dans un environnement où les flux financiers peuvent être déplacés rapidement et à l'échelle internationale, il apparaît nécessaire de renforcer les mécanismes d'identification afin de maintenir l'efficacité des cadres réglementaires.

5.4.9 Effets attendus

La mise en œuvre de cette mesure permettrait de freiner significativement les flux financiers liés à la fraude, d'augmenter le taux d'identification des fraudeurs et de faciliter les poursuites. Elle contribuerait également à une meilleure protection des victimes et à une réduction des pertes économiques associées aux stratagèmes frauduleux.

5.4.10 Portée élargie

Au-delà de l'usurpation d'identité, cette approche permettrait de lutter contre d'autres formes de fraude, notamment les stratagèmes d'arnaque amoureuse, les cas d'extorsion, les fraudes liées à des investissements fictifs ainsi que diverses formes de cybercriminalité.

5.4.11 Rôle de l'Autorité des marchés financiers

L'Autorité des marchés financiers serait appelée à jouer un rôle central dans la mise en œuvre de ce cadre. Elle pourrait encadrer les normes techniques applicables, superviser la conformité des plateformes, imposer des sanctions en cas de manquement et assurer une coordination avec les autorités nationales et internationales.

5.4.12 Impact économique et stratégique

Enfin, cette mesure présenterait des retombées positives significatives pour le Québec. Elle permettrait de réduire les pertes liées à la fraude, d'améliorer la confiance envers les plateformes numériques, de favoriser un alignement avec les standards internationaux et de positionner le Québec comme un leader en matière d'encadrement des flux financiers numériques.

Une telle mesure pourrait être mise en œuvre de manière progressive, notamment par la mise en place de projets pilotes ciblant les transactions à haut risque.

5.5 Les risques liés aux données biométriques et les limites des mécanismes d'identification

5.5.1 Constat

Les mesures visant à renforcer les mécanismes d'identification, notamment par le recours aux données biométriques, constituent des outils pertinents dans la lutte contre la fraude. Ces technologies, qui incluent notamment la reconnaissance faciale, la lecture de l'iris, la reconnaissance vocale et l'authentification par empreinte digitale, permettent à court terme d'améliorer de manière significative le niveau de sécurité des transactions et des processus d'identification.

Toutefois, leur efficacité doit être analysée à la lumière de l'évolution constante des capacités des fraudeurs.

5.5.2 Une évolution constante des capacités des fraudeurs

L'expérience des dernières décennies démontre que les acteurs criminels s'adaptent rapidement aux nouvelles mesures de sécurité. Il est observé de manière récurrente que les groupes criminels structurés adoptent les technologies émergentes avant même leur encadrement réglementaire, exploitant ainsi les zones grises du système.

L'utilisation de l'intelligence artificielle à des fins frauduleuses illustre particulièrement cette dynamique. Bien avant sa démocratisation auprès du grand public, certains réseaux criminels y recouraient déjà pour la création de faux contenus, l'automatisation d'attaques à grande échelle et la manipulation de l'information. Cette capacité d'adaptation suggère que les mécanismes de sécurité, aussi avancés soient-ils, tendent à être contournés à mesure que les technologies évoluent.

5.5.3 Des risques émergents liés à la biométrie

Bien que les données biométriques soient généralement perçues comme des identifiants fiables, elles présentent des vulnérabilités importantes à moyen et à long terme. Les avancées technologiques permettent désormais la reproduction de visages par hypertrucage, la synthèse vocale de haute précision et la simulation de comportements biométriques crédibles.

Par ailleurs, le vol et la réutilisation de données biométriques constituent un risque particulièrement préoccupant. Contrairement à un mot de passe, une donnée biométrique ne peut être modifiée une fois compromise. Ainsi, une fuite ou une exploitation frauduleuse de ces données peut entraîner des conséquences permanentes pour les individus concernés.

