L’injonction de type Anton Piller : un recours puissant à la disposition des municipalités et autres personnes morales de droit public

DHC Avocats - Anthony Pierre Freiji
10 août 2026

Dans le secteur privé, les entreprises reconnaissent généralement comme une priorité juridique la protection de leurs autres actifs commercialement sensibles, incluant, mais sans se limiter à leurs marques de commerce, leurs droits d’auteur, leurs brevets et leurs plans d’affaires. Cette préoccupation s’explique notamment par le fait que le piratage informatique, les vols d’informations découlant d’incidents de cybersécurité et les contrefaçons sont désormais omniprésents et constituent des risques à prévenir.

De la même manière, lorsqu’un employé s’approprie illégalement, sans droit ni autorisation, des fichiers ou des renseignements renfermant des informations hautement confidentielles et névralgiques — notamment des données exclusives, techniques, financières ou stratégiques — en raison de ses fonctions ou ses accès, un employeur doit agir rapidement afin de préserver ses intérêts.

Cette réalité est également partagée par les personnes morales de droit public régies par la *Loi sur les cités et villes****[1]*** ou le *Code municipal du Québec****[2]***, ainsi que la *Loi sur les compétences municipales****[3]***, ces dernières étant également assujetties, notamment, à la *Loi sur l’accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après la « **Loi sur l’accès** »), laquelle leur impose des obligations importantes à l’égard des renseignements personnels ou sensibles qu’elles recueillent dans le cadre de leurs activités à l’égard de citoyens, d’employés ainsi que de tiers avec lesquelles elles transigent.

En effet, ces dernières peuvent être confrontées à des cas d’appropriation illégale par des employés de telles données et un survol sommaire de la jurisprudence dénote que ces dernières ne se prévalent pas de l’arsenal procédural à leur disposition en vue de préserver leurs droits ainsi que ceux de tiers. Or, l’exfiltration de données ainsi que l’utilisation, la transmission ou même la vente de telles informations par un employé ou un intermédiaire peuvent causer un préjudice sérieux, voire irréparable aux municipalités. Une telle situation peut d’ailleurs être susceptible d’engager la responsabilité de la municipalité à l’égard de tiers, incluant ses citoyens, ses fournisseurs et/ou ses assureurs, de mettre en péril la sécurité de son infrastructure informatique et de ses serveurs, de perturber ses activités, notamment dans le cadre de négociations contractuelles ou de processus d’appels d’offres, et ultimement, de porter atteinte à l’intégrité et à la sécurité de ses systèmes de gestion des renseignements recueillis dans le cadre de ses activités en lien avec la Loi sur l’accès.

C’est dans ce contexte que l’ordonnance Anton Piller constitue une mesure exceptionnelle dont l’objectif est de permettre que soit saisie une preuve chez un défendeur, ce qui inclut un employé mal intentionné, sans qu’il en soit préalablement informé, afin d’éviter qu’il ne la détruise, la cache ou la fasse disparaître [4].

Une telle demande est présentée *ex parte*, c’est-à-dire sans que la partie adverse ne soit appelée à se défendre et à faire ses observations. En pratique, un défendeur n’est avisé de la situation qu’au moment où les avocats d’un demandeur, accompagnés d’un huissier de justice, d’un avocat superviseur indépendant et d’un expert informatique se présentent à son domicile ou lieu d’affaire en vue de procéder à la saisie des éléments de preuve permettant de prouver qu’il a enfreint ses droits — de propriété intellectuelle ou autres – et l’empêchant, sans scrupules, de profiter d’un préavis pour déjouer le processus judiciaire en faisant disparaître des éléments de preuve pertinents.

Afin qu’un juge ne prononce une telle ordonnance, des conditions strictes et essentielles, formulées dans l’arrêt *Anton Piller****[5]*** et reprises dans l’arrêt *Celanese****[6]***, doivent être rencontrées:

- **Preuve solide (*prima facie*)** : le demandeur doit démontrer une cause d’action extrêmement forte et bien fondée.
- **Préjudice grave** : le dommage réel ou potentiel pour le demandeur doit être très sérieux.
- **Possibilité de documents incriminants** : il faut une preuve claire que la partie adverse possède des objets ou documents visés.
- **Risque de destruction ou de disparation** : il doit exister une possibilité réelle que le défendeur détruise ou dissimule ces éléments avant qu’une audience sur le fond ait lieu.

Dans une affaire récente impliquant une municipalité et l’un de ses anciens cadres ayant procédé à l’exfiltration de milliers de fichiers[7], la Cour supérieure a émis une telle ordonnance, considérant qu’elle a pu démontrer de manière

claire et convaincante que son ancien employé s'est approprié sans droit, contrairement à son obligation de loyauté et les politiques de confidentialité en vigueur, détenant ainsi des renseignements confidentiels, sensibles, névralgiques et inconnus du public appartenant à la Ville ou des renseignements recueillis conformément aux dispositions de la Loi sur l'accès. Considérant le poste-clé du cadre, l'expérience en informatique, et les circonstances entourant l'exfiltration desdits renseignements, la Cour a conclu qu'il existait une possibilité réelle que ces derniers soient détruits ou cachés par le défendeur ou que celui-ci les fasse disparaitre, ou que ces derniers soient utilisés ou diffusés en violation des droits de son employeur ou de ceux de tiers.

Ceci dit, il y a lieu d'être sensibilisé de l'efficacité de cet outil indispensable dans le monde municipal où de tels incidents d'infiltrations peuvent survenir, et ce, considérant les risques susmentionnés.

L'accompagnement par un avocat spécialisé revêt incidemment une importance particulière, autant pour la partie qui demande et exécute l'ordonnance que pour celle qu'elle vise, compte tenu de l'ampleur des conséquences possibles de l'ordonnance.

Pour toute question en la matière, nous vous invitons à consulter notre équipe spécialisée.

---

[1] RLRQ c C-19.

[2] RLRQ c C-27.1.

[3] RLRQ c C-47.1.

[4] *IMS Health Canada Inc. c. Th!Nk Business Insights Ltd.*, 2013 QCCA 1303 paragr. 7, 8, 37, 39, 45, 48, 53 et 57.

[5] *Anton Piller KG v. Manufacturing Processes Ltd.*, [1976] 1 All ER 779 (C.A.).

[6] *Celanese Canada Inc. c. Murray Demolition Corp.,* [2006] 2 R.C.S. 189, 2006 CSC 36 paragr. 1, 28, 35, 36 et 40. Voir aussi *: Allen Entrepreneur général inc. c. Tardif*, 2023 QCCS 482 paragr. 36, 43, 111, 116, 117, 119, 120, 124, 143, 146, 148, 153, 220, 242, 247, 248, 257, 260, 270, 282, 291, 292 et 293.

[7] *A. c. B.* – l*e* dossier a été mis sous scellé jusqu'à nouvel ordre et des ordonnances de confidentialité ont été rendues – toutes références à la décision ont été omises afin d'assurer le respect des ordonnances.