2010-01F

Bibliothèque du Parlement | Library of Parliament

LES LOIS ANTI-POLLUPOSTAGE DES PAYS OCCIDENTAUX : ÉTUDE COMPARATIVE

Alysia Davies
Division des affaires juridiques et législatives

Le 18 janvier 2010

SERVICE D'INFORMATION ET DE RECHERCHE PARLEMENTAIRES
PARLIAMENTARY INFORMATION AND RESEARCH SERVICE

Le Service d'information et de recherche parlementaires de la Bibliothèque du Parlement travaille exclusivement pour le Parlement, effectuant des recherches et fournissant des informations aux parlementaires et aux comités du Sénat et de la Chambre des communes. Entre autres services non partisans, il assure la rédaction de rapports, de documents de travail et de bulletins d'actualité. Les analystes peuvent en outre donner des consultations dans leurs domaines de compétence.

THIS DOCUMENT IS ALSO PUBLISHED IN ENGLISH

TABLE DES MATIÈRES

Page

UINTRODUCTION 1

LES ÉTATS-UNIS 1

L'AUSTRALIE.....4

LA NOUVELLE-ZÉLANDE 6

L'UNION EUROPÉENNE.....8

LE ROYAUME-UNI 10

CANADA

BIBLIOTHÈQUE DU PARLEMENT
LIBRARY OF PARLIAMENT

LES LOIS ANTI-POLLUPOSTAGE DES PAYS OCCIDENTAUX : ÉTUDE COMPARATIVE

INTRODUCTION

Le Canada est le seul pays du G-8 qui n'a pas encore adopté de loi anti-pollupostage. Durant la dernière session du Parlement, le Comité sénatorial permanent des transports et des communications devait examiner un projet de loi émanant du gouvernement (Projet de loi C-27 : Loi sur la protection du commerce électronique), mais lorsque le Parlement a été prorogé, le 30 décembre 2009, ce projet de loi est mort au *Feuilleton*[1].

D'autres pays ont adopté des modèles de loi anti-pollupostage qui ont certaines similitudes avec le modèle proposé au Canada, quoiqu'ils comportent des différences en termes de consentement, d'exceptions et de sanctions. Nous ferons un tour d'horizon rapide de quelques-unes des principales caractéristiques des lois anti-pollupostage aux États-Unis, en Australie, en Nouvelle-Zélande, dans l'Union européenne et au Royaume-Uni.

LES ÉTATS-UNIS

Aux États-Unis, la principale loi anti-pollupostage est la *Controlling the Assault of Non-solicited Pornography and Marketing Act of 2003*, appelée plus communément CAN-SPAM Act. Elle s'applique aux messages électroniques commerciaux, qui sont définis au paragraphe 3(2) comme tout message électronique commercial qui a pour but principal de faire la publicité ou la promotion d'un produit ou d'un service et qui n'a rien à voir avec une transaction ou une relation commerciale préalable.

---

[1] Pour un résumé de ce projet de loi, voir Alysia Davies, *Projet de loi C-27 : Loi sur la protection du commerce électronique*, LS-645F, Ottawa, Service d'information et de recherche parlementaires, Bibliothèque du Parlement, révisé le 13 novembre 2009, http://www2.parl.gc.ca/Sites/LOP/LegislativeSummaries/Bills_ls.asp?lang=F&ls=c27&source=library_prb&Parl=40&Ses=2.

Le modèle de consentement retenu dans la CAN-SPAM Act est l'option d'opposition (art. 5), ce qui veut dire que le consentement à recevoir des messages électroniques est considéré comme implicite, à moins que le destinataire s'y oppose et indique qu'il ne veut plus recevoir ce genre de message. (La méthode est varie : on peut suivre des instructions de « désinscription » à la fin du message ou cliquer sur un lien facilitant la procédure d'opposition.) Selon la CAN-SPAM Act, les messages électroniques commerciaux doivent comprendre les éléments suivant :

i) une adresse de retour valide ou un autre mécanisme d'envoi par Internet qui permet au destinataire de s'opposer à la réception des messages et qui doit rester fonctionnel pendant au moins 30 jours après l'envoi du premier message (divisions 5(a)(3)(A)(i) et (ii) et 5(a)(5)(A)(ii));
ii) une mention claire et visible indiquant qu'il s'agit d'un message de publicité ou de sollicitation (division 5(a)(5)(A)(i));
iii) une adresse postale valide de l'expéditeur (division 5(a)(5)(A)(iii)).

