TABLEAU COMPARATIF DES LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Groupe de pratique Protection des renseignements confidentiels et vie privée de Fasken

FASKEN

Responsables du groupe à l'échelle nationale : Antoine Aylwin et Alex Cameron
Conseillère stratégique : Jennifer Stoddart[1]

		QUÉBEC	ALBERTA	COLOMBIE-BRITANIQUE	CANADA	UNION EUROPÉENNE
		Loi sur la protection des renseignements personnels dans le secteur privé (LPRPSP)[2]	*Alberta Personal Information Protection Act* (PIPA-AB)	*BC Personal Information Protection Act* (PIPA-BC)	*Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)*	*Règlement général sur la protection des données (RGPD)*
1.	**Entrée en vigueur**	le 1er janvier 1994, au Québec	le 1er janvier 2004, en Alberta	le 1er janvier 2004, en Colombie-Britannique	le 1er janvier 2001, au Canada (s'applique à toute organisation depuis le 1er janvier 2004)	le 27 avril 2016 (pleinement en vigueur depuis le 25 mai 2018), dans l'UE/EEE
2.	**Autorité responsable**	Commission d'accès à l'information du Québec (CAI)	Office of the Information and Privacy Commissioner of Alberta (OIPC-AB)	Office of the Information and Privacy Commissioner for British Columbia (OIPC-BC)	Office of the Privacy Commissioner of Canada (OPC)	• Autorité responsable de chaque État membre (par exemple en France : Commission nationale de l'informatique et des libertés -CNIL) • Comité européen de la protection des données
3.	**Champ d'application**	• Toute « entreprise » (au sens du Code civil du Québec) qui recueille, détient, utilise ou communique des renseignements personnels • À l'exclusion des organismes publics au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1)	• Toute organisation qui recueille, utilise ou divulgue des renseignements personnels • À l'exclusion des « informations sur la santé » auxquelles s'applique la *Health Information Act de* l'Alberta • À l'exclusion des renseignements personnels auxquels s'applique la *Freedom of Information and Protection of Privacy Act de l'Alberta* (c.-à-d. les organismes publics provinciaux de l'Alberta)	• Toute organisation qui collecte, utilise ou divulgue des renseignements personnels • Exclut les renseignements personnels auxquels s'applique la LPRPDE • Exclut les renseignements personnels auxquels s'applique la *Freedom of Information and Protection of Privacy Act* de la Colombie-Britannique (c'est-à-dire les organismes publics provinciaux de la C.-B.)	• Toute organisation qui recueille, utilise ou divulgue des renseignements personnels dans le cadre d'activités commerciales au Canada ou ayant un lien réel et substantiel avec le Canada • À l'exclusion des institutions gouvernementales auxquelles s'applique la Loi sur la protection des renseignements personnels (L.R.C. (1985), ch. P-21 2) • Possibility of exclusion from the application of PIPEDA in certain provinces (by decree) • Ne concerne que les employés ou les candidats à un emploi dans une organisation qui collecte, utilise ou divulgue des renseignements personnels dans le cadre de l'exploitation d'une entreprise fédérale	• Critère d'établissement : le responsable du traitement ou le sous-traitant doit être établi dans l'UE/EEE • Le responsable du traitement est établi en dehors de l'UE/EEE, mais ses activités de traitement sont liées à l'offre de biens ou de services aux personnes concernées dans l'UE/EEE ou sont liées à la surveillance du comportement des personnes concernées dans l'UE/EEE • Aucune distinction n'est faite entre le secteur privé et le secteur public

[1] *Avocats du groupe de pratique national Protection des renseignements confidentiels et vie privée de Fasken. Ce document ne prétend pas être exhaustif et ne constitue en aucune façon un avis juridique. Ce document a été mis à jour pour la dernière fois le 1er mars 2020.*

[2] *Le Projet de loi n°64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels a été présenté à l'Assemblé nationale le 12 juin 2020 et prévoit notamment plusieurs propositions d'amendements à la Loi sur la protection des renseignements personnels dans le secteur privé.*

[3] *L'expression « personne concernée » a été utilisée dans le présent document à des fins de commodité uniquement, et n'est pas nécessairement représentative de la terminologie utilisée dans les différentes lois et réglementations.*

