LE RUBICON

L’extorsion numérique transnationale au Canada, révélateur des vulnérabilités des démocraties libérales

Daniel Robson | 3 juillet 2026 | ARTICLES

En février 2026, Ottawa a reconnu publiquement que l’extorsion ne relevait plus d’une suite de faits divers isolés, mais d’une menace structurée portée par des réseaux opérant à travers les frontières et les plateformes numériques. Dans un communiqué annonçant de nouvelles mesures de coordination, le gouvernement fédéral soulignait en effet que ces crimes alimentaient la peur, fragilisaient le sentiment de sécurité et touchaient désormais aussi bien les individus que les entreprises. Quelques semaines plus tard, l’Agence des services frontaliers du Canada indiquait avoir ouvert 372 enquêtes en matière d’immigration liées à des réseaux d’extorsion.

L’extorsion numérique transnationale renvoie à des dispositifs de contrainte dans lesquels des menaces, des demandes de paiement ou des formes d’intimidation passent par des outils numériques, s’appuient sur des plateformes ou des communications à distance, et produisent une part substantielle de leurs effets au-delà du territoire d’émission. Statistique Canada a par ailleurs relevé que 47 % des incidents d’extorsion signalés en 2024 comportaient une composante cybernétique et que leur taux demeurait largement supérieur à celui observé une décennie plus tôt. La dynamique n’a donc rien d’abstrait.

Ce constat dépasse néanmoins le seul cas canadien. Les travaux consacrés aux formes contemporaines de coercition transfrontalière montrent que les États sur le territoire desquels ces dispositifs prennent appui ou produisent leurs effets sont de plus en plus confrontés à des menaces à distance, à l’intimidation numérique et à des campagnes de pression qui brouillent les frontières entre criminalité, technologie et souveraineté. Les recherches sur le crime organisé à l’ère numérique soulignent, elles aussi, que l’extorsion et le chantage se recomposent dans des environnements techniques qui étendent la portée géographique des auteurs et compliquent ainsi la réponse institutionnelle.

C'est dans cet espace qu'il faut situer notre réflexion sur les démocraties libérales, au sens de régimes fondés sur l'État de droit, la protection des libertés civiles et des garanties constitutionnelles et institutionnelles encadrant l'exercice du pouvoir. Dans cette acception classique, la dimension libérale de la démocratie tient moins à l'expression majoritaire seule qu'à l'existence de droits, de contre-pouvoirs et de mécanismes de contrôle inscrits dans une architecture institutionnelle plus large, que les approches comparatives de la démocratie rattachent également aux droits, à l'État de droit et aux freins institutionnels au pouvoir.

C'est précisément cette architecture – fondée sur l'ouverture informationnelle, la séparation fonctionnelle des compétences et des garanties procédurales denses – qui constitue leur force normative, mais aussi, dans certains contextes, une surface d'exploitation pour des acteurs capables d'agir vite, à distance et à travers plusieurs juridictions. Des analyses récentes ont ainsi montré que les formes numériques de coercition transfrontalière pouvaient affecter non seulement les individus visés, mais aussi la capacité concrète des États sur le territoire desquels ces dispositifs prennent appui ou produisent leurs effets à protéger les personnes visées, qualifier juridiquement les faits et coordonner leur réponse.

La question centrale de cet article est donc la suivante : pourquoi les démocraties libérales traitent-elles souvent l'extorsion numérique transnationale comme une juxtaposition de faits pénaux ou civils, alors qu'elle fonctionne déjà comme une forme de coercition distribuée ? Le Canada constitue ici un cas d'étude éclairant, puisque, comme nous le montrons, l'État fédéral a redéfini institutionnellement l'extorsion. Nous analysons ensuite deux configurations concrètes de coercition opérée depuis le territoire canadien. Enfin, nous revenons sur les limites d'une réponse publique qui découpe trop souvent en fragments ce que les acteurs, eux, ont déjà appris à organiser comme un système.

