

***Panama Papers* : Pascal Eydoux redoute « l'amalgame terrifiant » entre optimisation et fraude fiscales**

le 12 avril 2016

AVOCAT | Déontologie | Responsabilité professionnelle

Pascal Eydoux, président du Conseil national des barreaux, revient sur le rôle et la responsabilité des avocats dans l'évasion fiscale. Il en profite pour pointer les premiers responsables qui, selon lui, sont les pouvoirs publics.

La rédaction : Comment réagissez-vous à l'implication d'avocats dans le système de fraude révélé par le scandale des *Panama Papers* ?

Pascal Eydoux : Si un certain nombre de nos confrères participent de manière frauduleuse à des montages répréhensibles, il appartient aux ordres d'engager un certain nombre d'enquêtes déontologiques et qui déboucheront – ou non – selon leurs conclusions sur des poursuites disciplinaires. Il n'y a aucune ambiguïté, ce sont les ordres qui ont cette responsabilité et ils doivent l'assumer. Le Conseil national des barreaux (CNB) est là pour édicter les normes mais pas pour les exécuter.

Il faut cependant rappeler que les avocats sont soumis au secret professionnel, qu'ils ne vont pas aller raconter individuellement quels sont les montages qu'ils ont réalisés et qui seraient révélés dans le cadre des informations que l'on découvre. Cela vaut si leur activité est frauduleuse ou non, puisqu'il leur est interdit de dire ce qu'ils font, qui sont leurs clients et pourquoi ils le font. Si l'avocat ne répond pas, ce n'est pas parce qu'il n'a pas envie de répondre et qu'il est coupable de je ne sais quoi, c'est parce qu'il ne peut pas le faire pour des raisons structurelles liées au secret professionnel.

La rédaction : Un seul cabinet d'avocats, Mossack Fonseca, a centralisé un très grand nombre de montages frauduleux. Cela vous choque-t-il ?

Pascal Eydoux : Ce qui me choque, c'est que ce cabinet – et sans doute bien d'autres – créent intentionnellement des structures de blanchiment de capitaux frauduleux, que cela vienne de la fraude fiscale ou de la grande criminalité. C'est la raison pour laquelle il est normal qu'il y ait des enquêtes, il est normal que les avocats qui sont les complices de l'évasion fiscale, de l'utilisation frauduleuse de capitaux criminels fassent l'objet d'enquêtes et de poursuites, si leur participation active est avérée.

La rédaction : Si certains avocats peuvent participer à la fraude, à qui incombe la plus grande part de responsabilité dans ce système de fraude généralisée ?

Pascal Eydoux : Les pouvoirs publics ont une grande responsabilité dans ce qu'il se produit, et il faut quand même qu'ils l'assument. Nous sommes en présence de la démonstration d'une totale incapacité des pouvoirs publics, quels qu'ils soient, d'harmoniser les règles fiscales et économiques, que ce soit au sein de l'Union européenne ou ailleurs.

Étant incapables d'adopter des législations cohérentes et uniques, ils donnent la faculté à tous les intervenants économiques, honnêtes ou non, de créer un certain nombre de structures dans des conditions qui sont ou ne sont pas répréhensibles.

La rédaction : Craignez-vous également que la confusion entre optimisation et évasion fiscale nourrisse une opinion publique négative à l'égard des avocats ?

Pascal Eydoux : Oui, je redoute qu'il y ait un amalgame absolument total et terrifiant, entre l'optimisation et la fraude. Il y a des règles fiscales dont certaines permettent aux acteurs économiques de payer moins d'impôts dans un pays plutôt que dans un autre. Lorsque l'acteur économique demande à l'avocat de trouver un système pour payer le moins d'impôts possible, parce qu'économiquement c'est ce qu'il recherche, ce n'est pas

frauduleux de se servir d'un arsenal législatif qui existe, qui a été promulgué et qui permet de donner satisfaction au client.

Mais les pouvoirs publics cherchent systématiquement des boucs émissaires lorsqu'ils ne sont pas capables de faire leur travail. Lorsqu'on découvre ce genre de choses, je les sens tout enclin à dire que c'est parce qu'il y a des avocats qui favorisent l'optimisation et l'évasion fiscales. Mais l'optimisation fiscale n'est pas un délit. Et c'est au ministre du budget de reconnaître sa responsabilité, lorsqu'il n'est pas capable de trouver des textes législatifs qui empêchent une optimisation jugée excessive et immorale par l'opinion publique.

Par ailleurs, la réaction « surprise » des responsables politiques me paraît hypocrite, cynique *a minima*. On parle de paradis fiscaux dans le Pacifique, mais il y a tout ce qu'il faut près de chez nous, pas besoin d'aller accuser les Bahamas. Il faut que chacun se remette en question.

La rédaction : Que penser de la divulgation massive d'informations couvertes par le secret professionnel ?

Pascal Eydoux : On vit dans une société qui ne comprend plus la différence entre la transparence, le secret professionnel, la loyauté, l'honnêteté... Il faut que les sociétés se remettent en situation de confiance, et que si plus aucun acteur n'est capable d'être le réceptacle d'une confiance d'un client, les individus seront en danger, parce que le secret professionnel n'est pas un privilège de l'avocat, c'est une obligation au service de son client. Au nom d'une volonté frénétique de transparence, on ne respecte plus les règles fondamentales de la liberté de chacun, on jette en pâture un certain nombre d'individus avant la conclusion des enquêtes. Le fait de confier à l'opinion publique des éléments dont on ne sait pas tous s'ils sont frauduleux, c'est effrayant. Ça nous met en danger, nous avocats, et la structure même de la société.

La rédaction : Ne pensez-vous pas que si ces données ont été transmises aux médias plutôt qu'aux États, c'est que la source a jugé que cela serait plus efficace, que ces données seraient utilement exploitées ?

Pascal Eydoux : C'est probablement une intention délibérée, et c'est la responsabilité des autorités, pas des avocats ni des délinquants. Les pays n'arrivent pas à se mettre d'accord sur la création d'un procureur européen. S'ils sont capables de se mettre d'accord sur un certain nombre de structurations de leurs poursuites, ils n'auront plus besoin de ce genre de divulgations erratiques, anarchiques, qui créent des amalgames. Là aussi je pense vraiment que les États sont responsables.

Propos recueillis par Julien Mucchielli, journaliste.



Le droit d'alerte : signaler, traiter, protéger

Une étude du Conseil d'État



Une étude	p 2
Diffuser une culture de l'alerte	p 3
Un cadre juridique aujourd'hui inadapté	p 4
Mettre en place des procédures efficaces de signalement et de traitement de l'alerte	p 5
Renforcer la protection des lanceurs d'alerte	p 7
Sanctionner les abus	p 8
Synthèse des 15 propositions	p 9

Une étude

Pratique ancienne, **l'alerte éthique est aujourd'hui confrontée à des enjeux inédits**. Destinée à prévenir les dysfonctionnements des organisations publiques et privées, ses canaux d'expression se sont diversifiés, mondialisés et, dans une certaine mesure, dérégulés, avec le développement d'internet et l'explosion du numérique.

Si l'article 40 du code de procédure pénale oblige depuis 1957 les agents publics à signaler au Parquet les infractions pénales dont ils ont connaissance dans l'exercice de leurs fonctions, **la mise en place de dispositifs d'alerte en France est récente**. Elle s'est d'abord développée dans les entreprises, sans intervention du législateur. Du fait d'évolutions des règles internationales et après plusieurs affaires retentissantes, **le législateur français a toutefois, depuis 2007, adopté plusieurs dispositions importantes dont l'objet est de protéger les personnes émettant, de bonne foi, des alertes**.