Certaines exceptions permettent l'envoi de messages électroniques d'une manière différente, et il existe aussi certaines interactions entre les lois fédérales et les lois d'État qui font échapper d'autres types de messages électroniques à la compétence fédérale. Les messages électroniques découlant d'une transaction ou d'une relation commerciale préalable – par exemple lorsqu'il s'agit de régimes d'avantages, de soldes de compte, de rappels de produits, de mises à jour, de sécurité des produits ou d'abonnements – sont des exceptions à la définition de « messages électroniques commerciaux » et ne sont pas assujettis aux règles relatives à l'opposition prévues par la CAN-SPAM Act.

La CAN-SPAM Act porte également sur les messages électroniques frauduleux ou trompeurs, mais seulement dans la mesure où ils ne sont pas déjà visés par des lois d'État prévoyant d'autres infractions informatiques. Si un message frauduleux ou trompeur tombe sous le coup de lois d'État dans le cadre d'un autre type d'infraction informatique sanctionné par l'État, la CAN-SPAM Act n'est pas applicable (sous-al. 8(b)(2)(B)). Cependant, la loi fédérale (CAN-SPAM Act) l'emporte sur toutes les lois d'État régissant spécifiquement le pollupostage, de sorte que si le caractère problématique d'un message électronique a trait uniquement au pollupostage, c'est la loi fédérale et non la loi d'État qui est applicable. (Cela reste vrai même si la loi anti-pollupostage de l'État est plus restrictive que la loi fédérale, comme c'est le cas dans plusieurs États, dont la Californie.)

En cas d'infraction à la CAN-SPAM Act, les sanctions peuvent être d'ordre administratif, civil ou pénal, selon les dispositions qui sont violées. Les sanctions administratives sont appliquées par la Federal Trade Commission (FTC), qui est le principal organisme d'exécution de la CAN-SPAM Act, puisque les infractions à celle-ci sont considérées comme des actes ou des pratiques à caractère inéquitable et déloyal. Les poursuites au civil peuvent être intentées par un procureur général d'État ou par un fournisseur de services Internet (FSI) dans certains cas, bien qu'aucun droit d'action privé ne soit accordé aux citoyens ordinaires. Le département fédéral de la Justice s'occupe quant à lui des poursuites au criminel.

Certains autres organismes participent également à l'exécution de la CAN-SPAM Act, selon le type d'institution coupable d'une infraction et selon qu'il existe déjà un organisme d'exécution associé aux activités de cette institution. Par exemple, si une banque nationale fait du pollupostage, c'est l'Office of the Comptroller of the Currency qui sera l'organisme chargé de l'application de la CAN-SPAM Act. Si un courtier ou un négociant fait du pollupostage, c'est la Securities and Exchange Commission qui interviendra. Il existe d'autres organismes d'exécution éventuels, notamment la Federal Communications Commission, la Farm Credit Administration, le Secretary of Agriculture et le Secretary of Transportation, qui sont chargés de la réglementation des activités dans certains secteurs de l'économie (par. 7(b)).

Pour ce qui est des sanctions, les infractions pénales à la CAN-SPAM Act (entre autres, divers actes frauduleux comme la falsification des en-têtes de messages électroniques et l'accès non autorisé à des ordinateurs pour diffuser des pourriels) sont passibles d'amendes en vertu des dispositions du titre 18 du *United States Code*, d'une peine d'emprisonnement maximale de cinq, trois ou un ans, selon la nature de l'infraction, ou des deux. Il est également possible de demander la confiscation des biens d'un polluposteur dans le cadre de poursuites pénales (art. 4). Dans le cadre des poursuites au civil, des dommages-intérêts sont prévus par la CAN-SPAM Act, d'un maximum d'un ou de deux millions de dollars, selon que l'action est intentée par un FSI ou par un procureur d'État, outre des dommages-intérêts exemplaires le cas échéant (par. 7(f) et (g)). Quant aux sanctions administratives, la FTC jouit des pouvoirs que lui confère la *Federal Trade Commission Act* (par. 7(d)), laquelle semble inclure la possibilité de rendre des ordonnances administratives (dont la violation peut donner lieu à des amendes maximales de 11 000 $ dans chaque cas) ou d'intenter des poursuites dans certains cas, de la même façon que le département de la Justice[2]. Il lui est également loisible de rendre des injonctions (al. 7(f)(2)).

---

[2] Federal Trade Commission, « A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority », révisé en juillet 2008, http://www.ftc.gov/ogc/brfovrvw.shtm.