		Québec	Alberta	Colombie-Britanique	Canada	Union européenne
4.	**Renseignements personnels (ou « données à caractère personnel »)**	• Tout renseignement concernant une personne physique et permettant de l'identifier • Quelle que soit la nature de son support et de son format (écrit, graphique, enregistrement, film, fichier informatique ou autre) • Couvre également les employés et les candidats à un emploi	• Tout renseignement concernant une personne identifiable • Exclut les « coordonnées professionnelles » collectées, utilisées ou divulguées dans le but de permettre à une personne d'être jointe en rapport avec ses responsabilités professionnelles	• Tout renseignement concernant une personne identifiable, y compris les « renseignements personnels des employés » • Exclut les « coordonnées » et les « informations sur le produit du travail »	• Tout renseignement concernant une personne identifiable • Quels que soient le format ou les caractéristiques physiques • Régime particulier pour les « coordonnées professionnelles » (nom, fonction, titre, adresse, numéro de téléphone professionnel, etc.)	• Tout renseignement concernant une personne physique identifiée ou identifiable (y compris un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou un facteur propre à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale) • Quel que soit le support ou le format
5.	**Renseignements sensibles**	• Pas de définition de « renseignements sensibles » • Assurer un niveau de sécurité adapté à la sensibilité des renseignements	• Pas de définition de « renseignements sensibles » • En cas de consentement implicite, la collecte, l'utilisation ou la divulgation de renseignements personnels doit être raisonnable compte tenu de leur sensibilité	• Pas de définition de « renseignements sensibles » • En cas de consentement implicite, la collecte, l'utilisation ou la divulgation de renseignements personnels doit être raisonnable compte tenu de leur sensibilité	• Pas de définition des « renseignements sensibles » • Assurer un niveau de sécurité adapté à la sensibilité des renseignements	• Régime particulier pour les « catégories spéciales de données à caractère personnel » (y compris l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, les données biométriques, les données relatives à la santé, à la vie sexuelle ou à l'orientation sexuelle) • Pas de régime distinct pour les données financières
6.	**Consentement**	• Doit être manifeste, libre et éclairé, et doit être donné à des fins précises. Ce consentement n'est valable que pour la durée nécessaire pour la réalisation des objectifs pour lesquels il a été demandé • Aucun détail concernant le retrait du consentement • Non requis lorsqu'une exception s'applique	• Peut être explicite ou implicite, chacun étant soumis à des exigences et à des limites précises • Peut être retiré à tout moment moyennant un préavis raisonnable, à moins que le retrait du consentement n'empêche l'exécution d'une obligation légale • Non requis lorsque des exceptions s'appliquent (par exemple, dans le cas d'une « transaction commerciale »)	• Peut être explicite ou implicite, chacun étant soumis à des exigences et à des limites précises • Peut être retiré à tout moment moyennant un préavis raisonnable, à moins que le retrait du consentement n'empêche l'exécution d'une obligation légale • Non requis lorsqu'une exception s'applique (par exemple, dans le cas d'une « transaction commerciale »)	• Peut être explicite ou implicite selon les circonstances et le type de renseignements, en tenant compte des attentes raisonnables de la personne concernée • Doit généralement être exprimé lors du traitement de renseignements sensibles • Peut être retiré à tout moment, sous réserve de restrictions légales ou contractuelles et d'un préavis raisonnable • Non requis lorsque des exceptions s'appliquent (par exemple, dans le cas d'une « transaction commerciale »)	• Doit être librement donné, spécifique, éclairé et sans ambiguïté, sous une forme intelligible et accessible, et n'est valable qu'à des fins précises • Doit être « explicite » pour le traitement de catégories particulières de renseignements personnels • Peut être retiré à tout moment • Un autre motif juridique peut s'appliquer, comme la nécessité d'exécuter un contrat ou les finalités légitimes du responsable du traitement
7.	**Enfants**	Pas d'âge minimum pour le consentement des mineurs, à l'exception d'un article relatif aux renseignements de nature médicale ou sociale (mais sous réserve des règles générales du Code civil du Québec)	Pas d'âge minimum pour le consentement des mineurs, mais ils doivent être suffisamment âgés pour donner un consentement valable	Pas d'âge minimum pour le consentement des mineurs, mais ils doivent être suffisamment âgés pour donner un consentement valable	Pas d'âge minimum pour le consentement des mineurs, mais généralement valable à partir de 13 ans	• L'âge minimum pour le consentement des mineurs est de 16 ans, sauf autorisation du titulaire de la responsabilité parentale • Les États membres peuvent prévoir un âge inférieur à 16 ans, à condition que cet âge inférieur ne soit pas inférieur à 13 ans

