

Note

Secrets d'affaires et devoir de diligence: quelles mesures raisonnables pour protéger les secrets d'affaires?*Valentin de le Cour et Nicolas Heremans¹***A. INTRODUCTION**

1. Les entreprises utilisent aujourd'hui très largement la confidentialité pour protéger le résultat de leur innovation. Le secret d'affaires est ainsi devenu un outil de création de valeur essentiel pour organiser leur compétitivité et est à cette fin davantage utilisé que le brevet par une majorité d'entreprises européennes². Ce constat se confirme pour un nombre croissant de technologies, comme en témoigne par exemple l'intelligence artificielle dont les applications toujours plus nombreuses reposent principalement sur des algorithmes qui ne sont protégeables que par le biais du secret³.

2. Pour renforcer l'efficacité de ce mode de protection et remédier aux difficultés liées à des standards de protection disparates et inégaux au sein de l'Union européenne, le législateur européen a adopté le 8 juin 2016 la directive n° 2016/943 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (« directive n° 2016/943 »)⁴. La loi du 30 juillet 2018 relative à la protection des secrets d'affaires a transposé cette directive en droit belge⁵.

3. Un apport majeur de la directive 2016/943 est d'adopter une définition harmonisée et ouverte de la notion de « secret d'affaires »⁶. L'article I.17/1, 1°, du Code de droit économique transpose presque littéralement cette notion et

définit désormais le secret d'affaires comme l'« information qui répond à toutes les conditions suivantes:

- a) elle est secrète en ce sens que, dans sa globalité ou dans la configuration et l'assemblage exacts de ses éléments, elle n'est pas généralement connue des personnes appartenant aux milieux qui s'occupent normalement du genre d'information en question, ou ne leur est pas aisément accessible;
- b) elle a une valeur commerciale parce qu'elle est secrète;
- c) elle a fait l'objet, de la part de la personne qui en a le contrôle de façon licite, de dispositions raisonnables, compte tenu des circonstances, destinées à la garder secrète »⁷.

4. En droit belge, toute information de nature technique, financière ou commerciale, peut donc *a priori* constituer un secret d'affaires pour autant que l'entité qui en a le contrôle soit en mesure de démontrer qu'elle est secrète, qu'elle a une valeur commerciale en raison de son caractère secret et que des mesures de protection raisonnables ont été adoptées pour en préserver la confidentialité⁸.

5. Fonder une demande sur la base d'une atteinte à un secret d'affaires requiert donc de pouvoir démontrer l'adoption d'une série de mesures destinées à protéger le caractère secret de l'information⁹. Il s'agit là d'une condition essen-

¹. Avocats DALDEWOLF.

². Considérants 1 et 2 de la directive (UE) n° 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicite, (*J.O.U.E.*, L. 157, 15 juin 2016) (ci-après « directive n° 2016/943 » ou « directive secrets d'affaires »); COMMISSION EUROPEENNE, « The scale and impact of industrial espionage and theft of trade secrets through cyber », disponible sur www.ec.europa.eu/docsroom/documents/34841 (*J.O.U.E.*, 18 décembre 2018, p. 6); EUIPO, « Protecting Innovation Through Trade Secrets And Patents: Determinants For European Union Firms », disponible sur www.euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Trade%20Secrets%20Report_en.pdf, juillet 2017, p. 8.

³. « Podcast du Journal des tribunaux. Episode 3. Les secrets d'affaires », disponible sur www.larcier.com/fr/les-secrets-d-affaires/?utm_source=Larcier+-+FR&utm_campaign=08bb81459e-WAE20013B&utm_medium=email&utm_term=0_d4253043ac-08bb81459e-27542153&mc_cid=08bb81459e&mc_eid=4dd13c035b, s.d., consulté le 22 avril 2020.

⁴. Considérants 6 à 8 de la directive n° 2016/943; J.-M. LISSEN et E. GOUGE, « Implementation of the EU trade Secrets Directive in the EU and beyond: an introductory note », *Les Nouvelles*, 2019, p. 162.

⁵. Loi du 30 juillet 2018 relative à la protection des secrets d'affaires (*M.B.*, 14 août 2018) (ci-après « loi du 30 juillet 2018 » ou « loi secrets d'affaires »).

⁶. Considérant 14 et art. 2, 1., de la directive n° 2016/943.

⁷. Art. 1/17, 1°, du Code de droit économique (ci-après « CDE »).

⁸. La jurisprudence récente en la matière révèle que les juridictions belges vérifient aujourd'hui de façon assez systématique la réunion de ces trois conditions avant de qualifier ou non une information de secrets d'affaires, préalable nécessaire à l'examen des demandes formulées sur la base de ce fondement; Entr. Anvers, 16 octobre 2019, *inédit*, R.G. A/19/04068.

⁹. K. NACHTRAB, « Protecting Organizational Trade Secrets In View Of The EU Trade Secrets Directive », *Les Nouvelles*, 2019, p. 232.

tielle, dont l'absence ou le caractère insuffisant ne permettrait pas de qualifier l'information de secret d'affaires ce qui fera perdre le bénéfice du régime de protection mis en place par la loi du 30 juillet 2018¹⁰.

6. Or, ni la directive n° 2016/943, ni la loi du 30 juillet 2018 ne définissent les « *dispositions raisonnables, compte tenu des circonstances* » qu'il convient d'adopter pour garder l'information secrète, laissant à la jurisprudence le soin de préciser davantage les contours de cette notion¹¹.