L'AUSTRALIE

En Australie, le pollupostage est assujetti à la *Spam Act 2003* (ci-après « SA 2003 »). Le type d'activité auquel elle s'applique est décrit en détail : les « messages électroniques commerciaux » sont les messages qui sont envoyés par Internet ou par un autre service de transmission à un compte de messagerie électronique, à un système de messages instantanés, à un compte téléphonique ou à tout autre compte du même genre (art. 5) et qui sont liés à une liste précise de fins commerciales (art. 6). (Cela n'inclut cependant pas les appels par télécopieur ou par téléphone[3].) La notion de « message » comprend les textes, les données, les messages vocaux, la musique ou d'autres sons, les images (animées ou autres) et toute autre forme d'information (art. 4).

Un message est considéré comme « commercial » s'il est envoyé à l'une des fins suivantes : publicité, promotion ou offre de biens, de services, de terres ou d'intérêts fonciers ou possibilités d'affaires ou d'investissement. Tout message destiné à obtenir de façon malhonnête un gain, un avantage financier ou un bien appartenant à une autre personne par des moyens trompeurs tombe aussi sous le coup de la SA 2003 (art. 6).

Les exceptions à la définition sont énumérées à l'annexe 1 de la SA 2003, qui est intitulée « Designated commercial electronic messages » (messages électroniques commerciaux désignés). Les messages visés par ces exceptions, comme les messages électroniques commerciaux, doivent comprendre des renseignements sur la personne ou l'organisation qui autorise l'envoi du message (en application de l'art. 17 de la SA 2003), mais il n'est pas nécessaire qu'ils soient conformes à l'article 16 (interdiction de communications non sollicitées) ou à l'article 18 (obligation de fournir un moyen de désinscription).

Les exceptions comprennent les messages qui ne contiennent que des renseignements factuels accompagnés d'éléments spécifiques, par exemple les coordonnées de l'expéditeur et de l'auteur, qui ne sont pas de nature commerciale (art. 2 de l'annexe 1), ainsi que les messages autorisés par des organismes gouvernementaux, des partis politiques enregistrés, des organisations religieuses et des organismes caritatifs (art. 3 de l'annexe 1). Les messages transmis par des établissements d'enseignement à leurs étudiants ou anciens étudiants sont une autre exception (art. 4 de l'annexe 1). D'autres exceptions peuvent être précisées par règlement (art. 5 de l'annexe 1).

---

[3] Voir le par. 5(5) de la SA 2003 et l'art. 2.1 du *Spam Regulations 2004*.

Le modèle de consentement, qui est axé sur un système d'opposition, est explicité à l'annexe 2. Il peut être inféré du comportement d'une personne ou d'une organisation ainsi que de leurs liens d'affaires ou autres (art. 2 de l'annexe 2). Il y a aussi une disposition de « publication très visible » selon laquelle les adresses de courriel ne peuvent pas être recueillies pour être employées du simple fait qu'elles sont affichées dans un endroit accessible au public, mais elles peuvent être utilisées pour communiquer avec certaines catégories de personnes. La liste des exemples proposés inclut les adresses affichées d'employés, d'administrateurs, de partenaires et de détenteurs de charges officielles (al. 4(2)(a) et (b) de l'annexe 2). Cependant, si ces adresses sont accompagnées d'un avertissement indiquant que les titulaires de ces comptes ne souhaitent pas recevoir de messages électroniques non sollicités, elles ne peuvent pas être employées à cette fin (al. 4(2)(d) de l'annexe 2).

L'exécution de la SA 2003 passe par les tribunaux (notamment par la Cour fédérale de l'Australie), qui peuvent imposer des amendes au civil ainsi que des dommages-intérêts aux victimes, ou encore confisquer des avantages financiers pour le compte de la Couronne le cas échéant. Les tribunaux peuvent aussi rendre des injonctions et accepter un engagement des coupables par lequel ils acceptent de cesser certains types d'activité. Les poursuites peuvent être intentées par l'Australian Communications and Media Authority (ACMA), qui est le principal organisme d'exécution de la SA 2003 (art. 26). Si le tribunal conclut qu'un tiers a été victime d'une infraction à la SA 2003, l'ACMA ou le tiers en question peut demander une indemnisation en plus des sanctions imposées au civil (art. 28).