		QUÉBEC	ALBERTA	COLOMBIE-BRITANIQUE	CANADA	UNION EUROPÉENNE
8.	**Droit d'accès**	• Oui, sous réserve de certaines exceptions, notamment en cas de litige ou s'il risque de porter gravement préjudice à un tiers Oui, sous réserve de certaines exceptions, notamment en cas de litige ou s'il risque de porter gravement préjudice à un tiers • Demande d'accès par écrit avec preuve d'identité • Réponse dans les 30 jours • Gratuit (des frais raisonnables peuvent être exigés dans certaines conditions) • L'entreprise a l'obligation de fournir une assistance	• Oui, sous réserve de certaines exceptions, notamment lorsque les renseignements sont protégés par un privilège juridique ou que leur divulgation pourrait révéler des renseignements personnels sur une autre personne ou menacer sa vie ou sa sécurité • Demande d'accès par écrit • Réponse dans un délai de 45 jours civils (ce délai peut être prolongé) • Une redevance peut être exigée dans certaines conditions • Une organisation doit faire tous les efforts raisonnables pour aider chaque demandeur	• Oui, sous réserve de certaines exceptions, notamment lorsque les renseignements sont protégés par le secret professionnel de l'avocat ou que leur divulgation pourrait révéler des renseignements personnels sur une autre personne ou menacer sa santé ou sa sécurité • Demande d'accès par écrit • Réponse dans les 30 jours ouvrables (ce délai peut être prolongé) • Une redevance peut être exigée dans certaines conditions • Une organisation doit faire un effort raisonnable pour aider chaque demandeur	• Oui, sous réserve de certaines exceptions, notamment en cas de litige ou lorsque les renseignements contiennent des références à des tiers ou ne peuvent être divulgués pour des raisons juridiques, de sécurité ou commerciales • Demande d'accès par écrit • Réponse dans les 30 jours (ce délai peut être prolongé) • Une redevance peut être exigée sous certaines conditions • Une organisation doit aider toute personne qui en fait la demande	• Oui, sous réserve de certaines exceptions, y compris pour des raisons juridiques ou de sécurité • En cas de doute raisonnable sur l'identité de la personne concernée, il est possible de demander une confirmation de son identité • Réponse donnée par écrit ou verbalement (à la demande de la personne concernée) • La réponse doit être donnée sans retard excessif et dans tous les cas dans un délai d'un (1) mois (ce délai peut être prolongé) • Gratuit (des frais raisonnables peuvent être exigés, sous certaines conditions) • Obligation de faciliter l'exercice des droits d'accès
9.	**Droit de corriger (ou de rectifier)**	• Oui, si les renseignements sont inexacts ou incomplets • Les exigences en matière de droit d'accès s'appliquent avec les modifications nécessaires	• Oui, s'il y a une erreur ou une omission dans les renseignements personnels • Demande de correction par écrit • Doit corriger l'information dès que cela est raisonnablement possible • Aucuns frais ne peuvent être perçus	• Oui, s'il y a une erreur ou une omission dans les renseignements personnels • Demande de correction par écrit • Doit corriger l'information dès que cela est raisonnablement possible • Aucuns frais ne peuvent être perçus • Si la correction est refusée, doit annoter le dossier	• Oui, si les renseignements sont inexacts ou incomplets • Les exigences en matière de droit d'accès s'appliquent avec les modifications nécessaires	• Oui, si les données sont inexactes ou incomplètes • Les droits d'accès s'appliquent avec les modifications nécessaires
10.	**Droit à l'effacement (ou « droit à l'oubli »)**	Non	Non	Non	Non	Oui (sous certaines conditions)