B. LE JUGEMENT DU TRIBUNAL DE L'ENTREPRISE D'ANVERS DU 9 MAI 2019 (A/18/3273)

8. Dans cette affaire, le tribunal de l'entreprise d'Anvers a dû trancher la question de savoir si un prestataire de services externe, jouant un rôle clé au sein du département recherche et développement du demandeur, s'était rendu coupable d'une appropriation illicite de secrets d'affaires en copiant une quantité importante d'informations confidentielles provenant des serveurs de l'entreprise.

9. En l'espèce, les parties collaboraient depuis plus de 20 ans sans qu'aucun contrat n'ait été signé pour organiser leur relation (un projet avait été négocié mais pas signé). Le prestataire de services avait émis des factures qui avaient été payées par l'entreprise sur la seule base d'un accord verbal. Aucune obligation de confidentialité à charge du défendeur n'avait donc été formalisée par écrit.

10. Les fichiers copiés par le défendeur avaient trait aux lignes de production de l'entreprise et comprenaient des croquis, dessins techniques, schémas, manuels et photos qui, selon le demandeur, permettaient de comprendre l'intégralité de son procédé de production.

11. Le demandeur soutenait sur la base de l'article XI.332/4, § 1^{er}, du Code de droit économique qu'en copiant ces fichiers, le prestataire de services s'était rendu coupable d'une obtention illicite de secrets d'affaires, en parallèle de demandes fondées sur une violation alléguée du droit d'auteur et du droit des bases de données dont l'entreprise soutenait être titulaire^{12,13}.

7. La décision du tribunal de l'entreprise d'Anvers du 9 mai 2019 que nous commentons ci-après, et l'appréciation faite par le tribunal des mesures de protection du secret adoptées par le demandeur, offrent à cet égard un premier éclairage, certes limité, mais néanmoins intéressant. Cette décision, une des premières rendues sur la base du nouveau régime, confirme le caractère concret de cette appréciation qui doit se fonder sur les circonstances propres de l'espèce.

12. En défense, le prestataire de services invoquait notamment le fait que l'information copiée ne constituait pas un savoir-faire protégé et que, quand bien même ce serait le cas, il n'était pas lié par une obligation de confidentialité limitant son droit d'obtenir des secrets d'affaires du demandeur.

13. Dans son appréciation du devoir de diligence et des mesures de protection du secret adoptées, le tribunal a considéré que le demandeur avait démontré de façon convaincante (i) que l'entreprise utilisait des contrats avec ses fournisseurs et employés qui prévoyaient des obligations de confidentialité, et (ii) qu'elle avait réalisé des investissements en matière de sécurité informatique, comprenant notamment la mise en place d'une politique de gestion des accès à l'information confidentielle.

14. Concernant le caractère illicite de l'obtention des secrets d'affaires, le tribunal a tenu compte du fait (i) que le défendeur devait savoir que l'information en cause constituait un secret d'affaires de l'entreprise qu'il ne pouvait pas diffuser librement (plusieurs documents contenaient une notice de confidentialité précisant qu'ils ne pouvaient pas être diffusés) et (ii) que l'absence de clause expresse de confidentialité à charge du défendeur ne permettait pas de déroger à l'obligation d'exécution de bonne foi des conventions, un constat renforcé par le fait qu'il est courant dans les milieux spécialisés de la recherche et du développement de ne pas divulguer ou copier les résultats de la recherche et par l'apposition desdites notices de confidentialité sur certains documents.

¹⁰. V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », V. CASSIERS (dir.), *Secrets d'affaires, Dossiers J.T.*, n° 113, Bruxelles, Larcier, 2020, p. 26, n° 32 ; V. CASSIERS, « La transposition de la directive 2016/943/UE du 8 juin 2016 », *Droit de la propriété intellectuelle: actualité législative et jurisprudence récente de la Cour de justice de l'Union européenne*, N. BERTHOLD (dir.), Bruxelles, Larcier, 2019, p. 271, n° 24.

¹¹. Projet de loi relatif à la protection des secrets d'affaires, *Doc. parl.*, Chambre, 2017-2018, n° 54-3154/1 (« projet de loi secrets d'affaires »), p. 12.

¹². Art. XI.332/4, § 1^{er}, CDE: « L'obtention d'un secret d'affaires sans le consentement du détenteur du secret d'affaires est considérée comme illicite lorsqu'elle est réalisée par le biais: 1° d'un accès non autorisé à tout document, objet, matériel, substance ou fichier électronique ou d'une appropriation ou copie non autorisée de ces éléments, que le détenteur du secret d'affaires contrôle de façon licite et qui contiennent ledit secret d'affaires ou dont ledit secret d'affaires peut être déduit; 2° de tout autre comportement qui, eu égard aux circonstances, est considéré comme contraire aux usages honnêtes en matière commerciale. »

¹³. Le demandeur reprochait également au prestataire de services d'avoir porté atteinte à ses droits d'auteur (art. XI.165 et s. CDE) et d'avoir violé son droit de producteur de bases de données (art. XI.306 et s. CDE). Le tribunal a toutefois rejeté ces fondements et a jugé (i) que les fichiers copiés n'étaient pas protégés par le droit d'auteur, le demandeur n'ayant pas établi le caractère original des œuvres en cause, et (ii) que le demandeur n'avait pas apporté la preuve d'un investissement qualitativement ou quantitativement substantiel permettant de se prévaloir du droit de producteur de bases de données.