Le montant de l'amende varie selon que le coupable a des antécédents ou non, selon qu'il s'agit d'un particulier ou d'une entreprise et selon la disposition violée (par. 25(1)). Les sanctions sont formulées en termes d'« unités », notion australienne désignant une amende déterminée par la Couronne, qui est révisée et mise à jour régulièrement. Les amendes les plus importantes sont imposées lorsque le coupable a expédié des messages électroniques commerciaux non sollicités ou a fourni de l'aide, des moyens, des conseils, des instruments ou induit, sciemment participé ou conspiré avec d'autres dans le but d'expédier ce genre de messages. Dans ce cas, l'amende maximale qui peut être imposée à un particulier sans antécédents va de 20 unités par infraction à 400 unités par jour en cas d'infractions multiples. L'amende maximale applicable à une entreprise sans antécédents va de 100 unités par infraction à 2 000 unités par jour en cas d'infractions multiples (les amendes maximales augmentent si le

coupable a des antécédents). L'unité d'amende fédérale actuelle s'élève à 110 $A[4], de sorte qu'une sanction de 400 unités équivaut à 44 000 $A et une amende de 2 000 unités, à 220 000 $A.

Les amendes maximales applicables aux autres infractions à la SA 2003 (p. ex. le fait de ne pas inclure des renseignements exacts sur l'expéditeur) sont moindres.

LA NOUVELLE-ZÉLANDE

Les mesures anti-pollupostage de la Nouvelle-Zélande sont régies par la *Unsolicited Electronic Messages Act 2007* (ci-après « UEMA 2007 »), qui contient des dispositions très semblables à celles de la loi australienne, mais également certaines particularités.

Un message électronique commercial est défini comme tout message envoyé par un service de télécommunications à une adresse électronique dans le but de commercialiser ou de promouvoir des produits, des services, des propriétés, des intérêts fonciers ou des possibilités d'investissement ou de faciliter l'obtention d'un avantage financier ou d'un gain, par communication directe ou au moyen d'un lien (art. 5 et 6). Comme dans le cas de la loi australienne, le message électronique peut être un message envoyé à un compte de courriel, à un système de messages instantanés, à un compte téléphonique ou à tout autre compte du même genre, mais non un appel vocal ou un message télécopié (annexes de l'UEMA 2007). Sont également visées toutes les formes spécifiques d'information qui sont énumérées dans la loi australienne, qu'il s'agisse de textes, de vidéos ou d'enregistrements sonores, (art. 4).

La loi néo-zélandaise contient une liste très précise d'exceptions à la notion de message électronique commercial (art. 6). Sont exclus les cas suivants :

- fournir un prix ou une estimation concernant des produits et services à la demande du destinataire;
- faciliter, conclure ou confirmer une transaction commerciale préalablement convenue;
- fournir des renseignements en matière de garantie, de rappel ou de sécurité sur des produits ou services achetés par le destinataire;

[4] *Crimes Act 1914*, art. 4AA.

- fournir des renseignements factuels concernant un abonnement, une affiliation, un compte, un prêt ou toute autre transaction préalable;
- fournir de l'information renvoyant directement à une relation d'emploi ou à un régime d'avantages;
- fournir des produits et des services (p. ex. des mises à jour) que le destinataire est en droit de recevoir en raison d'une transaction préalable;
- fournir au destinataire de l'information sur les produits et les services d'un organisme gouvernemental ou d'un tribunal;
- remplir d'autres fonctions prévues par la réglementation.

Les messages électroniques commerciaux doivent remplir les conditions habituelles concernant l'exactitude des coordonnées de l'expéditeur et la possibilité de se désinscrire, et ils ne peuvent pas être non sollicités (art. 9 à 11).

Le modèle de consentement est celui de l'opposition, qui permet de considérer que le consentement est implicite d'après le comportement, les relations d'affaires ou autres ainsi que d'autres circonstances prévues dans la réglementation (art. 4). L'UEMA 2007 prévoit également une disposition de « publication très visible » qui permet de recueillir des adresses de courriel si elles sont affichées officiellement dans un endroit accessible au public sans message d'avertissement indiquant qu'elles ne peuvent pas être employées aux fins d'envoi de messages électroniques non sollicités (art. 4).

L'exécution de l'UEMA 2007 incombe au ministère des Affaires internes, qui comprend un service de vérification de la conformité à la réglementation anti-pollupostage chargé de recevoir les plaintes et de procéder aux enquêtes[5]. Celui-ci peut délivrer des avertissements et des avis d'infraction et accepter un engagement des coupables par lequel ils acceptent de cesser leurs activités (par. 19(b) et 19(c)). Ce service est également habilité à faire appel aux tribunaux pour obtenir des réparations en cas d'infraction à l'UEMA 2007 (par. 19(c)). Les causes tombant sous le coup de l'UEMA 2007 peuvent être portées à l'attention de la Cour de district ou de la Haute Cour, selon le type d'infraction (art. 37 et 38 de l'UEMA 2007).