		QUÉBEC	ALBERTA	COLOMBIE-BRITANIQUE	CANADA	UNION EUROPÉENNE
11.	**Autres droits**	Droit de soumettre une demande à la CAI pour l'examen d'un désaccord	Droit de déposer une plainte auprès de l'OIPC-AB ou de demander la révision de la décision d'une organisation relative à la demande d'un particulier portant sur des renseignements personnels	• Droit de déposer une plainte auprès de l'organisation • Droit de déposer une plainte auprès de l'OIPC-BC ou de demander la révision d'une décision prise par une organisation concernant la demande d'accès ou de correction de renseignements personnels d'une personne	• Droit d'adresser à l'organisation une contestation concernant la non-conformité à la LPRPDE • Droit de déposer une plainte auprès de l'OPC	• Droit de déposer une plainte auprès de l'autorité responsable compétente • Droit à la limitation du traitement des renseignements personnels • Droit à la portabilité renseignements personnels • Droit de s'opposer au traitement de renseignements personnels • Droit de ne pas faire l'objet d'une décision fondée uniquement sur un traitement automatisé
12.	**Responsable de la protection de la vie privée**	Pas de disposition spécifique	L'organisation doit désigner une ou plusieurs personnes responsables du respect de la PIPA-AB	L'organisation doit désigner une ou plusieurs personnes responsables du respect de la PIPA-BC, et mettre à disposition le nom ou le titre du poste et les coordonnées de chacune de ces personnes	Obligation de désigner une personne responsable du respect de la LPRPDE et de communiquer l'identité de cette personne	Obligation de désigner un « délégué à la protection des données » dans certaines circonstances, y compris le traitement à grande échelle de catégories particulières de données ou les opérations de traitement qui nécessitent un suivi régulier et systématique des personnes concernées à grande échelle
13.	**Obligations de transparence**	Obligation d'informer la personne concernée de l'objet du dossier, de l'utilisation qui sera faite des renseignements et des catégories de personnes qui y auront accès au sein de l'entreprise, ainsi que du lieu où le dossier sera conservé et des droits d'accès et de rectification	L'organisation doit fournir sur demande des renseignements sur ses politiques et pratiques de conformité à la PIPA-AB, y compris sur son recours à des fournisseurs de services à l'étranger pour la collecte, l'utilisation, la divulgation ou le stockage de renseignements personnels	Doit fournir sur demande des renseignements sur ses politiques et ses pratiques en matière de conformité avec la PIPA-BC, et sur sa procédure de réponse aux plaintes	• Doit rendre facilement accessibles aux personnes, sous un format généralement compréhensible, les politiques et pratiques relatives à la gestion des renseignements personnels • Doit informer la personne du type de renseignements personnels détenus par l'organisation, y compris un compte rendu général de leur utilisation, comprenant tous détails supplémentaires • Doit être en mesure d'expliquer aux personnes concernées les raisons pour lesquelles les renseignements sont recueillis	• Doit fournir à la personne concernée une grande variété de renseignements au moment où les données sont obtenues (finalités du traitement, fondements juridiques, destinataires, transfert des données, durée du stockage, droits applicables, coordonnées du responsable du traitement ou du délégué à la protection des données, etc.) • Doit fournir tout renseignement sous une forme concise, transparente, intelligible et facilement accessible, en utilisant un langage clair et simple