15. Le tribunal a ainsi considéré que le défendeur était effectivement tenu à une obligation de confidentialité et qu'il s'était rendu coupable d'une obtention illicite de secrets d'affaires, et a ordonné sur cette base une mesure

d'interdiction d'utiliser et de divulguer les secrets d'affaires en cause à l'encontre du prestataire de services, sous peine d'une astreinte de 25.000 EUR par infraction, plafonnée à 200.000 EUR.

C. LE DEVOIR DE DILIGENCE DU DÉTENTEUR DE SECRETS D'AFFAIRES

16. Si l'adoption de mesures raisonnables de confidentialité est une condition essentielle pour qu'une information puisse être qualifiée de secret d'affaires, la directive n° 2016/943 et la loi belge du 30 juillet 2018 n'offrent que peu de précisions sur la nature concrète des mesures à implémenter¹⁴.

17. Le considérant 23 de la directive n° 2016/943 se réfère à un devoir de diligence et précise « *que l'on attend des détenteurs légitimes de secrets d'affaires qu'ils exercent un devoir de diligence en ce qui concerne la protection du caractère confidentiel de leurs secrets d'affaires de valeur et le contrôle de leur utilisation* »¹⁵.

18. Les travaux préparatoires de la loi belge du 30 juillet 2019 disposent que « *les 'mesures raisonnables' visant à garder secrètes les informations visées sous l'°, c), sont évaluées par le juge* » et qu'elles « *peuvent revêtir différentes formes* », parmi lesquelles, à titre d'exemple, l'adoption « *de dispositions contractuelles, de mécanismes de sécurité physiques ou virtuels, de consigner une idée au moyen de l'idepot auprès de l'Office Benelux de la propriété intellectuelle, etc.* »¹⁶.

19. L'article 871bis du Code judiciaire, qui permet de solliciter des mesures de protection du secret dans le cadre de procédures judiciaires, précise quant à lui les deux règles générales et minimales de protection que sont (i) la limitation du nombre de personnes ayant accès à l'information en cause (autrement dit la gestion des accès aux secrets d'affaires), et (ii) l'imposition à ces mêmes personnes d'une obligation stricte de confidentialité¹⁷.

20. Au regard de ces textes, il apparaît que le détenteur de secrets d'affaires est tenu à un devoir de diligence qui lui impose de protéger proactivement le caractère confidentiel de ce type d'informations, en adoptant un ensemble de mesures de nature variée, qui sont d'ordres juridique (« *dispositions contractuelles* »), physique (« *mécanismes de sécurité physiques* ») et informatique (« *mécanismes de sécurité virtuels* »)¹⁸. Ces mesures viseront notamment à limiter et à contrôler l'accès à l'information en cause et imposer une obligation stricte de confidentialité à charge de toute personne y ayant (eu) accès¹⁹.

21. L'appréciation faite par le juge du caractère raisonnable des mesures adoptées sera fonction des circonstances, comme en témoigne la décision commentée du 9 mai 2019 du tribunal de l'entreprise d'Anvers.

D. LES BONNES PRATIQUES EN MATIÈRE DE PROTECTION DU SECRET DE L'INFORMATION

22. La directive n° 2016/943 et la loi belge du 30 juillet 2018 n'apportent donc qu'un éclairage limité sur les mesures concrètes de protection du secret qu'il convient d'adopter, laissant aux entreprises une certaine latitude dans la manière

de protéger leurs secrets d'affaires²⁰. Afin de répondre à cette obligation, il est donc recommandé de veiller à proactivement définir, implémenter et documenter des mesures de protection qui devront être raisonnables au regard des cir-

¹⁴. K. NACHTRAB, *o.c.*, p. 232. D'autres juridictions ont fait le choix de préciser davantage le contenu de cette condition. A titre d'exemple, la Cour populaire suprême chinoise a énuméré une liste non exhaustive de mesures de protection du secret de manière à guider les entreprises dans la protection de leurs secrets d'affaires (art. 11, Interpretation de la Cour populaire suprême chinoise du 12 janvier 2007, Fashi 2/2007 (Sup. People's Ct. 2007) (Chine): « (1) Limitation de l'accès aux informations confidentielles et divulgation uniquement en cas de nécessité ('need-to-know basis'); (2) Verrouillage du support contenant les informations confidentielles ou adoption de toute autre mesure préventive; (3) Notice de confidentialité apposée sur le support d'informations confidentielles; (4) Adoption de mots de passe ou de codes d'accès sur les informations confidentielles; (5) Signature d'accord de confidentialité; (6) Limitation de l'accès des visiteurs aux machines, usines, ateliers ou tout autre lieu de travail confidentiel, ou imposition d'obligations de confidentialité aux visiteurs; (7) Adoption de toute autre mesure appropriée pour assurer la confidentialité de l'information. »

¹⁵. Considérant 23 de la directive n° 2016/943.

¹⁶. Projet de loi secrets d'affaires, *o.c.*, p. 12.

¹⁷. V. CASSIERS, « La transposition de la directive 2016/943/UE du 8 juin 2016 », *o.c.*, p. 271, n° 24.

¹⁸. Projet de loi secrets d'affaires, *o.c.*, p. 12; V. CASSIERS, « La transposition de la directive 2016/943/UE du 8 juin 2016 », *o.c.*, p. 271, n°s 29 à 31; T. EWING et D. O'CONNEL, « Undiscovered country – building a trade secret culture », *IAM*, mai-juin 2017, p. 34.