---

[5] Ministère des Affaires internes de la Nouvelle-Zélande, « Anti-Spam », http://www.dia.govt.nz/DIAwebsite.nsf/wpg_URL/Services-Anti-Spam-Index.

Par ailleurs, toute personne victime d'une violation de l'UEMA 2007 jouit, en Nouvelle-Zélande, d'un droit d'action privé (par. 19(a)), et le service d'exécution du Ministère peut s'associer à toute action de ce genre (par. 19(c)).

Les tribunaux peuvent imposer des amendes maximales de 200 000 $NZ à un particulier et de 500 000 $NZ à une organisation (art. 45 et 48), ainsi que des indemnités ou des dommages-intérêts, le cas échéant (art. 46 et 48).

L'UNION EUROPÉENNE

Les directives de l'Union européenne (UE) doivent être adoptées sous forme de lois dans l'ensemble des 27 pays membres. La directive sur la protection de la vie privée dans le secteur des communications électroniques (ci après « DPVPSCE »)[6] a été adoptée en 2002, et ses principaux éléments ont depuis été intégrés à des lois nationales dans les pays membres, y compris le Royaume-Uni, dont nous parlerons à titre distinct dans la prochaine section.

La DPVPSCE s'appuie sur une directive antérieure, à savoir la directive sur la protection des données (ci-après « DPD »)[7] adoptée en 1995, qui fournissait un modèle de loi sur la protection de la vie privée que devaient suivre tous les pays membres. La DPD entrevoyait certains des problèmes associés au pollupostage et formulait certains principes généraux qui continuent d'être applicables dans le cadre de la lutte contre le pollupostage.

Les directives de l'UE s'appliquent à toutes les communications de vente directe par système d'appel automatique, télécopieur ou courriel (par. 13(1) de la DPVPSCE).

Le modèle de consentement est axé sur un régime d'adhésion, en fonction du précédent établi par la DPD, qui, dès son adoption, a appliqué un modèle d'adhésion optionnelle fondé sur le consentement explicite dans les situations concernant la protection de la vie privée dans les communications électroniques. Ce principe a été intégré et largement appliqué dans tous les pays de l'UE (art. 13 de la DPVPSCE; al. 14b) de la DPD).

---

6 *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)*, JO L 201 du 31.7.2002, p. 37 à 47.

7 *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, JO L 281 du 23.11.1995, p. 31 à 50.

Il y a, dans la DPVPSCE, une exception selon laquelle les coordonnées électroniques fournies volontairement par les consommateurs dans le cadre de la vente d'un produit ou d'un service peuvent être employées à des fins de vente directe de produits ou services similaires par la même entreprise selon un système d'opposition optionnelle. Le consommateur doit cependant avoir la possibilité de s'opposer dès le moment où ses coordonnées sont enregistrées ainsi que plus tard (par. 13(2) et préambule – art. 41 de la DPVPSCE).

Rappelons que cette exception est applicable aux « coordonnées électroniques en vue d'un courrier électronique » uniquement et non pas à la vente directe par les autres méthodes envisagées à l'article 13 de la DPVPSCE, à savoir par télécopieur ou par système d'appel automatique. Le régime d'adhésion reste la norme dans ces derniers cas. Le traitement des appels de vente commerciale de personne à personne est laissé, dans une certaine mesure, au gré de chaque pays, compte tenu du cadre législatif de chacun en matière de protection de la vie privée (préambule – art. 42 de la DPVPSCE).

Le « courrier électronique » est défini comme suit : « tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère » (art. 2 de la DPVPSCE).

Il y a également une distinction, dans le droit européen, entre « personne physique » (une personne) et « personne morale » (une entreprise ou organisation). La protection de la vie privée est considérée comme un droit dans le cadre juridique européen, et les dispositions relatives au consentement sont destinées à protéger les droits de toutes les personnes « physiques » qui peuvent être les destinataires de communications de vente directe, sans égard à l'expéditeur ou au moyen de communication employée. Lorsque c'est une personne « morale » (une entreprise ou organisation et non une personne « physique ») qui est le destinataire de communications de vente directe, les pays membres ont plus de latitude dans le choix de leur réglementation : certains décident, par exemple, de permettre aux entreprises de s'inscrire à un registre d'opposition pour éviter ce genre de communications. Il faut cependant prévoir une certaine protection législative pour les personnes morales également, quelle que soit la forme qu'elle prenne (par. 13(5) et préambule – art. 45 de la DPVPSCE).