Par une lettre du 17 juillet 2015, le Premier ministre a confié au Conseil d'État la réalisation d'une étude, lui demandant de dresser un bilan critique de ces dispositions et de faire des propositions pour en améliorer l'efficacité. Un groupe de travail a été mis en place. Il a rassemblé des membres du Conseil d'État, des représentants des ministères les plus concernés, des membres d'associations et de l'Université. Il a procédé à de nombreuses auditions, notamment des organisations représentatives des salariés et des employeurs. L'étude a enfin été adoptée par l'assemblée générale plénière du Conseil d'État en février 2016.

Au terme de ces travaux, **le constat qui s'impose est que les dispositifs existants sont peu utilisés. Cela tient sans doute au fait qu'ils ne forment pas un ensemble cohérent et ne sont pas suffisamment précis quant à la définition du lanceur d'alerte et aux procédures à mettre en œuvre pour recueillir et traiter les alertes. Ces dispositifs ne garantissent pas toujours aux lanceurs d'alerte une protection efficace** et ne permettent pas une conciliation satisfaisante entre les droits que ces dispositions instituent et d'autres droits ou obligations (secrets protégés pénalement, droits des personnes visées par des alertes abusives).

Le Conseil d'État fait quinze propositions pour améliorer et faciliter l'accès à ces dispositifs, tant dans les administrations que dans les entreprises. Il préconise l'adoption d'un socle de dispositions communes applicables à toute personne qui, confrontée à des faits constitutifs de manquement grave à la loi ou porteurs de risques graves, décide librement et en conscience de lancer une alerte dans l'intérêt général. S'inspirant de la jurisprudence de la Cour européenne des droits de l'homme et de législations étrangères, ce socle commun repose sur des procédures graduées, sécurisées et largement accessibles. Le Conseil d'État recommande d'assurer un traitement effectif de chaque alerte et de protéger plus efficacement les lanceurs d'alerte comme les personnes qui seraient la cible d'alertes abusives ou malveillantes.

Diffuser une culture de l'alerte

Qu'est-ce qu'un lanceur d'alerte ?

Le lanceur d'alerte est une personne qui, confrontée à des faits constitutifs de manquements graves à la loi ou porteurs de risques graves, décide librement et en conscience de lancer une alerte dans l'intérêt général.

Cette définition exclut les personnes qui émettent sciemment des signalements inexacts ou qui agissent dans l'intention de nuire. Elle exclut également les personnes dont le métier consiste à mener des enquêtes ou exercer des contrôles sur de tels faits : le lanceur d'alerte n'est pas un professionnel de l'alerte.

Le lanceur d'alerte contribue à l'intérêt général. C'est pourquoi l'étude du Conseil d'État est fondée sur la conviction qu'il convient de diffuser aussi largement que possible une culture de l'alerte.

Quel est le champ de l'étude ?

L'étude du Conseil d'État concerne les lanceurs d'alerte dans le secteur privé et dans le secteur public. Elle traite de l'alerte dans l'ensemble des champs susceptibles d'être concernés, qu'il s'agisse de la corruption, de la fraude fiscale, des conflits d'intérêts ou encore des risques pour l'environnement ou la santé publique.

Un cadre juridique aujourd'hui inadapté

Quel est le cadre juridique actuel ?

La France dispose depuis longtemps de divers mécanismes de signalement, dont celui des crimes et délits dont les agents publics ont connaissance dans l'exercice de leurs fonctions (article 40 du code de procédure pénale). Un premier droit d'alerte s'est, par ailleurs, développé depuis 1982 dans les entreprises et les administrations en matière de santé et de sécurité au travail. La diffusion de dispositifs d'alerte professionnelle est en revanche récente : elle a surtout concerné les grandes entreprises, sans intervention du législateur français.

Depuis 2007, le législateur a adopté de nombreuses lois concernant la protection des lanceurs d'alerte, dans différents secteurs : c'est le cas en matière de corruption, de prévention des risques graves pour la santé publique et l'environnement, de conflits d'intérêts, de fraude fiscale ou encore en matière de renseignement.

En quoi ce cadre est-il inadapté ?

L'étude du Conseil d'État démontre que ces dispositions législatives ne forment pas aujourd'hui un ensemble cohérent et sont insuffisamment précises quant aux procédures à mettre en œuvre dans les entreprises et dans les administrations pour recueillir et traiter l'alerte d'une part, pour protéger les lanceurs d'alerte d'autre part.

Elle montre aussi le retard des administrations face aux grandes entreprises, qui se sont presque toutes dotées de systèmes d'alerte professionnelle pour respecter des lois étrangères.

Mettre en place des procédures efficaces de signalement et de traitement de l'alerte

A qui un lanceur d'alerte doit-il s'adresser ?

Les dispositions récentes consacrées à la protection des lanceurs d'alerte ne fournissent pas de mode d'emploi clair quant aux canaux susceptibles d'être utilisés par une personne qui voudrait lancer une alerte.

L'étude du Conseil d'État recommande à un lanceur d'alerte de s'adresser en priorité au responsable désigné à cet effet au sein de l'organisation concernée. En l'absence de réponse dans un délai raisonnable ou, bien sûr, si cette saisine est dès l'origine impossible, le lanceur d'alerte doit s'adresser aux autorités administratives compétentes (inspections, services préfectoraux...) ou à l'autorité judiciaire. Si aucune suite n'est donnée à ses démarches, le lanceur d'alerte peut divulguer au public les faits qu'il veut signaler ; il peut le faire directement s'il y a une urgence avérée.

Cette démarche graduée correspond à l'approche retenue par la Cour européenne des droits de l'homme¹ (CEDH) et par le Conseil de l'Europe. Elle s'inspire aussi des législations britannique et irlandaise en matière de protection des lanceurs d'alerte.

Fondamentalement, cette approche répond à la volonté de favoriser le traitement de l'alerte : l'objectif est en premier lieu de permettre aux organisations mises en cause de se réformer elles-mêmes, puis de mettre en mesure les autorités administratives et judiciaires de faire cesser les manquements graves à la loi et de prévenir les risques graves qui seraient révélés.

Quelle procédure revient-il aux entreprises et aux administrations de mettre en œuvre pour recueillir l'alerte ?

Afin de rendre possible la saisine interne, **l'étude du Conseil d'État propose d'exiger des administrations la désignation en leur sein de personnes chargées de recueillir en interne les alertes. Elle propose d'encourager la diffusion de tels dispositifs dans les entreprises**, en retenant une approche différenciée selon la taille de celles-ci. S'agissant des très petites, petites et moyennes entreprises, l'enjeu consiste à identifier des interlocuteurs de proximité susceptibles d'être saisis en interne.

L'étude du Conseil d'État préconise d'instaurer par la loi le principe selon lequel les dispositifs de recueil de l'alerte garantissent la stricte confidentialité de l'identité de l'auteur de l'alerte. Ce principe de confidentialité s'appliquerait aussi aux personnes visées par le signalement aussi longtemps que sa véracité n'a pas été confirmée.

¹ Cour européenne des droits de l'homme, Grande chambre, 12 février 2008, *Guja c. Moldova*, n° 14277/04.

Que faire si l'on ne sait pas à quelle autorité administrative s'adresser ?

Pour les lanceurs d'alerte qui, une fois la saisine interne épuisée, ne sauraient pas à quelle autorité administrative s'adresser, **le Conseil d'État propose la création d'un portail unique de l'alerte**. Ce portail numérique aurait pour fonction de rediriger vers les autorités compétentes les alertes émises. Sa mise en place pourrait être confiée à la Commission nationale de la déontologie et des alertes en matière de santé publique et d'environnement, instituée par la loi n° 2013-316 du 16 avril 2013, en élargissant sa compétence au-delà du seul champ sanitaire et environnemental.

Concrètement, un lanceur d'alerte pourra voir son alerte redirigée, grâce à ce portail, vers la Haute autorité pour la transparence de la vie publique en matière de conflits d'intérêts, vers le Service central de prévention de la corruption en matière de corruption, ou encore vers l'Agence nationale de sécurité du médicament et des produits de santé en matière de risques causés par un médicament. L'effectivité du recueil de l'alerte est ainsi assurée.