5.5.4 Une dépendance excessive à l'identification technologique

Le développement des mécanismes d'identité numérique et des solutions biométriques ne doit pas conduire à une dépendance excessive à ces outils comme unique moyen de preuve d'identité. Aucun système technologique n'est infaillible et toute mesure de sécurité devient, à terme, une cible pour des acteurs malveillants.

Dans un contexte où la sophistication des attaques évolue parallèlement aux mécanismes de protection, il existe un risque réel que des fraudeurs soient en mesure, dans un avenir rapproché, de contourner les systèmes biométriques, d'usurper des identités numériques ou de reproduire des signaux d'authentification actuellement jugés fiables.

5.5.5 Implication pour le cadre juridique

Dans ce contexte, il apparaît essentiel de ne pas fonder la protection des citoyens exclusivement sur des mécanismes technologiques d'identification. Ceux-ci doivent être complétés par des mécanismes juridiques robustes et protecteurs, capables d'intervenir lorsque la technologie atteint ses limites.

5.5.6 Lien avec le renversement du fardeau de la preuve

Cette analyse renforce directement la pertinence de la recommandation formulée à la section 5.3 relative au renversement du fardeau de la preuve. En effet, si les mécanismes d'identification peuvent être contournés, il devient impératif de prévoir un cadre juridique permettant de protéger la victime, même en présence d'une authentification apparemment valide.

Le renversement du fardeau de la preuve permet ainsi de reconnaître la possibilité d'une fraude malgré une validation technologique, d'éviter que la victime ne soit pénalisée sur la seule base de systèmes techniques et de transférer la responsabilité vers les acteurs disposant des moyens d'enquête appropriés.

5.5.7 Recommandation

Il est recommandé de considérer les technologies biométriques comme des outils complémentaires, et non exclusifs, dans les processus d'identification. Il convient également de maintenir une approche juridique équilibrée, intégrant des mécanismes de protection des victimes, et d'éviter toute présomption absolue de validité fondée uniquement sur une authentification technologique.

5.5.8 Conclusion de la section

Les technologies biométriques constituent un levier important dans la lutte contre la fraude, mais elles ne peuvent, à elles seules, garantir une protection absolue. Dans un environnement où les fraudeurs sont organisés, technologiquement avancés et en constante adaptation, il est essentiel d'adopter une approche combinée, reposant à la fois sur des outils technologiques et des mécanismes juridiques.

Une telle approche est nécessaire afin d'assurer une protection réelle, durable et adaptée aux défis contemporains de l'usurpation d'identité.

6. Conclusion

L'usurpation d'identité constitue aujourd'hui bien plus qu'un simple enjeu individuel. Elle s'impose comme un phénomène systémique, structuré et en constante évolution, qui met à l'épreuve les mécanismes traditionnels de protection du public. Les constats exposés dans le présent mémoire démontrent clairement que les stratagèmes de fraude ne relèvent plus d'initiatives isolées, mais s'inscrivent dans des dynamiques organisées, portées par des acteurs technologiquement avancés et motivés par des objectifs économiques, exploitant simultanément les failles humaines, technologiques et réglementaires.

Le projet de loi n° 24 s'inscrit dans une volonté légitime et nécessaire de renforcer la protection des citoyens québécois face à ces nouvelles formes de criminalité. Il constitue, à cet égard, une avancée importante. Toutefois, l'analyse issue de la pratique terrain démontre que, sans ajustements ciblés, les mesures envisagées risquent de demeurer insuffisantes face à la rapidité d'adaptation et à la sophistication croissante des fraudeurs.