La vente directe par courriel au moyen d'une fausse identité ou sans mécanisme optionnel d'opposition est interdite (par. 13(4) de la DPVPSCE).

Les organismes d'exécution de la loi et les sanctions sont désignés par chaque pays membre dans sa loi nationale.

LE ROYAUME-UNI

Comme dans le cas de l'Union européenne, les règles anti-pollupostage du Royaume-Uni s'appuient sur un cadre législatif existant. La DPVPSCE de l'UE a été intégrée au droit britannique au moyen du *Privacy and Electronic Communications (EC Directive) Regulations 2003* (ci-après « Règlement »), qui, de concert avec la *Data Protection Act 1998* (ci-après « DPA 1998 »), prévoit des mesures précises contre le pollupostage.

Les règles britanniques en matière de pollupostages s'appliquent à toutes les communications de vente directe effectuées par système d'appel automatique, télécopieur ou courriel (y compris les textes, vidéos, enregistrements sonores ou images transmis par voie électronique). Les Britanniques incluent dans leur version les appels téléphoniques vocaux (art. 2 et 19 à 23 du Règlement).

Comme le prévoit la directive de l'UE et conformément à la perspective européenne de la protection de la vie privée, le modèle de consentement est du type adhésion (art. 19 à 22 du Règlement et art. 7 à 12 de la DPA 1998). Conformément à la directive de l'UE, il y a une exception, à savoir les adresses de courriel fournies volontairement par les consommateurs dans le cadre d'une vente ou de négociations en vue de la vente d'un produit ou service, qui peuvent être employées pour faire la promotion de produits ou services semblables, à la condition qu'il y ait une option d'opposition (art. 22 du Règlement). Il semble également exister des registres d'exclusion pour les appels par téléphone et par télécopieur (art. 25 et 26 du Règlement).

Il est interdit d'expédier des messages par courriel assujettis au Règlement sans indiquer l'identité exacte de l'expéditeur et une adresse valide de désinscription (art. 23 du Règlement).

L'exécution des mesures législatives incombe au commissaire à l'information, qui supervise l'application de la DPA 1998 et du Règlement et qui fait enquête sur les plaintes et rend ses conclusions sous la forme de divers « avis » (art. 31 et 32 du Règlement et partie V de la DPA 1998). Il est possible de faire appel des conclusions du commissaire auprès du Tribunal de l'information, lequel peut entendre les plaignants concernant tous les avis de décision, les avis

d'information, les avis d'exécution et les avis d'information spéciaux rendus par le commissaire (art. 48 de la DPA 1998). D'autres appels sont autorisés sur des points de droit seulement (art. 49 de la DPA 1998).

Le non-respect d'un avis du commissaire à l'information constitue une infraction pénale pouvant faire l'objet de poursuites et d'une amende maximale fixée actuellement à 5 000 £ en Angleterre et au Pays de Galle, et à 10 000 £ en Écosse[8] (art. 47 et 60 de la DPA 1998)[9].

Toute personne qui souhaite demander des dommages-intérêts en raison d'une violation du Règlement jouit d'un droit d'action privé (art. 30 du Règlement).

---

8 *Criminal Justice Act 1982*, art. 74, interprétée parallèlement avec la *Magistrates' Courts Act 1980*, par. 32(9) (pour l'Angleterre et le Pays de Galles), telle que modifiée par la *Criminal Justice Act 1991*, art. 17; *Criminal Procedure (Scotland) Act 1995*, par. 225(8), modifiée (pour l'Écosse).

9 Les seuls cas dans lesquels une amende d'un montant différent peut être imposée en vertu de la loi sont ceux d'entrave ou de non-assistance à l'exécution d'un mandat ou à l'inspection de systèmes d'information étrangers par le commissaire. Dans de tels cas, l'amende peut atteindre le maximum du barème normal (une mesure distincte du maximum fixé par la DPA 1998), qui est de 5 000 £ en Angleterre, en Écosse et au Pays de Galle (*Criminal Justice Act 1982*, art. 37, à laquelle se substituent la *Criminal Justice Act 1991*, art. 17 (pour l'Angleterre et le Pays de Galle), et la *Criminal Procedure (Scotland) Act 1995*, art. 225 (pour l'Écosse)).