Comment s'assurer que l'alerte est traitée ?

Afin de favoriser un traitement effectif des alertes par ceux qui en sont destinataires, le Conseil d'État propose d'obliger, dans le secteur public, et d'inciter, dans le secteur privé, à informer le lanceur des suites données à son alerte. En l'absence d'une telle information de la part des autorités saisies, le droit d'alerte se vide en effet de sa substance.

Surtout, l'étude du Conseil d'État souligne qu'il est dans l'intérêt des organisations mises en cause de traiter les alertes dont elles sont saisies lorsque ces alertes sont fondées : ne pas donner suite à une alerte révélant des faits de corruption dans une entreprise l'expose, ainsi que ses dirigeants, à des poursuites pénales pour les faits en cause.

Renforcer la protection des lanceurs d'alerte

Le juge est-il le seul recours pour un lanceur d'alerte victime de mesures de représailles ?

Les lois actuelles font du juge le seul recours pour un lanceur d'alerte victime de mesures de représailles ; or celui-ci intervient souvent trop tard. Son action se borne le plus souvent à réparer les dommages déjà subis par le lanceur d'alerte.

Le Conseil d'État préconise d'instituer des mécanismes préventifs de tels contentieux. C'est pourquoi **l'étude du Conseil d'État propose d'étendre la compétence du Défenseur des droits à la protection, dès le lancement de l'alerte, des lanceurs d'alerte s'estimant victimes de mesures de représailles.**

Quelles sont les mesures de représailles contre lesquelles un lanceur d'alerte est protégé ?

Les mesures de représailles dont un lanceur d'alerte peut faire l'objet sont très variées : licenciement, discriminations, diminution de salaire, mutation, non renouvellement de contrat etc...

C'est pourquoi **l'étude du Conseil d'État propose d'inscrire dans la loi le principe selon lequel toute mesure de représailles, quelle qu'elle soit, est nulle dès lors qu'il apparaît devant le juge qu'elle a été motivée par l'alerte.**

Ce faisant, l'étude du Conseil d'État propose d'harmoniser les différentes lois en vigueur autour de ce principe qui permettra au juge de protéger, au cas par cas, les droits du lanceur d'alerte.

Les pouvoirs dont dispose le juge sont-ils suffisants ?

En matière de protection des lanceurs d'alerte, l'étude du Conseil d'État propose d'étendre et de préciser les pouvoirs du juge sur deux points :

- **pour les agents publics, il est proposé de permettre au juge d'imposer à une administration de réintégrer un agent qui aurait été démis de ses fonctions à raison d'une alerte émise de bonne foi.** Une telle mesure pourrait ainsi s'appliquer aux cas de licenciement, de non-renouvellement de contrat ou de révocation ;
- **pour les lanceurs d'alerte faisant l'objet de procédures en diffamation abusives, il est proposé d'inciter les parquets à requérir des sanctions civiles contre les auteurs de telles procédures.**

Un lanceur d'alerte ne s'expose-t-il pas à des poursuites pour violation du secret professionnel ?

Dans le cadre juridique actuel, un lanceur d'alerte peut être poursuivi pénalement pour violation d'un secret protégé (secret médical, secret de la défense nationale, secret professionnel, etc...), faute de texte levant ce secret en cas de lancement d'une alerte.

L'étude du Conseil d'État rappelle qu'une disposition législative est nécessaire pour qu'un lanceur d'alerte puisse lever l'un des secrets pénalement protégés et que cette dérogation doit être prévue secret par secret, après des arbitrages délicats qui sont de la responsabilité du législateur. S'agissant des secrets les plus importants (secret professionnel et en particulier, secret médical ou secret de la défense nationale, etc), d'autres systèmes peuvent être également envisagés, comme l'alerte faite auprès d'une personne habilitée au secret défense.

Sanctionner les abus

Comment faire face aux alertes abusives ou malveillantes ?

Le droit actuel fournit des outils suffisants. **L'auteur d'alertes abusives ou malveillantes s'expose déjà à des sanctions disciplinaires, voire à des sanctions pénales (pour dénonciation calomnieuse par exemple) ou civiles (en cas de diffamation).**

Comment protéger les personnes injustement mises en cause ?

Au-delà des sanctions décrites ci-dessus, **l'étude du Conseil d'État préconise que soit garantie une stricte confidentialité des informations relatives aux personnes mises en cause jusqu'à ce que le bien-fondé d'une alerte soit établi.** Cette confidentialité apparaît en effet comme la meilleure manière d'éviter les drames résultant d'une mise en cause infondée.

Harmoniser les dispositions existantes par l'adoption d'un socle commun

Comment mettre en œuvre l'ensemble de ces recommandations ?

Afin d'harmoniser les lois existantes et à venir, **le Conseil d'État préconise l'adoption d'un socle de dispositions communes qui traduirait l'ensemble des propositions émises par l'étude**

Synthèse des 15 propositions

Proposition 1

Outre la définition du lanceur d'alerte, ce socle commun préciserait :

- les procédures graduées et sécurisées mises à la disposition des lanceurs d'alerte pour émettre un signalement ;
- les modalités de traitement qu'il reviendrait aux destinataires de l'alerte de mettre en œuvre ;
- la protection dont disposeraient les lanceurs d'alerte de bonne foi contre toute mesure de représailles.

Vecteur : loi.

Proposition 2

Instituer, en s'inspirant de la jurisprudence de la Cour européenne des droits de l'homme et des législations en vigueur au Royaume-Uni et en Irlande, une gradation des canaux susceptibles d'être saisis par les lanceurs d'alerte appartenant à l'organisation mise en cause : canal hiérarchique, canal interne spécifique (déontologie, dispositif d'alerte professionnelle, inspection générale), canaux externes (autorité administrative compétente, ordres professionnels, autorité judiciaire). La divulgation au public ne saurait être envisagée qu'en dernier recours.

Le respect de cette gradation par un lanceur d'alerte appartenant à l'organisation mise en cause serait l'un des critères pris en compte par le juge afin de déterminer le degré de protection à lui accorder.

Vecteur : loi (socle commun).

Proposition 3

Rendre les dispositifs d'alerte mis en place dans les entreprises et les administrations accessibles aux collaborateurs extérieurs et occasionnels exerçant leurs fonctions au sein ou pour le compte de ces organisations.

Vecteur : actes réglementaires s'agissant des administrations de l'Etat et des établissements de santé, loi s'agissant des collectivités territoriales et des entreprises.

Proposition 4

Rendre les dispositifs d'alerte mis en place dans les entreprises et les administrations accessibles, selon des modalités adaptées, aux personnes physiques et morales extérieures, sans que ce recours ne soit obligatoire.

Vecteur : loi et actions de communication.

Proposition 5

Instaurer et garantir la stricte confidentialité de l'identité des auteurs de l'alerte ainsi que, avant que le bien-fondé de l'alerte soit confirmé, des personnes qu'elle vise et des informations recueillies par l'ensemble des destinataires, internes et externes, de l'alerte.

Vecteur : loi (socle commun).

Proposition 6

I. Instituer l'obligation de désigner des personnes chargées de recueillir l'alerte interne et, le cas échéant, externe, dans l'ensemble des administrations de l'Etat, des établissements de santé et des grandes collectivités territoriales. Ces destinataires de l'alerte pourraient, selon les cas, être une inspection générale, un comité d'éthique ou de déontologie ou un référent déontologue. Ils devront, en tout état de cause, disposer d'une autonomie suffisante et être placés à un niveau élevé de la hiérarchie.

Vecteur : actes réglementaires s'agissant des administrations de l'Etat et des établissements de santé, loi s'agissant des collectivités territoriales.