Les deux cas étudiés ici n'épuisent évidemment pas le spectre des coercitions transfrontalières observées au Canada. Ils permettent toutefois de rendre visible, à une échelle plus immédiatement saisissable, une mécanique que les autorités canadiennes décrivent aussi dans d'autres contextes : l'usage de relais locaux, de canaux numériques, de pressions à distance et de dommages extraterritoriaux. À cet égard, leur intérêt ne tient pas à l'identité géopolitique exacte des acteurs, mais à la structure commune de la contrainte qu'ils rendent observable sur le territoire canadien.

La redéfinition canadienne de l'extorsion

Le changement de statut de l'extorsion dans le discours public canadien est déjà, en lui-même, révélateur. En janvier 2026, dans un document de contexte sur les rôles et responsabilités en matière de lutte contre l'extorsion, Sécurité publique Canada explique que les services locaux, provinciaux et fédéraux doivent désormais partager leurs renseignements et coordonner leurs stratégies afin de perturber des réseaux qui ciblent entreprises et résidents. L'extorsion n'apparaît plus comme un simple délit ponctuel, mais comme un phénomène appelant des réponses intégrées à plusieurs niveaux de l'État.

Les autorités canadiennes décrivent d'ailleurs de plus en plus clairement les milieux et les configurations criminelles dans lesquels s'inscrit ce phénomène. Lors d'un sommet dans la région de Peel, Ottawa soulignait que l'extorsion servait à financer et à contrôler d'autres marchés criminels, notamment le trafic de stupéfiants, le vol d'automobiles et la contrebande d'armes à feu, et que les groupes qui s'y adonnent recourent à des dispositifs qui reposent sur des menaces adressées à des commerçants ou à des entrepreneurs, sur l'usage des médias sociaux comme relais d'intimidation et, dans certains cas, sur des violences périphériques – notamment des incendies criminels – destinées à renforcer la crédibilité de la contrainte.

Dans les basses-terres continentales de la Colombie-Britannique, la mise en place d'un groupe de travail régional contre l'extorsion confirme la consolidation de réseaux associant extorsion, intimidation, incendies criminels et violence armée. De son côté, l'Agence des services frontaliers du Canada cite explicitement les cas d'Arshdeep Singh et de Sukhnaaz Singh Sandhu, tous deux liés, selon les autorités, à des organisations criminelles associées à l'extorsion. Le tournant a été encore plus explicite avec la présentation du projet de loi C-22 en mars 2026. Le gouvernement y explique que des réseaux criminels mondialisés exploitent l'environnement numérique pour commettre des crimes graves et qu'il faut moderniser les outils d'enquête pour suivre cette transformation.

Cette redéfinition institutionnelle s'inscrit dans une évolution plus large. Selon Statistique Canada, le taux d'extorsion déclaré par la police a diminué en 2024 par rapport à 2023, mais il demeurait environ quatre fois plus élevé qu'une décennie plus tôt, tandis que près de la moitié des incidents signalés comportaient une composante cybernétique. L'enjeu n'est donc pas seulement celui d'une hausse ponctuelle, mais bien celui d'une transformation plus profonde des modes opératoires.

Ce déplacement apparaît également dans la manière dont l'État fédéral parle aujourd'hui des crimes financiers. Le Centre de coordination contre la criminalité financière classe explicitement l'extorsion, le chantage, la fraude et le blanchiment dans un

continuum menaçant non seulement la sécurité publique, mais aussi la sécurité nationale et l'intégrité du système financier.

L'idée est importante : l'argent de l'extorsion n'est plus appréhendé comme un simple produit accessoire du délit, mais comme l'un des vecteurs d'une économie plus large de la coercition. Pourtant, cette redéfinition institutionnelle n'a pas encore abouti à une doctrine pleinement cohérente. Certes, l'État canadien perçoit de mieux en mieux l'extorsion lorsqu'elle s'inscrit dans des réseaux visibles et identifiables par leurs effets sur l'ordre public. En revanche, il la saisit beaucoup moins bien lorsqu'elle prend la forme d'une coercition réputationnelle et transnationale, projetée depuis le Canada vers des cibles situées hors du territoire.