¹⁹. V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », *o.c.*, p. 26, n° 31.

²⁰. K. NACHTRAB, *o.c.*, p. 232.

constances propres à l'entreprise²¹. Les dispositions raisonnables consisteront typiquement à identifier et à documenter les secrets d'affaires de valeur, et à définir ensuite un ensemble de mesures de protection de nature organisationnelle, physique, juridique et informatique.

a) L'identification des secrets d'affaires de l'entreprise et la création d'un inventaire

23. Pour qu'une entreprise puisse efficacement protéger ses secrets d'affaires, une bonne pratique consistera tout d'abord à identifier ce qu'il convient de protéger à ce titre par le biais d'un audit de ses informations confidentielles²². Il s'agit de les cartographier et de veiller à distinguer les secrets d'affaires des informations non protégeables à ce titre (informations courantes, expériences acquises par les travailleurs dans l'exercice normal de leurs fonctions, et toute information généralement connue ou aisément accessible des milieux concernés qui ne répond donc pas à la définition de « secrets d'affaires » au sens de l'art. I.17/1 CDE)²³. L'identification systématique des secrets d'affaires communiqués par des tiers ne devra pas être négligée²⁴.

24. En parallèle, l'entreprise procédera à une évaluation des risques pour cerner les besoins de l'organisation et identifier les mesures concrètes de protection à implémenter, ce qui aboutira généralement à l'élaboration d'une politique de confidentialité transversale dont le but est d'organiser la gestion des secrets d'affaires au sein de l'entreprise²⁵.

25. Ce travail d'identification pourra utilement déboucher sur la création d'un registre interne à l'entreprise, reprenant les secrets d'affaires ayant le plus de valeur et auxquels seront associés un ensemble d'informations ou de métadonnées (à titre d'exemple, citons le titre/numéro/référence permettant d'identifier le secret d'affaires en cause, sa date de

création, sa localisation, ses créateurs, détenteurs et les personnes en charge de sa gestion; sa nature technique, commerciale, opérationnelle ou financière; sa valeur et son importance pour l'entreprise et le niveau de confidentialité correspondant; les personnes ayant (eu) accès à l'information et les conditions d'accès; les risques éventuels d'appropriation illicite; et les mesures de protection du secret qui y sont associées)²⁶. La tenue d'un tel registre sera souvent le prérequis d'une gestion rationnelle et effective d'un portefeuille de secrets d'affaires et pourra, le cas échéant, jouer un rôle déterminant pour établir qu'une information peut être qualifiée de secret d'affaires²⁷.

b) La mise en place de mesures de protection du secret

26. La constitution d'un registre et l'identification des secrets d'affaires de valeur que l'entreprise entend protéger, facilitera la définition des mesures concrètes de protection du secret à implémenter. Nous énumérons ci-après, de façon non exhaustive, un nombre de mesures organisationnelles, physiques, juridiques et informatiques qui sont typiquement considérées à cette fin²⁸.

i. Mesures organisationnelles de protection

27. Parmi les mesures organisationnelles de protection, il convient de relever notamment la définition d'une politique organisant l'accès, l'utilisation et la divulgation des secrets d'affaires au sein de l'entreprise²⁹; la désignation d'une personne, voire d'une équipe, responsable de la protection des secrets d'affaires de l'entreprise³⁰; le recours à des dispositifs permettant de donner une date certaine à l'information protégée (tel un i-depot)³¹; l'apposition systématique de notices de confidentialité sur l'information visée³²; la confirmation écrite du caractère confidentiel de tout secret d'affaires

²¹. V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », *o.c.*, p. 26, n° 32; K. NACHTRAB, *o.c.*, p. 232; R.M. HALLIGAN et R.F. WEYAND, *Trade Secret Asset Management 2018: A Guide to Information Asset Management Including RICO and Blockchain*, Weyand Associates, 2018, p. 21.

²². T. EWING et D. O'CONNEL, *o.c.*, p. 35.

²³. Considérant 14 de la directive secrets d'affaires *jo.* art. I.17/1, 1°, CDE; K. NACHTRAB, *o.c.*, p. 233; R. BINNS, « The trade secret recipe: a 'reasonable' step-by-step guide to protecting your confidential information », *European Intellectual Property Review*, 2019, p. 5, n° 6; R.M. HALLIGAN et R.F. WEYAND, *o.c.*, pp. 116 et 117.

²⁴. K. NACHTRAB, *o.c.*, p. 233.

²⁵. Une telle politique détaillera les mesures à prendre pour identifier, évaluer et classer l'information à protéger ainsi que les règles à suivre en matière de divulgation et d'utilisation des secrets d'affaires, tant au sein de l'organisation que par les tiers avec lesquels l'information est partagée; R.M. HALLIGAN et R.F. WEYAND, *o.c.*, pp. 139 à 143; T. EWING et D. O'CONNEL, *o.c.*, p. 34.

²⁶. R. BINNS, *o.c.*, p. 5; K. NACHTRAB, *o.c.*, p. 235; R.M. HALLIGAN et R.F. WEYAND, *o.c.*, pp. 112 à 121; T. EWING et D. O'CONNEL, *o.c.*, p. 33; CREATE.org, « 'Reasonable Steps' to protect trade secrets: leading practices in an evolving legal landscape », disponible sur www.joneswalkertrade-secret.lexblogplatformthree.com/wp-content/uploads/sites/323/2015/07/Reasonable-Steps.pdf, 2015, p. 10.