II. Encourager la diffusion de dispositifs d'alerte internes spécifiques dans les entreprises en retenant une approche différenciée consistant :

- dans les grandes entreprises, à consolider, en les adossant aux structures existantes, par exemple les directions de la conformité ou les déontologues, et à faire connaître les dispositifs d'ores et déjà mis en place ;

- dans les petites et moyennes entreprises, à sensibiliser les interlocuteurs habituels de l'alerte que sont les responsables hiérarchiques et les institutions représentatives du personnel, lorsqu'elles existent.

Vecteur : droit souple (guides de bonnes pratiques).

Proposition 7

Conserver à l'alerte son caractère de faculté et non d'obligation, à la différence de ce qui est d'ores et déjà prévu par la loi pour des dispositifs de signalement spécifiques (article 40 du code de procédure pénale pour le signalement des crimes et délits, droit d'alerte et de retrait en matière de santé et de sécurité au travail, article 434-1 du code pénal s'agissant de l'information des autorités judiciaires ou administratives d'un crime dont une personne a connaissance et dont il est encore possible de prévenir ou de limiter les effets ; article 434-3 du code pénal s'agissant de la maltraitance d'enfants ou de personnes vulnérables ; articles 223-6 et 223-7 du code pénal s'agissant de l'omission de porter secours.)

Vecteur : loi (socle commun).

Proposition 8

Préciser les modalités de la conciliation à opérer entre les dispositions relatives au droit d'alerte et chacun des secrets pénalement protégés, en déterminant les conditions dans lesquelles il est possible d'y déroger pour lancer une alerte.

Vecteur : lois sectorielles.

Proposition 9

Mettre en place un portail chargé, le cas échéant, de transmettre aux autorités compétentes les alertes émises par des personnes ne sachant pas à quelles autorités s'adresser, en élargissant la compétence de la Commission nationale de la déontologie et des alertes instituée par la loi du 16 avril 2013 au-delà du seul champ sanitaire et environnemental, plutôt qu'en créant une autorité unique en charge du traitement de l'alerte.

Vecteur : loi (socle commun).

Proposition 10

I. Instituer, dans les administrations de l'Etat, les établissements de santé et les grandes collectivités territoriales, l'obligation pour le responsable saisi d'accuser réception de l'alerte, puis de tenir informé le lanceur d'alerte des suites données à sa démarche.

Vecteur : actes réglementaires s'agissant des administrations de l'Etat et des établissements de santé, loi s'agissant des collectivités territoriales.

II. Promouvoir, dans les entreprises, la bonne pratique consistant, pour le responsable saisi, à accuser réception de l'alerte, puis à tenir informé le lanceur d'alerte des suites données à sa démarche.

Vecteur : droit souple (guides de bonnes pratiques).

Proposition 11

Prevoir des modalités appropriées pour l'information de la personne mise en cause par une alerte et définir les cas dans lesquels cette information n'est pas souhaitable, en particulier pour éviter la destruction de preuves.

Vecteur : droit souple (instructions pour les administrations, guides de bonnes pratiques pour les entreprises)

Proposition 12

I. Affirmer dans la loi le principe selon lequel toute mesure de représailles prise par l'employeur à l'encontre d'un lanceur d'alerte de bonne foi est frappée de nullité ; dresser une liste indicative la plus complète possible de ces mesures et renvoyer au juge le soin d'apprécier, dans chaque cas d'espèce, si les mesures illégales entrent dans ces prévisions.

Vecteur : loi (socle commun).

II. Harmoniser les dispositions législatives sectorielles relatives à la protection des lanceurs d'alerte en conséquence de ce principe.

Vecteur : lois sectorielles.

Proposition 13

Compléter le pouvoir d'injonction du juge administratif en prévoyant explicitement, dans les dispositions législatives applicables au secteur public, qu'il pourra enjoindre à l'administration de réintégrer effectivement l'agent public dont le licenciement, le non-renouvellement de contrat ou la révocation a été regardé comme une mesure de représailles prise à raison d'une alerte.

Vecteur : loi (socle commun).

Proposition 14

Inciter les parquets à faire usage de la possibilité de requérir le prononcé de sanctions civiles à l'encontre d'une personne intentant contre un lanceur d'alerte de bonne foi des procédures en diffamation déclarées abusives par le juge, tout en restant attentifs aux alertes revêtant un caractère diffamatoire.

Vecteur : instruction au parquet.

Proposition 15

Étendre les compétences du Défenseur des droits à la protection, dès le lancement de l'alerte, des lanceurs d'alerte s'estimant victimes de mesures de représailles.

Vecteur : loi organique.

Document 52013PC0813

About this document Text Procedure Linked documents All

Collapse all | Expand all

Title and reference

Proposition de DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites

/* COM/2013/0813 final - 2013/0402 (COD) */

Languages and formats available

	BG	ES	CS	DA	DE	ET	EL	EN	FR	GA	HR	IT	LV	LT	HU	MT	NL	PL	PT	RO	SK	SL	FI	SV
HTML																								
DOC																								
PDF																								

Multilingual display

Language 1 English (en) Language 2 Please choose Language 3 Please choose

Text

52013PC0813

Proposition de DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites /* COM/2013/0813 final - 2013/0402 (COD) */

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION.

L'Europe dispose de tous les atouts nécessaires pour devenir un leader mondial sur le plan de la science et de l'innovation. La qualité scientifique est non seulement l'objectif des chercheurs, mais aussi une source de gains importants tant pour le secteur public que pour le secteur privé. Néanmoins, l'apport des entreprises à la recherche et développement (R&D) est insuffisant si l'on compare la situation de l'Union européenne à celle de ses grands partenaires commerciaux, notamment les États-Unis et le Japon. Or, des investissements sous-optimaux des entreprises dans la R&D ont une incidence négative sur le lancement de nouveaux produits, procédés, services et savoir-faire.

Il est donc souhaitable d'améliorer les conditions dans lesquelles se déroulent les activités innovantes des entreprises. Dans le cadre plus large de sa stratégie Europe 2020, la Commission s'est engagée à créer une Union de l'innovation afin de protéger les investissements dans la base de connaissances, de réduire la fragmentation coûteuse et de faire de l'Europe un terre d'accueil plus intéressante pour l'innovation. Un environnement favorable à l'innovation devrait en particulier encourager la hausse des investissements du secteur privé dans la R&D, par des collaborations plus étendues en matière de recherche et de développement technologique entre les universités et les entreprises, notamment de pays différents, l'innovation ouverte et de meilleures possibilités de valorisation de la propriété intellectuelle (PI), afin de donner aux entités économiques spécialisées dans la recherche et l'innovation un meilleur accès au capital-risque et au financement. Cependant, réaliser ces objectifs exclusivement au niveau national ne serait pas suffisant et entraînerait, à l'échelle de l'Union, des efforts redondants.

Dans l'économie numérique, les coûts de transaction très fortement réduits ont favorisé l'apparition de nouvelles formes de coopération, fondées sur la science ouverte et l'innovation ouverte, qui débouchent souvent sur de nouveaux modèles économiques visant à utiliser les connaissances ainsi créées. Les droits de propriété intellectuelle (DPI) constituent néanmoins une part essentielle d'une politique d'innovation. Les DPI donnent aux innovateurs et aux créateurs les moyens de s'approprier les résultats de leurs travaux, immatériels par nature, ce qui représente l'incitation nécessaire pour des investissements dans de nouveaux savoir-faire, solutions et inventions. Les DPI tendent à protéger les résultats d'efforts créatifs ou inventifs, mais leur couverture est limitée.

En effet, durant le processus de recherche et de création, une grande quantité d'informations sont compilées et développées. Des connaissances d'une valeur économique importante sont ainsi progressivement élaborées; elles ne peuvent souvent pas faire l'objet d'une protection par les DPI, mais elles sont tout aussi importantes pour l'innovation et pour la compétitivité des entreprises en général. Lorsque ces informations doivent rester secrètes, notamment en vue d'attirer des investisseurs et des financements, les entreprises, les laboratoires, les universités ainsi que les inventeurs et créateurs individuels utilisent l'outil le plus courant et le plus ancien qui existe à cette fin: la confidentialité.