Une coercition plus rapide que la réponse publique

L'extorsion contemporaine ne se réduit plus à une demande de paiement assortie d'une menace explicite. Elle peut passer par des campagnes d'intimidation relayées sur les médias sociaux, comme l'ont relevé les autorités dans la région de Peel et dans les basses-terres continentales de la Colombie-Britannique, ou par des formes plus intimes de contrainte, comme la « sextorsion », où des images sont utilisées pour obtenir de l'argent, contraindre au silence ou produire de nouveaux contenus. Dans ces configurations, l'argent n'est plus le seul résultat souhaité : la peur, la dissuasion et l'autocensure deviennent eux aussi des effets recherchés de la contrainte.

Cette évolution complique la réponse institutionnelle. Le droit pénal, les plateformes, les autorités frontalières et les services chargés des flux financiers n'isolent pas les mêmes objets, alors que les victimes subissent une expérience de coercition unifiée. Les analyses du crime organisé numérique et l'évaluation européenne des menaces criminelles de 2025 convergent sur ce point : la numérisation n'a pas remplacé les formes antérieures de criminalité organisée, mais leur a donné une capacité d'adaptation, de projection et de mise en réseau plus rapide.

Un même dossier peut ainsi relever simultanément d'infractions pénales, de signalements aux plateformes, d'enjeux migratoires, de questions de conformité financière et, parfois, de contentieux civils, sans qu'aucune de ces portes d'entrée ne suffise à elle seule à saisir l'ensemble du dispositif. C'est ce décalage entre des acteurs qui opèrent déjà en système et des institutions qui continuent souvent de répondre par compartiments qui explique la résilience de l'extorsion numérique transnationale.

Le territoire canadien comme base d'émission d'un préjudice extraterritorial

Le dossier Abdelmejid Tounarti, un Canado-Marocain résidant dans la région de Québec, constitue à cet égard un cas d'étude particulièrement révélateur. Il démontre en effet comment une coercition peut être opérée à partir du Québec, tout en produisant l'essentiel de ses effets en dehors du territoire. Selon des témoignages de victimes, des documents judiciaires marocains et d'autres éléments, une page Facebook administrée depuis le Québec, Lfercha, servait à diffuser des propos calomnieux contre des Marocains influents, parmi lesquels des hommes d'affaires et des responsables publics, dans un cadre que plusieurs victimes ont explicitement décrit comme lié à l'extorsion.

Ce qui donne à ce dossier sa portée analytique n'est pas seulement la gravité alléguée des faits, mais la structure qu'il rend visible : une menace émise depuis le Canada, l'usage de plateformes numériques comme vecteurs de contrainte, l'existence de relais locaux et un dommage principalement causé à l'étranger. C'est cette combinaison, plus que la seule singularité biographique du dossier, qui en fait un observatoire utile d'une vulnérabilité canadienne plus générale.

Ce cas d'étude met en lumière une difficulté juridique classique des contentieux numériques transfrontaliers : le lieu d'émission, le lieu de réception et le lieu du dommage ne coïncident pas nécessairement, ce qui complique à la fois la qualification des faits, la compétence des autorités et l'articulation entre réputation, poursuite pénale et coopération judiciaire, comme l'a rappelé la Cour suprême du Canada dans l'affaire *Haaretz.com c. Goldhar*. Une femme d'affaires d'Agadir y affirme avoir été accusée de prostitution et de proxénétisme. Un homme d'affaires y dénonce de fausses informations le présentant comme incarcéré dans une affaire criminelle. L'intérêt du dossier tient moins à la violence verbale des publications qu'au mécanisme qu'elles semblaient nourrir : une pression publique suffisamment forte pour pousser certaines cibles à payer afin d'empêcher la poursuite ou l'aggravation des atteintes.