²⁷. K. NACHTRAB, *o.c.*, p. 235; R.M. HALLIGAN et R.F. WEYAND, *o.c.*, p. 121.

²⁸. K. NACHTRAB, *o.c.*, p. 233; CREATE.org, « 'Reasonable Steps' to protect trade secrets: leading practices in an evolving legal landscape », *o.c.*, p. 6.

²⁹. K. NACHTRAB, *o.c.*, p. 232.

³⁰. K. NACHTRAB, *o.c.*, p. 233; T. EWING et D. O'CONNEL, *o.c.*, p. 34; CREATE.org, « Protecting Trade Secrets from Cyber and Other Threats: 'Reasonable Steps' and Leading Practices », disponible sur www.create.org/wp-content/uploads/2015/07/CREATE.org-Protecting-Trade-Secrets-from-Cyber-and-Other-Threats-April-2018.pdf, 2018, p. 6; CREATE.org, « 'Reasonable Steps' to protect trade secrets: leading practices in an evolving legal landscape », *o.c.*, p. 11.

³¹. Projet de loi secrets d'affaires, *o.c.*, p. 12; V. CASSIERS, « La transposition de la directive 2016/943/UE du 8 juin 2016 », *o.c.*, p. 271, n° 29.

³². K. NACHTRAB, *o.c.*, p. 233.

res divulgué oralement³³; la compartimentalisation de l'information³⁴; la définition d'un plan d'action en cas d'appropriation illicite d'un secret d'affaires³⁵ et la mise à jour périodique du registre inventoriant les secrets d'affaires (notamment les personnes qui ont (eu) accès à un secret d'affaires déterminé et l'évolution des mesures de confidentialité adoptées)³⁶.

ii. Mesures physiques de protection

28. Les mesures physiques de protection du secret visent notamment des mécanismes et procédures d'authentification, de contrôle d'identité et de limitation physique d'accès à certains locaux³⁷; le recours à des systèmes de vidéosurveillance et des vigiles ou agents de sécurité à l'entrée des locaux³⁸; l'application de politiques de « clean desk » et de destruction contrôlée de documents contenant des secrets d'affaires³⁹; ou le stockage de l'information confidentielle dans des armoires sécurisées et utilisées à cet effet⁴⁰.

iii. Mesures juridiques de protection

29. L'adoption de mesures juridiques de protection consiste principalement à imposer une obligation de confidentialité aux personnes auxquelles le secret est divulgué. Il s'agit d'une mesure minimale de protection même si, dans certaines circonstances et moyennant une certaine insécurité juridique, l'obligation de confidentialité pourra découler de l'usage et de normes plus générales comme le principe d'exécution de bonne foi des conventions⁴¹. C'est d'ailleurs ce que confirme la décision commentée du tribunal de l'entreprise d'Anvers du 9 mai 2019 qui se réfère expressément à la bonne foi et aux usages du secteur pour confirmer l'obligation de confidentialité mise à la charge du défendeur⁴².

30. Outre l'adoption d'une politique de gestion des secrets d'affaires transversale à l'organisation, ces mesures juridiques consisteront à conclure des accords de confidentialité (ou « Non-Disclosure Agreements ») à l'entame de négociations avec des tiers, dès lors que des informations confidentielles sont susceptibles d'être échangées⁴³. Des clauses de confidentialité devront par ailleurs être incluses de façon systématique dans les différents contrats qui encadrent les relations de l'entreprise avec des tiers – travailleurs, consultants, intérimaires, stagiaires, fournisseurs, clients, partenaires – et qui peuvent impliquer la création, l'utilisation ou le partage d'informations confidentielles⁴⁴. La protection juridique résidera enfin dans l'engagement de poursuites en cas d'atteinte au secret d'affaires et qui contribueront bien souvent au maintien du secret⁴⁵.

31. Les accords et clauses de confidentialité définissent généralement l'information qui doit être traitée comme confidentielle par les parties, encadrent strictement l'accès à l'information confidentielle partagée ou générée, et imposent au récepteur des obligations claires de secret (définition de l'usage limité qui peut être fait de l'information confidentielle et imposition d'obligations de non-divulgaration et de non-utilisation en dehors du cadre strict du contrat). Elles seront par ailleurs utilement assorties d'une obligation de restitution ou d'effacement en fin de contrat de l'information échangée et d'une clause pénale suffisamment dissuasive que pour inciter au respect de ces obligations⁴⁶.

32. Depuis l'entrée en vigueur de la loi du 30 juillet 2018, il convient en particulier de s'assurer que des mesures raisonnables de protection du secret seront effectivement mises en place par le(s) récepteur(s) de l'information. L'adoption d'une série de mesures de protection clairement identifiées pourra ainsi, le cas échéant, être imposée contractuellement (une pratique courante dans certains secteurs comme le pharmaceutique)⁴⁷.

33. Entr. Anvers, 9 mai 2019, A/18/3273; K. NACHTRAB, *o.c.*, p. 233; V. CASSIERS, « La transposition de la directive 2016/943/UE du 8 juin 2016 », *o.c.*, p. 271, n° 29.

34. R.M. HALLIGAN et R.F. WEYAND, *o.c.*, p. 73.

35. CREATE.org, « 'Reasonable Steps' to protect trade secrets: leading practices in an evolving legal landscape », *o.c.*, p. 13.

36. V. CASSIERS, « La transposition de la directive 2016/943/UE du 8 juin 2016 », *o.c.*, p. 271, n° 29; R.M. HALLIGAN et R.F. WEYAND, *o.c.*, p. 67.