Puisque la recherche s'appuie sur les travaux antérieurs, la transmission des connaissances et des nouvelles découvertes joue un rôle important pour l'innovation. Dans certains cas, en fonction du modèle économique de l'innovateur, la confidentialité peut être nécessaire pour permettre à la propriété intellectuelle de fructifier et de déboucher sur des innovations et une compétitivité accrue. Tout DPI commence par un secret: un écrivain ne dévoile pas l'intrigue sur laquelle il travaille (futur objet du droit d'auteur), un constructeur automobile ne diffuse pas les premiers croquis d'un nouveau modèle de véhicule (futur dessin ou modèle), une entreprise ne révèle pas les premiers résultats de ses expériences technologiques (objet d'un futur brevet) ou les informations relatives au lancement d'un nouveau produit de marque (future marque de commerce), etc.

En terminologie juridique, des informations qui sont gardées confidentielles afin de préserver un avantage compétitif

sont appelées «secrets d'affaires», «renseignements non divulgués» ou «informations commerciales confidentielles». Les entreprises et les universitaires utilisent parfois d'autres dénominations, comme «savoir-faire exclusif» ou «technologie propriétaire».

Les secrets d'affaires sont tout aussi importants pour la protection des innovations non technologiques. Le dynamisme du secteur des services, lequel représente environ 70 % du PIB de l'UE, repose sur la création de connaissances innovantes. Cependant, ce secteur ne recourt pas autant que l'industrie manufacturière aux procédés technologiques et à l'innovation de produit (protégés par des brevets). La confidentialité, dans ce secteur essentiel de l'économie de l'UE, est utilisée dans le contexte de l'innovation «douce», qui couvre l'utilisation de diverses informations commerciales stratégiques qui vont au-delà des connaissances technologiques, par exemple les informations relatives aux clients et aux fournisseurs, les processus d'entreprise, les plans d'affaires, les études de marché, etc.

D'après les économistes, les entreprises, indépendamment de leur taille, accordent au moins autant de valeur aux secrets d'affaires qu'à n'importe quelle autre forme de PI. Ces secrets sont particulièrement importants pour les petites et moyennes entreprises (PME) et les start-ups, qui n'ont souvent pas les ressources humaines spécialisées ni l'assise financière nécessaires pour faire enregistrer leurs DPI, les gérer, les faire respecter et les protéger.

Bien qu'ils ne soient pas protégés comme des DPI classiques, les secrets d'affaires constituent un instrument complémentaire essentiel à la nécessaire appropriation des actifs intellectuels qui constituent les moteurs de l'économie de la connaissance du XXI^e siècle. Le détenteur d'un secret d'affaires ne détient pas de droits exclusifs sur les informations couvertes par ce secret. Cependant, afin de promouvoir l'efficacité économique et la compétitivité, il est justifié d'imposer des restrictions à l'utilisation d'un secret d'affaires lorsque les savoir-faire ou les informations en question ont été obtenus de manière malhonnête et contre la volonté de leur détenteur. L'appréciation au cas par cas du caractère nécessaire et proportionné de ces restrictions relève des tribunaux.

Ainsi, le développement de solutions identiques, similaires ou de remplacement par des entreprises concurrentes doit être permis et même encouragé afin que l'innovation fasse l'objet d'une saine concurrence. Mais tricher, voler ou tromper pour obtenir des informations confidentielles élaborées par d'autres doit être interdit.

Tandis que le développement et la gestion de la connaissance et de l'information sont toujours plus essentiels au bon fonctionnement de l'économie de l'UE, l'exposition des renseignements et des savoir-faire de valeur non divulgués (secrets d'affaires) au vol, à l'espionnage et à d'autres techniques d'appropriation illicite ne fait qu'augmenter (mondialisation, sous-traitance, allongement des chaînes d'approvisionnement, usage accru des TIC, etc.). Il existe également un risque croissant que des secrets d'affaires volés soient utilisés dans des pays tiers pour produire des produits en infraction qui entreront ensuite en concurrence sur le territoire de l'UE avec ceux de la victime de l'appropriation illicite. Cependant, l'hétérogénéité et la fragmentation actuelles du cadre juridique en matière de protection des secrets d'affaires contre l'obtention, l'utilisation ou la divulgation illicites entrave la R&D transfrontière et la circulation des connaissances innovantes en affaiblissant la capacité des entreprises européennes de réagir aux attaques malhonnêtes à l'encontre de leur savoir-faire.

L'amélioration de l'infrastructure en matière de PI constitue un pilier important de l'Union de l'innovation; dans ce contexte, la Commission a adopté une stratégie globale pour la PI en mai 2011 et a engagé un examen de la protection des secrets d'affaires[1]. La présente proposition est une concrétisation supplémentaire de son engagement à créer un marché unique de la propriété intellectuelle.

2. RÉSULTATS DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

2.1. Consultation publique

La présente initiative est fondée sur une évaluation de l'importance des secrets d'affaires pour l'innovation et pour la compétitivité des entreprises, de la mesure dans laquelle ces secrets sont utilisés, de leur rôle, et de leur rapport avec les DPI, dans le contexte de l'élaboration de connaissances et d'actifs immatériels et de leur exploitation économique; et du cadre juridique pertinent. Cette évaluation a été réalisée au moyen de deux études externes et de vastes consultations des parties intéressées.

Une première étude (publiée en janvier 2012) présente une évaluation comparative des législations en matière de protection contre l'appropriation illicite des secrets d'affaires dans les différents États membres de l'UE. Une deuxième étude, publiée en mai 2013, a porté sur une évaluation des fondements économiques des secrets d'affaires et de la protection contre leur appropriation illicite, ainsi que sur une analyse plus approfondie de la protection juridique des secrets d'affaires dans toute l'UE. Elle a confirmé que dans l'Union, la protection des secrets d'affaires contre leur appropriation illicite était fragmentée et hétérogène, et que d'une manière générale, elle était opaque et porteuse de coûts et risques inutiles. Selon cette étude, un système permettant de sauvegarder les résultats de la R&D de façon efficiente est une condition préalable à l'innovation dans le secteur privé, une protection fiable du secret d'affaires donnant aux entreprises la liberté nécessaire pour innover dans l'environnement économique actuel. Sa conclusion est que l'harmonisation de la législation en matière de secrets d'affaires dans l'UE améliorerait les conditions d'élaboration, d'échange et d'utilisation des connaissances innovantes par les entreprises.

Les opinions des parties intéressées ont été collectées en 3 étapes. Premièrement, la société civile, les entreprises, les chercheurs et les pouvoirs publics ont discuté du sujet lors d'une conférence organisée par la Commission en juin 2012.

Deuxièmement, une enquête sur l'utilisation des secrets d'affaires, les risques qui y sont liés et leur protection juridique a été lancée en novembre 2012, dans le contexte de la 2^e étude. Cette enquête visait un échantillon représentatif d'entreprises de toute l'UE, dont 60 % de PME. Au total, 537 réponses à l'enquête ont été reçues. 75 % des répondants ont estimé que les secrets d'affaires revêtaient une importance stratégique pour la croissance, la compétitivité et la capacité d'innovation de leur entreprise. L'enquête a révélé que dans l'UE, au cours des dix dernières années, environ un répondant sur cinq a subi au moins une tentative d'appropriation illicite, et que le risque d'une telle appropriation des secrets d'affaires avait augmenté selon près de deux répondants sur cinq. Deux répondants sur trois se sont déclarés favorables à une proposition législative de l'UE.