Pris ensemble, ces éléments font apparaître une configuration plus cohérente. L'enquête évoque d'abord des victimes décrivant une pression réputationnelle associée à des demandes d'argent. Elle s'appuie ensuite sur un jugement marocain et sur d'autres pièces judiciaires mentionnant des complicités dans l'obtention de sommes contre une promesse de silence. Elle fait enfin apparaître plusieurs relais canadiens, ainsi que des éléments de circulation financière reliant le dispositif à des personnes installées au Canada. Le mécanisme apparaît ainsi moins comme une succession d'épisodes dispersés que comme une chaîne de contrainte dont l'émission peut être localisée au Canada alors même que le dommage principal se matérialise à l'étranger.

Cette lecture est renforcée par le cas d'un autre Canadien d'origine marocaine, Mohammed E., qui dit avoir porté plainte auprès de la Sûreté du Québec, de la Gendarmerie royale du Canada et du service de police de Québec après qu'un de ses amis a été accusé d'exploiter un « club de prostitution ». Or, le dossier aurait été fermé, une source policière expliquant qu'il était difficile de déposer des accusations puisqu'aucune personne n'avait été victime d'extorsion sur le territoire québécois. Ce détail illustre la difficulté des institutions canadiennes à traiter une coercition émise depuis le Canada, mais subie principalement à l'étranger.

Le cas El Amine Serhani ajoute ici une dimension essentielle. Installé à Montréal, il a engagé une poursuite civile contre Meta Platforms et contre Abdelmejid Tounarti après avoir été dépeint comme criminel et espion. Cette affaire rappelle que la coercition ne se joue pas seulement entre auteur et victime : elle est aussi rendue possible par l'architecture des plateformes, leur lenteur à agir, leur capacité à laisser renaître des pages supprimées et leur rôle objectif dans la reproduction d'un espace de contrainte. Dans ce dossier, la plateforme avait supprimé une première page Lfercha pour violation de ses standards communautaires, avant qu'une nouvelle page, puis deux pages de repli, ne réapparaissent rapidement et ne rassemblent à nouveau plusieurs centaines de milliers d'abonnés, ce qui donne une mesure concrète de la difficulté à neutraliser durablement ce type de dispositif dans l'environnement des grandes plateformes.

La deuxième série d'éléments disponibles dans cette affaire renforce encore davantage la lecture transnationale du dossier. Selon des documents de la police judiciaire marocaine, un jugement relatif à un complice condamné, des éléments bancaires et des plaintes communiquées aux autorités, le mécanisme reposerait en partie sur le *hawala*, procédé informel de transfert de fonds reposant sur des chaînes de compensation entre intermédiaires. L'enquête fait aussi apparaître plusieurs relais financiers, depuis des remises d'espèces jusqu'à des virements effectués au profit d'Abdelmejid Tounarti, ce qui renforce l'hypothèse d'un dispositif appuyé sur des circuits de circulation d'argent plus opaques que ceux d'une simple publication diffamatoire. Cette même documentation rappelle que le *hawala* n'est pas en soi forcément illégal, mais qu'il peut contrevenir à la loi canadienne s'il est pratiqué en dehors des obligations d'enregistrement et de conformité exigées par le Centre d'analyse des opérations et déclarations financières du Canada. Ce point est capital : il montre que l'extorsion numérique transnationale ne relève pas seulement d'un usage abusif de Facebook ou de WhatsApp. Elle peut aussi s'appuyer sur des techniques de circulation d'argent qui brouillent la traçabilité et compliquent la lecture pénale classique. Ce n'est donc pas seulement un problème de contenu ; c'est un problème d'infrastructure.