		QUÉBEC	ALBERTA	COLOMBIE-BRITANIQUE	CANADA	UNION EUROPÉENNE
14.	**Mesures de sécurité**	Mettre en œuvre les mesures de sécurité nécessaires pour assurer la protection des renseignements personnels qui sont raisonnables compte tenu de la sensibilité des renseignements, des fins auxquelles ils seront utilisés, de la quantité et de la répartition des renseignements et du support sur lequel ils sont stockés	L'organisation doit prendre des mesures de sécurité raisonnables contre des risques comme l'accès, la collecte, l'utilisation, la divulgation, la copie, la modification, l'élimination ou la destruction non autorisés	Doit prendre des mesures de sécurité raisonnables pour empêcher l'accès, la collecte, l'utilisation, la divulgation, la copie, la modification, l'élimination non autorisés ou tout autre risque	• Mettre en œuvre des mesures de sécurité, y compris des mesures physiques, organisationnelles et technologiques, en fonction de la sensibilité des renseignements, de la quantité, de la répartition et du format des renseignements, ainsi que la méthode de stockage • Obligation de sensibiliser les employés à l'importance de préserver la confidentialité des renseignements personnels	Mettre en œuvre des mesures techniques et organisationnelles pour assurer un niveau de sécurité adapté au risque (y compris la pseudonymisation et le cryptage des données, le cas échéant)
15.	**Signalement d'une atteinte**	Signalement facultatif (formulaire disponible en ligne)	• Signalement à l'OIPC-AB dès que possible de tout accès non autorisé à des renseignements personnels ou de toute divulgation de ceux-ci qui crée un « risque réel de préjudice important » • L'OIPC-AB peut exiger une notification aux personnes qui courent un « risque réel de préjudice important »	• Aucune obligation • Signalement facultatif à l'OIPC-BC (formulaire disponible en ligne)	• Signalement au Commissariat à la protection de la vie privée, dès que possible, de toute violation qui crée un « risque réel de préjudice important » • Signalement à la personne dès que possible de toute infraction qui crée un « risque réel de préjudice important » pour elle • Conserver un registre de chaque violation de données et, sur demande, donner au Commissariat à la protection de la vie privée l'accès à ce registre (*Règlement sur les atteintes aux mesures de sécurité)*	• Signalement à l'autorité de contrôle sans retard injustifié et, si possible, au plus tard 72 heures après avoir eu connaissance de l'incident dans certaines circonstances • Communiquer avec la personne concernée sans retard injustifié lorsque la violation des données est susceptible d'entraîner un risque élevé pour les droits et libertés, sous certaines conditions
16.	**Transfert permis vers des territoires étrangers**	• Hors Québec • Oui, y compris par voie contractuelle, en prenant toutes les mesures raisonnables pour garantir que les renseignements ne seront pas utilisés à des fins non pertinentes par rapport à l'objet du dossier ni communiqués à des tiers sans le consentement des personnes concernées	• En dehors de l'Alberta • Oui, mais si l'organisation utilise un fournisseur de services à l'extérieur du Canada pour recueillir, utiliser, divulguer ou conserver des renseignements personnels, alors la politique de confidentialité doit divulguer des renseignements concernant a) les pays autres que le Canada où la collecte, l'utilisation, la divulgation ou la conservation peuvent avoir lieu, et b) les fins pour lesquelles le fournisseur de services à l'extérieur du Canada a été autorisé à recueillir, utiliser ou divulguer des renseignements personnels	• En dehors de la Colombie-Britannique • Oui, mais la divulgation dans la politique de confidentialité est recommandée par l'OIPC-BC	• À l'extérieur du Canada • Oui, par voie contractuelle ou autre, à condition qu'un niveau comparable de protection soit assuré pour les renseignements personnels • Les personnes doivent être informées que leurs renseignements peuvent être envoyés vers un pays étranger à des fins de traitement et qu'ils peuvent être accessibles aux tribunaux et aux autorités chargées de l'application de la loi et de la sécurité nationale de ce pays (conformément aux lignes directrices sur le transfert transfrontalier de renseignements personnels)	• En dehors de l'UE/EEE • Oui, s'il existe une « décision d'adéquation » ou d'autres garanties appropriées dans le cadre du GDPR, comme des clauses contractuelles types approuvées par la Commission européenne, des règles d'entreprise contraignantes, l'adhésion à un code de conduite ou un mécanisme de certification • Obligation de désigner un « représentant » dans un contexte extraterritorial, sous certaines conditions