Troisièmement, du 11 décembre 2012 au 8 mars 2013, les services de la Commission ont mené une consultation publique ouverte consacrée aux options politiques existantes et à leurs incidences. Le nombre de réponses reçues s'est élevé à 386, provenant en majorité de particuliers (principalement d'un État membre) et d'entreprises. Parmi les répondants, 202 ont estimé que la protection juridique contre l'appropriation illicite des secrets d'affaires devrait faire l'objet d'une action de l'UE. Cependant, un clivage était visible entre les réponses des deux principaux groupes de répondants (particuliers d'une part, entreprises de l'autre). Trois particuliers sur quatre considéraient que les secrets d'affaires avaient peu d'importance pour la R&D et jugeaient excessive la protection juridique existante de ces secrets; 75 % estimaient qu'une action de l'UE n'était pas nécessaire. En revanche, les entreprises ayant répondu à l'enquête considéraient les secrets d'affaires comme très importants pour la R&D et pour leur compétitivité. Une forte majorité jugeait faible la protection existante, en particulier sur le plan transfrontière, et estimaient que les différences entre cadres juridiques nationaux avaient des incidences négatives, par exemple un risque commercial plus élevé dans les États membres où la protection est la plus faible, une moindre incitation à engager des activités de R&D dans d'autres pays, ou des dépenses accrues en mesures préventives de protection des informations.

2.2. Analyse d'impact

L'analyse d'impact a montré les divergences nationales existant en matière de protection des secrets d'affaires: peu d'États membres ont des lois qui définissent ce qu'est un secret d'affaires ou précisent quand ce dernier doit être protégé; il n'est pas toujours possible d'ordonner au contrevenant de mettre fin à l'infraction; les règles traditionnelles de calcul des dommages-intérêts sont souvent inadaptées dans les cas d'appropriation illicite d'un secret d'affaires, en l'absence, notamment, de méthodes de substitution (par exemple, calcul du montant qui aurait été dû dans le cadre d'un accord de licence); les règles pénales ne visent pas le vol de secret d'affaires dans tous les États membres. En outre, de nombreux États ne disposent pas de règles visant à préserver les secrets d'affaires durant les procédures judiciaires, ce qui décourage les victimes d'appropriation illicite d'un secret de demander réparation en justice.

Deux problèmes principaux en sont ressortis:

- des incitations sous-optimales pour les activités d'innovation transfrontières. Lorsqu'il existe un risque d'appropriation illicite des secrets d'affaires lié à une protection légale inefficace, les incitations à entreprendre des activités d'innovation (y compris à l'échelle transfrontière) sont réduites, parce que i) la valeur attendue de l'innovation fondée sur les secrets d'affaires est plus faible et les coûts pour sa protection sont plus élevés, et ii) le risque commercial lors de la communication de tels secrets est plus élevé. Ainsi, 40 % des entreprises de l'UE s'abstiendraient de communiquer des secrets d'affaires à des tiers de crainte que les informations ne fassent l'objet d'une utilisation abusive ou ne soient diffusées sans leur autorisation, perdant ainsi leur caractère confidentiel. Cela freine l'innovation, et en particulier la recherche collaborative et l'innovation ouverte, qui nécessitent que de multiples entreprises et partenaires de recherche échangent des informations de valeur;
- les avantages concurrentiels fondés sur un secret d'affaires sont menacés (compétitivité réduite): la protection juridique fragmentée ne garantit pas une protection et un niveau de recours comparables dans tout le marché intérieur de l'UE, ce qui met ces avantages en péril, qu'ils soient liés ou non à l'innovation, et fragilise la compétitivité des détenteurs de secret d'affaires. Par exemple, l'industrie chimique européenne, qui dépend fortement de l'innovation de procédé reposant sur des secrets d'affaires, estime que l'appropriation illicite d'un secret d'affaires peut, dans de nombreux cas, faire perdre jusqu'à 30 % du chiffre d'affaires.

L'objectif de l'initiative est de faire en sorte que la compétitivité des entreprises et organismes de recherche européens qui se fonde sur des savoir-faire et informations commerciales non divulgués (secrets d'affaires) soit protégée de manière adéquate, ainsi que d'améliorer les conditions-cadres pour le développement et l'exploitation de l'innovation et pour le transfert de connaissances au sein du marché intérieur. En particulier, l'initiative vise à renforcer l'efficacité de la protection juridique des secrets d'affaires contre l'appropriation illicite dans le marché intérieur.

Pour résoudre ce problème, les options suivantes ont été envisagées:

- Statu quo.
- Sensibilisation aux mesures, procédures et réparations existant au niveau national contre les appropriations illicites de secrets d'affaires, et diffusion d'informations à ce sujet.
- Convergence des droits civils nationaux en ce qui concerne le caractère illicite des actes d'appropriation de secrets d'affaires (mais les règles en matière de réparations et de protection du caractère confidentiel des secrets d'affaires durant les actions en justice seraient adoptées au niveau national).
- Convergence des voies de recours en droit civil en cas d'appropriation illicite de secrets d'affaires et des règles sur la protection du caractère confidentiel des secrets d'affaires pendant et après une action en justice (en sus de l'option 3).
- Convergence des droits pénaux nationaux, y compris des règles sur les sanctions pénales minimales, en sus de la convergence des droits civils (option 4).

Selon les conclusions de l'analyse d'impact, l'option 4 est proportionnée aux objectifs poursuivis et la mieux à même de permettre leur réalisation.

Sur le plan des incidences, la convergence des voies de recours en droit civil permettrait aux entreprises innovantes de défendre leurs secrets d'affaires légitimes de façon plus efficace dans toute l'UE. En outre, si les détenteurs de secret d'affaires pouvaient compter sur la confidentialité durant les procédures judiciaires, ils seraient davantage enclins à demander une protection juridictionnelle contre les dommages qu'ils pourraient subir en cas d'appropriation illicite de leurs secrets d'affaires. Une sécurité juridique et une convergence législative renforcées contribueraient à accroître la valeur des innovations que les entreprises souhaitent protéger en tant que secrets d'affaires, puisque le risque d'appropriation illicite serait réduit. Cela aurait des incidences positives sur le fonctionnement du marché intérieur, puisque les entreprises, en particulier les PME, et les chercheurs pourraient mieux tirer profit de leurs idées innovantes en coopérant avec les meilleurs partenaires de toute l'UE, ce qui contribuerait à augmenter les investissements du secteur privé dans la R&D au sein du marché intérieur. Parallèlement, il ne devrait pas y avoir de restrictions de la concurrence puisque l'octroi de droits exclusifs n'est pas prévu, tout concurrent étant libre d'obtenir de façon indépendante (y compris par ingénierie inverse) les connaissances protégées par le secret d'affaires. De même, la proposition ne devrait pas avoir d'incidences négatives sur l'embauche et la mobilité de main-d'œuvre hautement qualifiée (ayant accès aux secrets d'affaires) dans le marché intérieur. Au fil du temps, des effets positifs sur la compétitivité et la croissance de l'économie de l'UE devraient se faire sentir. L'initiative ne devrait pas avoir d'incidence négative en matière de droits fondamentaux. En particulier, elle promouvra le droit de propriété et la liberté d'entreprise. En ce qui concerne l'accès aux documents lors de procédures judiciaires, des mesures de sauvegarde des droits de la défense ont été mises en place. L'initiative contient aussi des mesures de sauvegarde visant à ce que la liberté d'expression et d'information soit garantie.

L'initiative est compatible avec les obligations internationales, notamment avec l'accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (accord sur les ADPIC). D'importants partenaires commerciaux de l'UE ont une législation similaire en la matière.