La réputation comme levier de coercition transfrontalière

Le dossier de Muhammad Luqman Rana, un Canadien de Vaughan en Ontario, offre un second angle d'analyse, moins centré sur la diffamation publique que sur la menace de divulgation, l'atteinte à la réputation et la coercition intime exercée au moyen d'outils numériques. Selon sa condamnation aux États-Unis en mai 2023, il a écopé de 32 ans de prison fédérale pour production d'images pédopornographiques et pour extorsion liée à un dispositif de « sextorsion » ayant visé cinq victimes mineures américaines. Selon son plaidoyer de culpabilité et d'autres pièces judiciaires américaines, Muhammad Luqman Rana a utilisé des sites de clavardage gratuits pour cibler des victimes aux États-Unis et au Canada, obtenir des images embarrassantes ou sexuellement explicites, puis forcer certaines d'entre elles à produire de nouveaux contenus par crainte qu'il ne rende publics les fichiers déjà obtenus. Les autorités américaines soulignent que certaines victimes ont été terrorisées presque quotidiennement pendant des mois, parfois pendant plus d'un an.

Le point décisif, pour notre propos, tient au fait que l'acte d'accusation fédéral américain décrivait explicitement l'affaire comme une extorsion exercée par menace de porter atteinte à la réputation d'autrui. Le même dossier fait apparaître une coopération étroite entre le Bureau fédéral d'enquête des États-Unis (FBI), la police de Toronto et les mécanismes d'entraide et d'extradition entre le Canada et les États-Unis. Autrement dit, on retrouve ici, sous une forme différente, un schéma déjà familier : un acteur installé au Canada, des victimes situées principalement à l'étranger, des plateformes numériques comme vecteur de contrainte et une réponse judiciaire qui ne devient pleinement efficace qu'au prix d'une coopération transfrontalière établie.

Ce dossier montre que la coercition numérique ne passe pas nécessairement par des publications visibles par tous. Elle peut aussi reposer sur la détention de fichiers intimes, sur la menace de leur diffusion et sur l'exploitation d'une vulnérabilité réputationnelle. Les moyens diffèrent, mais la logique reste la même : établir un rapport de force durable entre l'auteur et la cible. La différence avec les formes plus classiques de diffamation numérique mérite donc d'être soulignée, sans pour autant remettre en cause l'argument central de cet article. Elle invite plutôt à élargir l'analyse : le territoire canadien peut servir non seulement de point de départ à des campagnes de réputation diffusées en ligne, mais aussi de support à des formes plus discrètes et plus personnalisées de coercition transfrontalière, dont les principaux effets sont subis ailleurs.

Le rapprochement entre l'affaire *Tounarti* et l'affaire *Rana* permet surtout de distinguer deux modalités d'une même logique. Dans la première, la pression passe par une page Facebook, des demandes de paiement, des intermédiaires et des circuits de transfert informels. Dans la seconde, elle repose sur la captation de contenus intimes, la menace de divulgation et une coopération judiciaire rendue nécessaire par le caractère transfrontalier du préjudice. Dans les deux cas, toutefois, le territoire canadien apparaît comme un point d'émission d'une contrainte prolongée vers des cibles situées à l'extérieur.

Ce que l'État voit en fragments, les réseaux l'exploitent comme un système

Le nœud du problème canadien apparaît ici avec plus de netteté. Dans les deux dossiers, les éléments matériels ne manquent pas : plaintes, témoignages, documents judiciaires, relevés bancaires, messages, pages, intermédiaires et parfois déjà des condamnations. Ce qui demeure fragile, en revanche, c'est leur saisie d'ensemble. La réponse publique continue souvent à distribuer ces éléments entre catégories distinctes, là où les dispositifs de coercition, eux, les articulent déjà comme un continuum. En effet, la justice pénale isole des infractions distinctes. Les autorités frontalières traitent l'inadmissibilité ou la coopération internationale. Les spécialistes du blanchiment suivent des flux opaques. Les plateformes évaluent des contenus au regard de leurs propres standards. Or, les dispositifs d'extorsion, eux, articulent souvent ces dimensions comme une même chaîne d'action.