37. K. NACHTRAB, *o.c.*, p. 236; V. CASSIERS, « La transposition de la directive 2016/943/UE du 8 juin 2016 », *o.c.*, p. 271, n° 29; CREATE.org, « 'Reasonable Steps' to protect trade secrets: leading practices in an evolving legal landscape », *o.c.*, p. 9.

38. V. CASSIERS, « La transposition de la directive 2016/943/UE du 8 juin 2016 », *o.c.*, p. 271, n° 29.

39. CREATE.org, « 'Reasonable Steps' to protect trade secrets: leading practices in an evolving legal landscape », *o.c.*, p. 9.

40. Liège, 2 septembre 2004, *J.L.M.B.*, 2006, p. 508; V. CASSIERS, « La transposition de la directive 2016/943/UE du 8 juin 2016 », *o.c.*, p. 271, n° 29.

41. V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », *o.c.*, p. 30, n° 42.

42. Entr. Anvers, 9 mai 2019, A/18/3273: « *Partijen zijn echter niet alleen gebonden tot hetgeen uitdrukkelijk is bepaald, maar ook tot alle gevolgen die voortkomen uit de aanvullende werking van de goede trouw.* »

43. B. VANBRABANT, « Les contrats relatifs au savoir-faire et autres secrets d'affaire », *Les contrats commerciaux en pratique*, R. AYDOGDU (dir.), Bruxelles, Larcier, 2016, pp. 177 à 181.

44. K. NACHTRAB, *o.c.*, pp. 233 et 234; B. VANBRABANT, *o.c.*, p. 176.

45. V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », *o.c.*, p. 31, n° 44; K. NACHTRAB, *o.c.*, p. 235.

46. K. NACHTRAB, *o.c.*, p. 234; B. VANBRABANT, *o.c.*, pp. 177 à 179; C. BOULANGER et S. GILSON, « L'obligation de secret du travailleur: une 'vie privée' de l'employeur? », *L'entreprise et le secret*, V. CASSIERS et S. GILSON (dirs.), Bruxelles, Larcier, 2014, pp. 121 et 122.

47. K. NACHTRAB, *o.c.*, pp. 234 et 235; R. BINNS, *o.c.*, p. 362; H. VANHEES, « De nieuwe wettelijke regeling betreffende de bescherming van bedrijfsgeheimen », *R.W.*, 2018, pp. 1642 et 1644; V. CASSIERS, « La directive 2016/943/UE du 8 juin 2016 sur les secrets d'affaires », *J.T.*, 2017, p. 389.

iv. Mesures informatiques de protection

33. L'omniprésence des technologies de l'information et la dépendance qui en résulte pour les entreprises a pour corollaire une augmentation massive d'appropriations illicites de secrets d'affaires par le biais du piratage informatique⁴⁸. Les entreprises européennes y sont particulièrement exposées et la menace est croissante, quel que soit le type et la taille de l'entreprise. Or, malgré ce constat, le niveau de sécurité informatique est généralement insuffisant, en raison d'un déficit de prise de conscience et d'information des entreprises⁴⁹. L'adoption d'un arsenal de mesures de protection de nature informatique devra donc être prioritaire et sera bien souvent nécessaire pour qu'une information confidentielle puisse être qualifiée de secret d'affaires et bénéficier du cadre juridique de protection correspondant⁵⁰.

34. Parmi les mesures informatiques à envisager, on relèvera typiquement l'utilisation de pare-feux (« *firewalls* »)⁵¹ et de logiciels antivirus (régulièrement mis à jour)⁵²; des mesures d'identification et de gestion des accès aux différents composants de l'infrastructure informatique de l'entreprise et à certaines catégories de données⁵³; l'utilisation de login et de mots de passe suffisamment sûrs pour accéder au système informatique⁵⁴; le recours à des logiciels de cryptage pour la communication d'informations particulièrement sensibles et la sécurisation de certains fichiers par l'adoption de mots de passe⁵⁵; l'encadrement, voire le blocage technique, du recours à des supports de stockage externes au sein de l'entreprise (clés USB ou disques durs)⁵⁶; le recours à des outils de traçage des téléchargements de fichiers sensibles⁵⁷; l'adoption de règles claires relatives à l'usage des équipements informatiques par le travailleur, la gestion de l'accès à distance au système de messagerie de l'entreprise et l'encadrement strict de l'utilisation d'ordinateurs privés en lien avec l'activité professionnelle du travailleur⁵⁸.

v. L'attention particulière qu'il convient de donner aux travailleurs et les bonnes pratiques à implémenter en matière de ressources humaines

35. La grande majorité des cas d'appropriation illicite de secrets d'affaires n'est pas le fait de pirates informatiques ou d'espionnage industriel organisé mais de travailleurs ou de partenaires commerciaux bien connus de l'entreprise, à qui l'information confidentielle a été volontairement communiquée et qui l'utilise ou la divulgue ensuite de façon illicite⁵⁹. La gestion des risques que représentent les travailleurs (anciens, actuels et sur le point de rejoindre l'organisation) doit ainsi être placée au centre des mesures organisationnelles, physiques, juridiques et informatiques de protection et le département des ressources humaines sera utilement associé à la protection des secrets d'affaires de l'organisation.