3. ÉLÉMENTS JURIDIQUES DE LA PROPOSITION

L'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE) prévoit l'adoption de règles de l'UE relatives au rapprochement des législations nationales lorsque cela est nécessaire au bon fonctionnement du marché intérieur. L'objectif de la proposition est d'établir un niveau suffisant et comparable de recours dans tout le marché intérieur en cas d'appropriation illicite d'un secret d'affaires (tout en mettant en place des mesures de sauvegarde suffisantes pour prévenir les abus). Les réglementations nationales existantes offrent un niveau inégal de protection des secrets d'affaires contre l'appropriation illicite, ce qui met en péril le bon fonctionnement du marché intérieur de l'information et du savoir-faire. En effet, afin que le plein potentiel économique des informations de valeur (e.a. procédés de fabrication, nouvelles substances et nouveaux matériaux, technologies non brevetées, processus d'entreprise) puisse se réaliser, ces informations doivent pouvoir être transférées en toute confiance, étant donné que chaque acteur est susceptible de les utiliser différemment dans sa propre zone géographique, générant ainsi des revenus pour les créateurs et permettant une répartition efficiente des ressources. Le cadre légal disparate réduit

aussi les incitations à entreprendre toute activité transfrontière innovante qui dépendrait de l'utilisation d'informations protégées par le secret d'affaires, par exemple s'établir dans un autre État membre pour y fabriquer ou commercialiser des produits ou services basés sur de tels secrets, fournir des produits ou services à une entreprise dans un autre État membre ou sous-traiter la fabrication à une telle entreprise. Dans ces situations, si le secret d'affaires fait l'objet d'une appropriation illicite dans un autre pays ayant un niveau de protection plus faible, des produits en infraction risquent d'être diffusés sur le marché. Les réglementations nationales existantes rendent donc la R&D et l'innovation transfrontières en réseau moins attractives et plus difficiles. Elles entraînent par ailleurs un niveau plus élevé de risque commercial dans les États membres où le niveau de protection est le plus faible, ce qui a des effets négatifs sur l'ensemble de l'économie de l'UE, étant donné que, d'une part, les incitations au commerce transfrontière diminuent et, d'autre part, des «produits en infraction» originaires de ces États membres (ou importés via leur territoire) peuvent se répandre dans le marché intérieur. La proposition devrait faciliter la coopération transfrontière en matière de R&D: une protection claire, organisée et uniformisée des secrets d'affaires contre leur appropriation illicite encourage l'échange et le transfert d'informations commerciales et de savoir-faire confidentiels d'un pays à l'autre en réduisant les risques perçus et les coûts de transaction liés à la gestion de législations multiples. Elle devrait aussi améliorer les incitations au commerce transfrontière, grâce à la réduction de la concurrence déloyale exercée par des opportunistes dans le marché transfrontière.

En ce qui concerne la subsidiarité, les problèmes relevés dans l'analyse d'impact résultent de l'hétérogénéité et de l'incohérence du cadre réglementaire existant, qui ne garantit pas des conditions de concurrence égales pour les entreprises de l'UE, ce qui a des conséquences négatives sur leur compétitivité et, plus globalement, sur celle de l'UE. Une plus grande cohérence des mécanismes de recours d'un État membre à l'autre est cruciale pour remédier à ces problèmes. Cependant, cette cohérence ne peut pas être obtenue par des actions entreprises uniquement au niveau des États membres: l'expérience dans ce domaine montre que, même lorsque les États se coordonnent entre eux, comme par exemple dans le cadre de l'accord sur les ADPIC, l'harmonisation des règles nationales reste insuffisante sur le fond. Par conséquent, l'action proposée doit être menée au niveau de l'UE, tant en ce qui concerne son échelle que ses effets.

4. INCIDENCE BUDGÉTAIRE

La proposition n'a aucune incidence sur le budget de l'Union européenne. Toutes les actions à entreprendre par la Commission qui figurent dans la proposition sont en conformité et compatibles avec le nouveau cadre financier pluriannuel 2014-2020.

5. Analyse de la proposition

5.1. Dispositions générales

Le chapitre I définit l'objet de la proposition (article 1er): la directive concerne l'obtention, la divulgation et l'utilisation illicites de secrets d'affaires et les mesures, procédures et réparations à mettre en place aux fins des recours civils en la matière.

Toujours dans le chapitre I, l'article 2 définit les concepts clés. La définition d'un «secret d'affaires» comporte trois éléments: i) les informations doivent être confidentielles; ii) elles ont une valeur commerciale en raison de ce caractère confidentiel; iii) le détenteur du secret d'affaires a pris des dispositions raisonnables pour préserver sa confidentialité. Cette définition est calquée sur celle des «renseignements non divulgués» qui figure dans l'accord sur les ADPIC.

La définition d'un «détenteur de secret d'affaires» inclut comme élément clé le concept du caractère licite du contrôle sur le secret, qui figure également dans l'accord sur les ADPIC. Elle permet donc une défense du secret d'affaires non seulement par son détenteur initial, mais aussi par les titulaires d'une licence.

La définition d'un «produit en infraction» intègre une évaluation de la proportionnalité. Il faut que les produits qui sont conçus, fabriqués ou commercialisés à l'aide d'un comportement illicite bénéficient de manière notable du secret d'affaires en question pour qu'ils soient considérés comme des produits en infraction. Cette évaluation devrait être faite dès lors que sont envisagées des mesures ayant une incidence directe sur des produits fabriqués ou mis sur le marché par un contrevenant.

Le chapitre II définit les circonstances dans lesquelles l'obtention, l'utilisation ou la divulgation d'un secret d'affaires est illicite (article 3), ce qui donne le droit au détenteur dudit secret de demander l'application des mesures et réparations prévues par la directive. L'élément-clé pour que ces actes soient considérés comme illicites est l'absence de consentement du détenteur du secret d'affaires. L'article 3 rend illicite l'utilisation d'un secret d'affaires par un tiers n'ayant pas participé directement à l'obtention, l'utilisation ou la divulgation illicites initiales, mais qui a ou aurait dû avoir connaissance de cet acte illicite initial, ou qui a été informé de son caractère illicite. L'article 4 précise expressément que la découverte indépendante et l'ingénierie inverse sont des moyens légitimes d'obtenir une information.

5.2. Mesures, procédures et réparations

Le chapitre III détermine les mesures, procédures et réparations qui devraient être mises à la disposition du détenteur d'un secret d'affaires en cas d'obtention, d'utilisation ou de divulgation illicite de ce secret par un tiers.

La section 1 établit les principes généraux applicables aux instruments de droit civil visant à empêcher et à réprimer les actes d'appropriation illicite d'un secret d'affaires, qui doivent notamment être effectifs, équitables et proportionnés (article 5), ainsi que des mesures de sauvegarde pour empêcher l'usage abusif de procédures judiciaires (article 6). L'article 7 instaure un délai de prescription. L'article 8 impose aux États membres de prévoir des mécanismes permettant aux autorités judiciaires de protéger le caractère confidentiel des secrets d'affaires divulgués devant une juridiction aux fins de la procédure. Parmi les mesures possibles doivent figurer: la restriction de l'accès à tout ou partie des documents soumis par les parties ou par des tiers; la restriction de l'accès aux audiences et rapports d'audience; la possibilité d'obliger les parties ou des tiers de rédiger des versions non confidentielles des documents qui contiennent des secrets d'affaires; la rédaction de versions non confidentielles des décisions judiciaires. Ces mesures devraient être appliquées de manière proportionnée, de façon à ne pas nuire au droit des parties à un procès équitable. Les mesures de confidentialité doivent s'appliquer pendant l'action en justice, mais aussi après celle-ci pour les demandes d'accès du public aux documents, aussi longtemps que les informations en question demeurent un secret d'affaires.

La section 2 prévoit des mesures provisoires et conservatoires, sous la forme d'ordonnances de référé ou de saisies conservatoires de produits en infraction (article 9). Elle établit aussi des mesures de sauvegarde afin de garantir le caractère équitable et proportionné de ces mesures provisoires et conservatoires (article 10).