Dans ce contexte, le présent mémoire propose une évolution du cadre législatif fondée sur une approche structurée et cohérente. Celle-ci repose d'abord sur la nécessité d'agir en amont, en renforçant la surveillance proactive des données, en encadrant les pratiques des entreprises et en prévenant les fuites d'information, lesquelles constituent la principale source des stratagèmes d'usurpation d'identité. Elle implique également d'intervenir au cœur même du système, en encadrant plus rigoureusement les plateformes numériques et les mécanismes de transfert de fonds, qui représentent le principal vecteur de monétisation de la fraude. Enfin, elle commande de protéger efficacement les victimes, notamment par la mise en place de mécanismes juridiques adaptés, tels que le renversement du fardeau de la preuve, afin de rétablir un équilibre procédural et d'éviter que les citoyens ne soient pénalisés par un système qu'ils ne contrôlent pas.

Le mémoire met également en lumière une réalité fondamentale : aucune solution technologique, y compris les mécanismes biométriques, ne peut à elle seule garantir une protection absolue. Dans un environnement où les fraudeurs disposent déjà d'outils avancés, notamment en matière d'intelligence artificielle, il devient essentiel d'adopter une approche intégrée, combinant à la fois des leviers technologiques et des mécanismes juridiques robustes, afin d'assurer une protection durable et efficace.

Au-delà de la seule protection des consommateurs, les mesures proposées représentent une véritable opportunité stratégique pour le Québec. Elles permettraient non seulement de renforcer la confiance envers les institutions financières et numériques, mais également de soutenir le développement d'un écosystème québécois en cybersécurité et en protection des données, tout en réduisant de manière significative les pertes économiques liées à la fraude.

L'évolution rapide des stratagèmes impose aujourd'hui une réponse législative proactive, cohérente et pleinement adaptée aux réalités contemporaines. Il ne s'agit plus uniquement de réagir aux fraudes une fois qu'elles sont commises, mais bien de repenser en profondeur les mécanismes de protection dans un environnement numérique en constante transformation.

En définitive, l'usurpation d'identité doit être reconnue comme un enjeu central de sécurité économique et sociale. Le législateur dispose à cet égard d'une occasion déterminante : celle de mettre en place un cadre moderne, équilibré et efficace, capable de protéger les citoyens tout en responsabilisant les acteurs du système.