36. Parmi les bonnes pratiques à implémenter en la matière, la première sera d'informer correctement les travailleurs sur ce que constitue un secret d'affaires, sur leur valeur pour l'organisation et sur la nécessité et la manière de les protéger⁶⁰. Tel que précédemment relevé, il convient de définir et d'implémenter des politiques de confidentialité internes à l'entreprise qui contiennent des directives claires et de s'assurer que les travailleurs en ont pris connaissance et les ont effectivement comprises. Des formations périodiques sur la question pourront être envisagées à cette fin⁶¹.

37. Pour les nouveaux travailleurs, en particulier venant d'entreprises concurrentes, la tenue de briefings d'entrée orientés sur la protection des secrets d'affaires permettra de les sensibiliser à la stratégie de protection, tout en limitant les risques de pollution de l'entreprise par des secrets d'affaires de l'ancien employeur qui seraient illicitement divulgués⁶². Des briefings de sortie devront être organisés avec les travailleurs sur le départ pour obtenir la restitution et la destruction des informations confidentielles en leur possession et pour leur rappeler les obligations de confiden-

48. V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », *o.c.*, p. 33, n° 47.

49. COMMISSION EUROPÉENNE, *o.c.*, pp. 6 à 9.

50. V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », *o.c.*, p. 34, n° 49; CREATE.org, « The importance of Cybersecurity for trade secret protection », www.create.org/resource/importance-cybersecurity-trade-secret-protection/, 2016, p. 5.

51. R. BINNS, *o.c.*, p. 362; CREATE.org, « Protecting Trade Secrets from Cyber and Other Threats: 'Reasonable Steps' and Leading Practices », *o.c.*, p. 5.

52. CREATE.org, « Protecting Trade Secrets from Cyber and Other Threats: 'Reasonable Steps' and Leading Practices », *o.c.*, p. 5.

53. V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », *o.c.*, p. 52, n° 52; K. NACHTRAB, *o.c.*, p. 236; CREATE.org, « The importance of Cybersecurity for trade secret protection », *o.c.*, p. 7.

54. V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », *o.c.*, p. 52, n° 52.

55. K. NACHTRAB, *o.c.*, p. 236; R. BINNS, *o.c.*, p. 362; CREATE.org, « 'Reasonable Steps' to protect trade secrets: leading practices in an evolving legal landscape », *o.c.*, p. 5.

56. K. NACHTRAB, *o.c.*, p. 236; CREATE.org, « The importance of Cybersecurity for trade secret protection », *o.c.*, p. 7.

57. K. NACHTRAB, *o.c.*, p. 236; CREATE.org, « The importance of Cybersecurity for trade secret protection », *o.c.*, p. 8.

58. V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », *o.c.*, p. 32, n° 46; CREATE.org, « 'Reasonable Steps' to protect trade secrets: leading practices in an evolving legal landscape », *o.c.*, p. 5.

59. INTERNATIONAL CHAMBER OF COMMERCE (ICC), « Protecting Trade Secrets — Recent EU And US Reforms », disponible sur www.iccmex.mx/uploads/final-icc-report-protecting-trade-secrets.pdf, 2019, p. 13.

60. V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », *o.c.*, p. 32, n° 46; K. NACHTRAB, *o.c.*, p. 235.

61. R. BINNS, *o.c.*, p. 363; INTERNATIONAL CHAMBER OF COMMERCE (ICC), *o.c.*, p. 14; T. EWING et D. O'CONNEL, *o.c.*, p. 34.

62. K. NACHTRAB, *o.c.*, p. 235.

tialité auxquelles ils restent tenus après la cessation de la relation de travail⁶³.

38. Enfin, si les travailleurs sont tenus en droit belge à une obligation générale de confidentialité en vertu de l'article 17, 3°, de la loi du 3 juillet 1978 relative aux contrats de travail, il est recommandé de préciser le contenu de cette obligation en insérant une clause de confidentialité dans le contrat de travail ou dans le règlement de travail de l'entreprise⁶⁴.

c) Le caractère raisonnable des mesures de protection du secret: le devoir de diligence est fonction des circonstances propres de l'espèce

39. La définition du secret d'affaires précise que les mesures de protection du secret doivent être « raisonnables, compte tenu des circonstances »⁶⁵. L'appréciation de cette condition se fera donc *in concreto*, au terme d'un examen au cas par cas, le détenteur du secret étant tenu à une obligation de moyen (il ne doit donc pas implémenter des mesures de protection disproportionnées ou hors d'atteinte)⁶⁶.

40. La décision commentée du tribunal de l'entreprise d'Anvers du 9 mai 2019 confirme le large pouvoir d'appréciation du juge et la flexibilité qu'il convient d'adopter dans l'analyse de cette condition⁶⁷. Le demandeur avait omis de formaliser par écrit une obligation de confidentialité dans un contrat avec un prestataire de service externe, qui avait pourtant assumé un rôle clé dans son département de recherche et

développement lui donnant accès à de l'information technique hautement sensible. Le tribunal a toutefois jugé qu'il n'y avait pas de manquement au devoir de diligence de l'entreprise et s'est appuyé sur le principe plus général d'exécution de bonne foi des conventions et sur les usages propres à la fonction du défendeur pour confirmer une obligation de confidentialité à sa charge.

41. L'exigence de protection proactive du secret est donc flexible par nature: il n'existe pas de catalogue de mesures de protection à implémenter de manière uniforme et le niveau de protection attendu d'une multinationale ne sera pas équivalent à celui d'une start-up⁶⁸.