La section 3 précise les mesures qui peuvent être ordonnées par un jugement au fond. L'article 11 prévoit l'interdiction de l'utilisation ou de la divulgation du secret d'affaires, l'interdiction de fabriquer, d'offrir, de mettre sur le marché ou d'utiliser des produits en infraction (ou d'importer ou de stocker de tels produits à ces fins), ainsi que des mesures correctives. Ces mesures sont, entre autres, la destruction par le contrevenant de toutes les informations qu'il détient en rapport avec le secret d'affaires obtenu, utilisé ou divulgué de façon illicite, ou leur remise au détenteur initial de ce secret. L'article 12 établit des mesures de sauvegarde pour garantir le caractère équitable et proportionné des mesures prévues à l'article 11.

L'octroi de dommages-intérêts au détenteur du secret d'affaires pour le préjudice subi en raison de l'obtention, de l'utilisation ou de la divulgation illicites de son secret est prévu à l'article 13, qui prescrit que soient pris en considération tous les facteurs pertinents, y compris les bénéfices injustement réalisés par le défendeur. La possibilité de calculer les dommages-intérêts sur la base des redevances hypothétiques est également offerte, sur le modèle de ce qui est prévu en cas d'infraction aux droits de propriété intellectuelle.

L'article 14 permet aux autorités judiciaires compétentes d'adopter, à la demande du requérant, des mesures de publicité, y compris la publication de la décision au fond, à condition que le secret d'affaires ne soit pas divulgué et que le caractère proportionné de la mesure ait été vérifié.

La directive ne contient pas de règles sur l'exécution transfrontière des décisions judiciaires étant donné que les règles générales de l'UE en la matière s'appliquent, permettant l'exécution dans tous les États membres d'une décision de justice interdisant les importations de produits en infraction dans l'UE.

5.3. Sanctions, rapports et dispositions finales

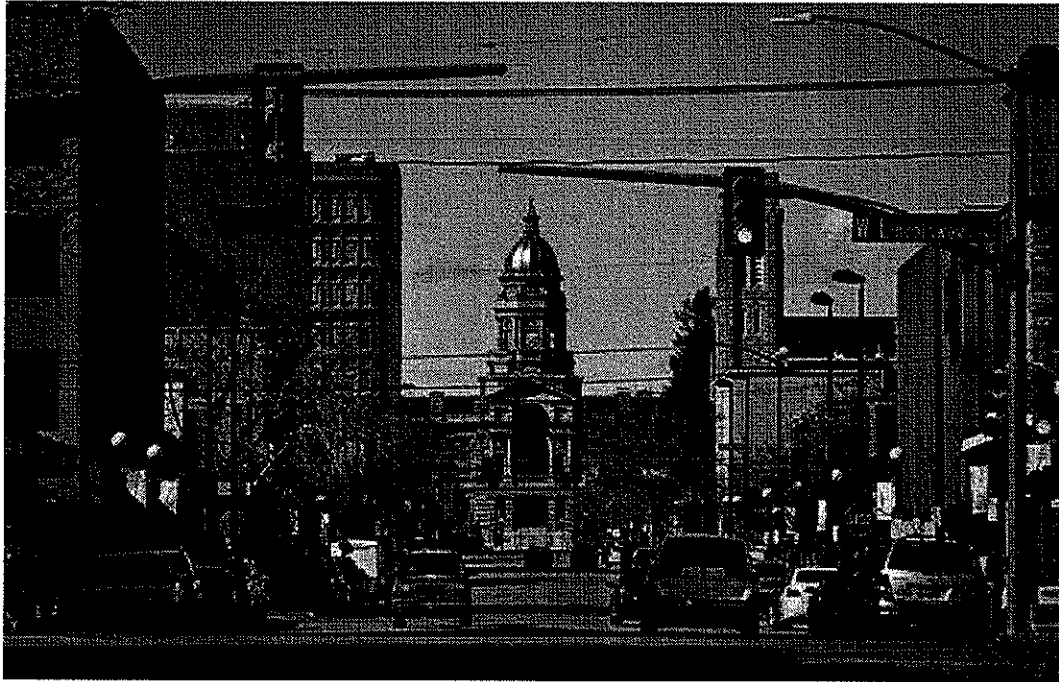
Afin d'assurer l'application effective de la directive et la réalisation des objectifs poursuivis, le chapitre IV prévoit l'application de sanctions en cas de non-respect des mesures prévues au chapitre III et comporte des dispositions en matière de suivi et de rapports.

La Commission considère que, sur la base des déclarations communes sur les documents explicatifs[2], il n'existe pas suffisamment d'arguments justifiant de demander formellement aux États membres qu'ils communiquent des documents expliquant le lien entre les éléments de la directive et les parties correspondantes des instruments nationaux de transposition. D'un point de vue technique, la directive n'est pas particulièrement complexe; elle ne contient qu'un nombre limité d'obligations juridiques nécessitant une transposition en droit national et traite d'un sujet bien délimité qui a déjà été réglementé au niveau national en rapport avec les DPI, domaine voisin. La transposition au niveau national ne devrait donc pas présenter de difficultés, ce qui devrait faciliter son suivi.

2013/0402 (COD)

L'administration Obama promet d'agir contre les sociétés offshore américaines

Le Monde.fr avec AFP | 16.04.2016 à 16h50



Le Wyoming, Etat américain le moins peuplé, est l'un des principaux "paradis fiscaux" des Etats-Unis. Marc Piscotty / McClatchy

L'offensive « anti-offshore » de l'administration Obama se précise : annoncé au *Monde* (économie/article/2016/03/31/barack-obama-pret-a-reformer-le-paradis-fiscal-du-delaware_4893196_3234.html) le 31 mars par le secrétariat au Trésor, le plan de lutte contre l'opacité des sociétés-écrans (#huit-anchor-societeecran) créées aux Etats-Unis est en cours de finalisation, selon le secrétaire au Trésor, Jack Lew. « *L'évasion fiscale (#huit-anchor-evasionfiscale) [...] nuit aux finances publiques, affecte l'équité de nos systèmes fiscaux et freine la croissance mondiale* », a-t-il estimé.

Cette initiative intervient alors que l'onde de choc des « Panama papers », qui a mis au jour un vaste réseau de sociétés-écrans dans des paradis fiscaux, continue de se propager et a conduit le G 20 Finances à ébaucher vendredi une première contre-offensive, en appelant à se doter des moyens de savoir qui se cache derrière les sociétés-écrans et à établir une nouvelle liste des paradis fiscaux non coopératifs.

Lire aussi : Panama, Vanuatu et Liban sont menacés de figurer sur la liste noire des paradis fiscaux (panama-papers/article/2016/04/16/panama-papers-panama-vanuatu-et-liban-sont-menaces-de-figurer-sur-la-liste-noire-des-paradis-fiscaux_4903528_4890278.html)

Identifier les bénéficiaires réels

Les Etats-Unis ont été relativement épargnés par ces révélations mais sont régulièrement mis à l'index pour la possibilité offerte par certains Etats américains (Delaware, Wyoming...) d'ouvrir une société sans dévoiler le nom de son réel bénéficiaire (#huit-anchor-ayantdroit). « *Nous sommes sur le point de proposer une régulation qui exigerait d'un réel bénéficiaire d'une société individuelle à responsabilité limitée de s'identifier auprès de l'Internal Revenue Service [le fisc américain] afin de combler une faille que certains ont réussi à exploiter* », a assuré M. Lew dans sa déclaration écrite au FMI, en marge de l'assemblée de printemps de l'institution.

Des sociétés-écrans immatriculées aux Etats-Unis ont été utilisées pour contourner les sanctions américaines ou abriter les revenus de trafiquants d'armes.

Le Trésor est également en train de « finaliser » une autre règle qui forcerait les banques à identifier le réel bénéficiaire d'une société nouvellement formée avant d'ouvrir un compte, a ajouté M. Lew.

Les banques américaines ne sont pour l'heure tenues qu'à une obligation générale de « connaître leurs clients » qui ne les empêche pas de traiter avec des sociétés offshore.