		QUÉBEC	ALBERTA	COLOMBIE-BRITANIQUE	CANADA	UNION EUROPÉENNE
17.	**Autres obligations et dispositions**	Régime particulier pour les « listes nominatives » (c'est-à-dire les listes de noms, de numéros de téléphone, d'adresses géographiques de personnes physiques ou d'adresses technologiques où une personne physique peut recevoir la communication de documents ou de renseignements technologiques)			Obligation d'enquêter sur toutes les plaintes et, si une plainte est jugée justifiée, l'organisation doit prendre les mesures appropriées, y compris, si nécessaire, modifier ses politiques et ses pratiques	• Mettre en œuvre la protection des données dès la conception (*privacy by design*) et par défaut (*privacy by default*) • Les relevés d'activités de traitement requis, sauf pour une entreprise ou une organisation employant moins de 250 personnes, sous réserve de certaines conditions • L'évaluation de l'impact sur la protection des données est requise dans certaines circonstances
18.	**Rétention de renseignements**	• Pendant le temps nécessaire aux fins identifiées ou pour permettre à la personne concernée d'épuiser les recours prévus par la loi • Veiller à ce que tout dossier détenu concernant une autre personne soit à jour et exact lorsqu'il est utilisé par une entreprise pour prendre une décision visant la personne concernée • Aucun calendrier de conservation établi par un règlement gouvernemental	• Aussi longtemps que l'organisation a raisonnablement besoin des renseignements personnels à des fins juridiques ou commerciales • L'organisation doit alors a) détruire les dossiers contenant les renseignements personnels, ou b) rendre les renseignements personnels non identifiables afin qu'ils ne puissent plus être utilisés pour identifier une personne	• Obligation de détruire ses dossiers contenant des renseignements personnels, ou supprimer les moyens par lesquels les renseignements personnels peuvent être associés à des personnes en particulier, dès qu'il est raisonnable de supposer que a) le but pour lequel ces renseignements personnels ont été recueillis n'est plus servi par la conservation des renseignements personnels, et b) la conservation n'est plus nécessaire à des fins juridiques ou commerciales • Si une organisation utilise les renseignements personnels d'une personne pour prendre une décision qui la concerne directement, elle doit les conserver pendant au moins un an	• Pendant le temps nécessaire aux fins identifiées ou pour permettre à la personne d'épuiser ses recours prévus par la loi • Maintenir les renseignements personnels aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés	Pendant le temps nécessaire, mais limité au strict minimum
19.	**Sanctions statutaires**	• De 1 000 $ à 10 000 $ pour une contravention aux dispositions de la loi • De 5 000 $ à 50 000 $ pour une infraction aux règles régissant la communication de renseignements personnels à l'extérieur du Québec • Les sanctions pour les infractions ultérieures sont doublées	Jusqu'à 10 000 $ pour les particuliers et jusqu'à 100 000 $ pour les personnes autres que les particuliers si l'OIPC détermine l'infraction	Responsabilité jusqu'à 10 000 $ pour les particuliers et jusqu'à 100 000 $ pour les personnes autres que les particuliers si l'OIPC détermine l'infraction	Jusqu'à 10 000 $ (procédure sommaire) ou 100 000 $ (acte d'accusation), lorsqu'une personne fait obstruction à l'enquête sur une plainte ou à une vérification ou ne respecte pas les dispositions relatives au signalement des atteintes	Jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial ou jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial (le montant le plus élevé étant retenu) selon la nature de l'infraction

	QUÉBEC	ALBERTA	COLOMBIE-BRITANIQUE	CANADA	UNION EUROPÉENNE
20. Autres recours	• Recours possibles auprès de la CAI • Les recours possibles auprès des tribunaux (y compris l'action collective)	• Ordonnances de l'OIPC-AB sur l'achèvement d'une enquête • Dommages-intérêts pour perte ou préjudice résultant d'une violation de la PIPA-AB si l'OIPC-AB a rendu une ordonnance définitive (par le biais d'une requête au tribunal)	• Ordonnances de l'OIPC-BC sur l'achèvement d'une enquête • Dommages-intérêts pour préjudice réel résultant d'une violation du PIPA-BC si l'OIPC-BC a rendu une ordonnance définitive (par le biais d'une requête au tribunal)	• Remboursements disponibles auprès du Commissariat à la protection de la vie privée du Canada • Les recours possibles auprès des tribunaux (y compris par l'action collective)	• Remboursements disponibles auprès de l'autorité de surveillance compétente • Les recours possibles auprès des tribunaux (y compris l'action collective)