42. La flexibilité qui découle de l'absence d'un tel catalogue de mesures prédéfinies entraîne toutefois une certaine insécurité juridique et le défi que doivent relever les entreprises, quel que soit leur taille et leur secteur d'activité, est de déterminer quelles mesures raisonnables de protection adopter pour rencontrer cette condition.

43. Plusieurs critères peuvent être pris en compte pour évaluer ce caractère raisonnable, parmi lesquels figurent la nature du secret d'affaires⁶⁹, sa valeur pour l'entreprise et l'avantage commercial ou concurrentiel que le secret lui procure⁷⁰, le secteur d'activité du détenteur⁷¹, la taille de l'entreprise et les moyens techniques, financiers et humains dont elle dispose⁷², le coût des mesures de protection à implémenter et la manière dont le secret d'affaires est utilisé par l'entreprise⁷³.

E. POUR CONCLURE

44. Les entreprises utilisent aujourd'hui très largement la confidentialité comme outil de protection du résultat de leur innovation. En ce sens, l'adoption de la loi belge du 30 juillet

2018 relative à la protection des secrets d'affaires a été bien accueillie puisqu'elle a considérablement renforcé ce régime de protection.

⁶³. K. NACHTRAB, *o.c.*, p. 234; INTERNATIONAL CHAMBER OF COMMERCE (ICC), *o.c.*, p. 14.

⁶⁴. V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », *o.c.*, p. 31, n° 45; K. NACHTRAB, *o.c.*, pp. 235-236; R. BINNS, *o.c.*, pp. 363 et 364; T. EWING et D. O'CONNEL, *o.c.*, p. 34; C. BOULANGER et S. GILSON, *o.c.*, pp. 118 et s.

⁶⁵. Art. 1.17/1, 1°, CDE, inséré par la loi du 30 juillet 2018 relative à la protection des secrets d'affaires.

⁶⁶. Projet de loi secrets d'affaires, *o.c.*, p. 12; V. CASSIERS, « La transposition de la directive 2016/943/UE du 8 juin 2016 », *o.c.*, p. 277; M. VAN MEERBEECK et T. ROBRECHTS, « De Belgische wet bedrijfsgeheimen: een algemeen overzicht », *I.R.D.I.*, 2018, p. 186, n° 3; N. SOUSA et E. SILVA, « What exactly is a trade secret under the proposed directive? », *Journal of Intellectual Property Law & Practice*, 2014, p. 930, n° 11.

⁶⁷. Entr. Anvers, 9 mai 2019, A/18/3273.

⁶⁸. V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », *o.c.*, p. 36, n° 53; CREATE.org, « Protecting Trade Secrets from Cyber and Other Threats: 'Reasonable Steps' and Leading Practices », *o.c.*, p. 4; M. VAN MEERBEECK et T. ROBRECHTS, *o.c.*, p. 186, n° 17.

⁶⁹. D.W. SLABY, J.C. CHAPMAN et G.P. O'HARA, « Trade Secret Protection: An Analysis of the Concept Efforts Reasonable under the Circumstances to Maintain Secrecy », *Santa Clara Computer and High-Technology Law Journal*, 1989, p. 332.

⁷⁰. V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », *o.c.*, p. 37, n° 53; K. NACHTRAB, *o.c.*, p. 232; V. CASSIERS, « La protection des secrets d'affaires dans l'environnement numérique », *o.c.*, p. 118, n° 55; D.W. SLABY, J.C. CHAPMAN et G.P. O'HARA, *o.c.*, p. 332.

⁷¹. V. CASSIERS, « La transposition de la directive 2016/943/UE du 8 juin 2016 », *o.c.*, p. 278; K. NACHTRAB, *o.c.*, p. 232; N. SOUSA et E. SILVA, *o.c.*, p. 931.

⁷². V. CASSIERS, « Les notions clés du régime de protection des secrets d'affaires », *o.c.*, p. 37, n° 53; K. NACHTRAB, *o.c.*, p. 232; N. SOUSA et E. SILVA, *o.c.*, p. 931; D.W. SLABY, J.C. CHAPMAN et G.P. O'HARA, *o.c.*, p. 334.

⁷³. K. NACHTRAB, *o.c.*, p. 232.

45. Nous l'avons vu, le bénéfice de la nouvelle loi est toutefois soumis à l'adoption proactive de mesures de protection du secret, qui doivent être raisonnables compte tenu des circonstances. La rencontre de cette condition flexible et multiforme relèvera d'une appréciation au cas par cas, ce qui n'est pas sans entraîner une certaine insécurité juridique et il appartiendra à la jurisprudence de préciser davantage les contours de cette condition.

46. En ce sens, la décision commentée du tribunal de l'entreprise d'Anvers du 9 mai 2019 confirme le large pouvoir d'appréciation du juge et la flexibilité inhérente à l'exigence de protection du secret. Si cette décision est favorable

au détenteur de secrets d'affaires, le juge s'étant appuyé sur la fonction complétive de la bonne foi pour déduire une obligation de confidentialité à la charge du défendeur, elle ne peut toutefois occulter la nécessité pour chaque entreprise de mettre en place une gestion proactive de la confidentialité. Il s'agit en effet d'une condition essentielle de protection et d'un exercice nécessaire pour réduire les risques de voir une information confidentielle de valeur perdre le bénéfice du nouveau régime de la loi du 30 juillet 2018 et par là, d'une protection devenue essentielle pour la compétitivité, la gestion de l'innovation et la création de valeur au sein des entreprises.