Les travaux du Centre national de cybersécurité du Royaume-Uni et de l'Agence nationale britannique de lutte contre la criminalité consacrés à l'écosystème cybercriminel de l'extorsion, ainsi que le manuel de l'Initiative mondiale contre la criminalité transnationale organisée consacré à l'extorsion insistent précisément sur cette capacité des acteurs criminels à combiner intimidation, ressources techniques et logique économique dans des dispositifs de contrainte intégrés. Cette dissociation n'est pas seulement descriptive : elle a des effets pénaux concrets, car elle disperse les leviers de qualification, de poursuite, de saisie des avoirs et de coopération, alors même que les auteurs tirent profit de l'unité fonctionnelle de leur dispositif. C'est cette asymétrie qui donne aujourd'hui à l'extorsion transnationale son avantage structurel. L'auteur ou le réseau ne font pas étalage de l'unité de leur action ; ils bénéficient au contraire de sa fragmentation. L'État, lui, doit patiemment reconstituer des liens entre des actes, des lieux, des personnes, des supports et des flux. Tant qu'il le fera à travers des appareils trop compartimentés, il réagira plus lentement que les acteurs coercitifs. Et cette lenteur, dans un environnement numérique, n'est jamais neutre : elle devient une ressource pour les auteurs.

Se pose alors une question de souveraineté très concrète. Une démocratie libérale ne se définit pas seulement par la qualité de ses normes, mais aussi par sa capacité à empêcher que son territoire, ses infrastructures numériques ou ses circuits financiers soient utilisés comme supports d'une contrainte exercée au détriment de personnes situées à l'extérieur. Lorsqu'un dispositif de chantage, de diffamation ou de pression financière peut être piloté depuis le Canada, mobiliser des relais canadiens et produire ses effets principaux à l'étranger sans réponse suffisamment intégrée, c'est la capacité même de l'État à qualifier, coordonner et protéger qui se trouve fragilisée. L'enjeu n'est donc pas seulement d'établir qu'une infraction a été commise, mais de comprendre pourquoi un tel dispositif peut encore trouver au Canada les conditions de sa projection et de sa durée.

Une vulnérabilité canadienne, un avertissement pour les démocraties libérales

Le premier impératif pour le Canada est d'ordre intellectuel. Il faut cesser de traiter l'extorsion numérique transnationale comme une juxtaposition de faits criminels et davantage la lire comme une chaîne de coercition. Cette chaîne peut inclure diffamation, publication de renseignements privés, menaces, transferts de fonds, intermédiaires, comptes de repli, circuits informels et contournement d'ordonnances judiciaires. Tant que l'analyse restera fragmentée, la réponse restera en retard.

Le deuxième impératif est institutionnel. Les informations détenues par la police, les autorités frontalières, les cellules de lutte contre le blanchiment, les procureurs et, lorsque c'est pertinent, les services de renseignements criminels doivent pouvoir être agrégées plus rapidement autour des dossiers d'extorsion transnationale. Le Canada a commencé à s'en approcher avec les groupes de travail, les sommets intergouvernementaux, la mobilisation de l'Agence des services frontaliers et la lecture financière du phénomène. Pour autant, cette logique demeure encore trop centrée sur l'extorsion de réseau criminel classique, alors qu'elle doit intégrer pleinement le versant réputationnel, informationnel et extraterritorial de la menace.

Cette montée en puissance suppose aussi des formes plus spécialisées de réponse. Sans transposer mécaniquement les modèles européens, le Canada gagnerait à mieux articuler ses capacités de poursuite avec les instruments de coopération déjà disponibles : l'entraide judiciaire et l'extradition coordonnées par le Groupe d'entraide internationale du ministère de la Justice, les échanges policiers via INTERPOL, la coopération opérationnelle avec EUROPOL, et, lorsque cela est pertinent, des formes de coordination judiciaire plus intégrées inspirées des pratiques d'EUROJUST et des équipes communes d'enquête. L'idée n'est pas

de présenter le Canada comme isolé, mais de souligner que l'institutionnalisation de ce type de contentieux y demeure moins intégrée que dans certaines configurations européennes.