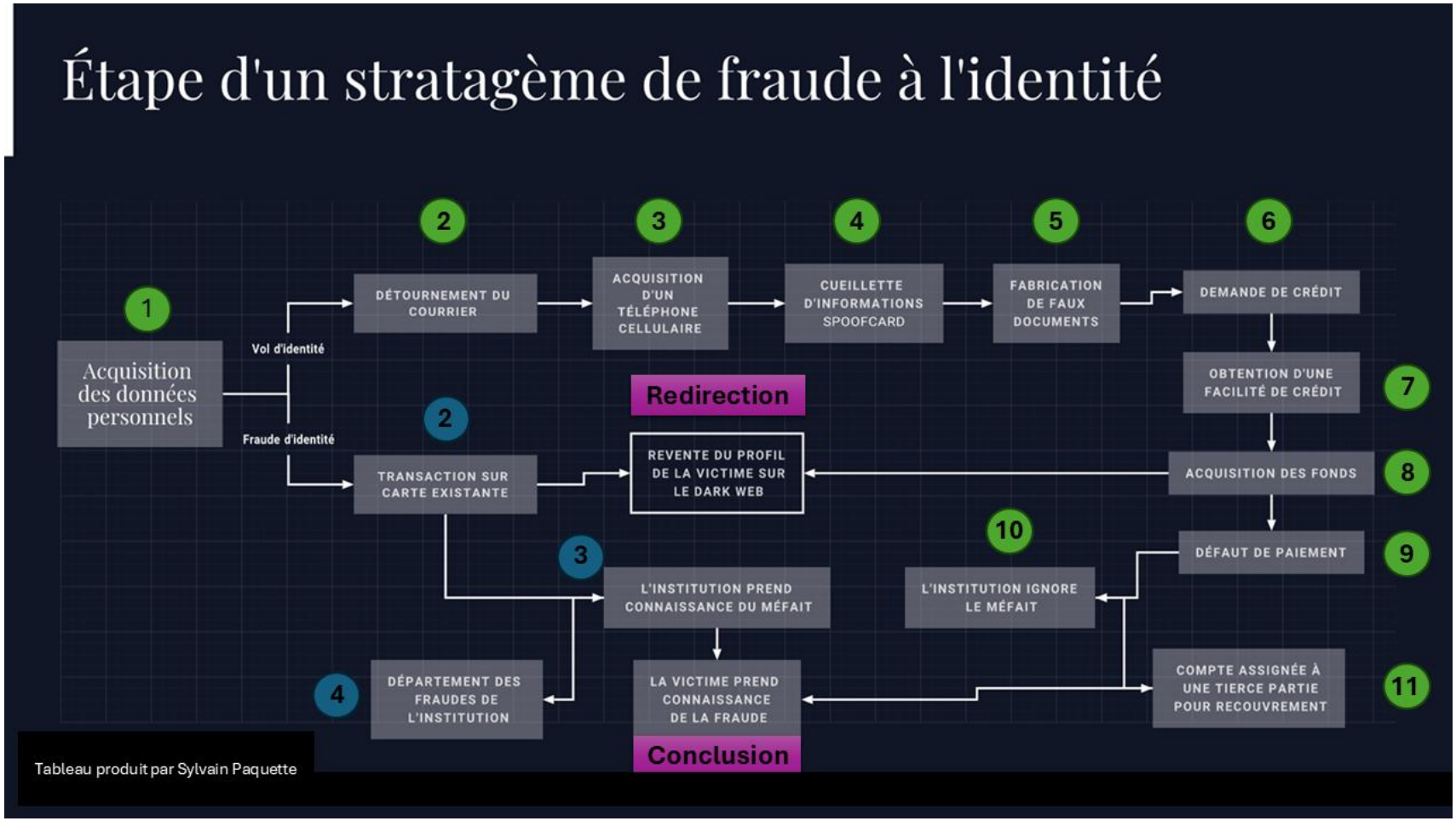
Chaque cas d'usurpation d'identité non résolu ou mal traité contribue directement à miner la confiance des citoyens envers les institutions financières, les plateformes numériques et, plus largement, envers l'État.

L'usurpation d'identité doit également être comprise comme un outil pouvant être utilisé à des fins de déstabilisation personnelle ou économique, ce qui renforce la nécessité d'un encadrement robuste.

Le présent mémoire s'inscrit dans cette perspective, en proposant des solutions concrètes, applicables et ancrées dans la réalité terrain, afin de contribuer à une réponse législative à la hauteur des enjeux.

Sylvain Paquette
Directeur principal, enquêtes et conformité
Pointages.ca
Courriel : spaquette@pointages.ca

ANNEXE


Étape d'un stratagème de fraude à l'identité
1
Acquisition des données personnels
Vol d'identité
Fraude d'identité
2
DÉTOURNEMENT DU COURRIER
3
ACQUISITION D'UN TÉLÉPHONE CELLULAIRE
4
CUEILLETTE D'INFORMATIONS SPOOFCARD
5
FABRICATION DE FAUX DOCUMENTS
6
DEMANDE DE CRÉDIT
OBTENTION D'UNE FACILITÉ DE CRÉDIT
7
ACQUISITION DES FONDS
8
DÉFAUT DE PAIEMENT
9
Redirection
2
TRANSACTION SUR CARTE EXISTANTE
REVENTE DU PROFIL DE LA VICTIME SUR LE DARK WEB
10
L'INSTITUTION IGNORE LE MÉFAIT
3
L'INSTITUTION PREND CONNAISSANCE DU MÉFAIT
4
DÉPARTEMENT DES FRAUDES DE L'INSTITUTION
LA VICTIME PREND CONNAISSANCE DE LA FRAUDE
COMPTE ASSIGNÉE À UNE TIERCE PARTIE POUR RECOUVREMENT
11
Conclusion
Tableau produit par Sylvain Paquette