Le troisième impératif est juridique. Le Canada doit mieux penser le préjudice extraterritorial lorsque la chaîne de coercition est administrée depuis son territoire. Il ne suffit pas de constater qu'aucune victime n'a été extorquée « au Québec » si l'intimidation, la diffusion, les relais ou les flux partent du Québec. Dans l'environnement numérique, le lieu d'émission de la contrainte compte autant que le lieu où elle produit son dommage maximal. Une démocratie sérieuse ne peut pas s'exonérer de sa responsabilité analytique et opérationnelle sous prétexte que la victime principale se trouve à l'étranger.

Le quatrième impératif est financier. Cette réflexion prend d'ailleurs un relief particulier depuis que le gouvernement fédéral a confirmé, au printemps 2026, la création de l'Agence canadienne des crimes financiers. Une telle structure pourrait utilement renforcer la lutte contre les dispositifs décrits ici, en améliorant la traçabilité des flux, le suivi des montages opaques et l'articulation entre blanchiment, fraude et extorsion. Elle ne suffira toutefois pas à elle seule si la réponse publique ne parvient pas aussi à intégrer le versant réputationnel, numérique et extraterritorial de la contrainte. L'opacité des circuits informels de transfert, comme le *hawala* lorsqu'il est utilisé hors des cadres de conformité, doit être traitée non comme une note de bas de page, mais comme une composante centrale de l'extorsion transnationale. Dès lors que la coercition numérique s'accompagne de flux opaques, de relais canadiens et de montages destinés à brouiller la traçabilité des fonds, la lutte contre le chantage devient aussi une lutte pour l'intégrité du système financier et pour la capacité de l'État à suivre la matérialité économique de la menace.

*
* *

Le cas canadien éclaire ainsi un problème plus large propre aux démocraties libérales. Leur vulnérabilité ne tient pas d'abord à l'absence de normes, mais à la difficulté de reconnaître qu'une coercition contemporaine peut être simultanément réputationnelle, financière, technique, transfrontalière et juridiquement éclatée. Tant que cette réalité reste saisie à travers des catégories séparées, les institutions publiques continueront à réagir plus lentement que des acteurs qui, eux, ont déjà appris à articuler ces dimensions dans une même chaîne d'action.

Les démocraties ouvertes protègent à juste titre la circulation de l'information, les garanties procédurales et les libertés publiques. Mais elles doivent aussi comprendre que ces mêmes espaces peuvent être convertis en instruments de pression durable lorsqu'ils sont investis par des acteurs qui ne cherchent ni l'information ni le débat, mais l'avantage coercitif. Le Canada a commencé à nommer le problème. L'enjeu, désormais, n'est plus seulement de le documenter, mais de construire une réponse capable de saisir ensemble la plateforme, le flux financier, le dommage extraterritorial et la logique systémique qui les relie. C'est à cette condition que les démocraties libérales pourront réduire l'avantage structurel qu'elles offrent encore, souvent malgré elles, à la coercition transnationale.

Crédits photo : daoleduc

•— ••— — • ••— •—• •••

Daniel Robson

Daniel Robson (@Daniel_Robson_) est un journaliste canadien indépendant spécialisé dans l'extrémisme, le terrorisme et la criminalité. Il s'intéresse également à la sécurité nationale et communautaire, ainsi qu'aux dimensions juridiques, institutionnelles et politiques de la sécurité publique (analyse des menaces, lutte contre l'impunité et réflexion sur les enjeux de sécurité au Canada).

Comment citer cette publication

Daniel Robson, « L’extorsion numérique transnationale au Canada, révélateur des vulnérabilités des démocraties libérales », *Le Rubicon*, vol. 6, 3 juillet 2026 [https://lerubicon.org/lextorsion-numerique-transnationale-au-canada-revelateur-des-vulnerabilites-des-democraties-liberales/].