Jugement LuxLeaks : un hacking en bonne et due forme, pas de protection pour les lanceurs d'alerte

Pouvez-vous imaginer pire situation que la publication dans la presse de documents confidentiels relatifs à vos clients ? Une telle situation menace quotidiennement votre société et vous mettez certainement en œuvre tous les moyens en votre possession pour protéger votre organisation. Pourtant, un paramètre essentiel vous échappe certainement encore : l'Humain. L'affaire LuxLeaks démontre une nouvelle fois que l'Humain est la première faille en matière de cybersécurité. Le jugement du Tribunal d'Arrondissement de Luxembourg en date du 29 juin dernier est l'occasion d'aborder la fuite d'informations sous l'angle juridique.

L'affaire a été relayée par nombre de médias, les faits en sont simples : deux salariés ont subtilisé des fichiers informatiques confidentiels à leur employeur et les ont transmis à un journaliste, qui les a ensuite publiés.

Il est toutefois intéressant de s'arrêter sur les *modi operandi* des deux prévenus. Le premier a copié sur l'ordinateur portable mis à sa disposition par son employeur plus de 45.000 pages de documents confidentiels et les a ensuite recopiés chez lui sur le disque dur de son ordinateur personnel. Le second a quant à lui créé une boîte mail, y a laissé les documents confidentiels attachés à un brouillon puis a transmis le mot de passe au journaliste, ce qui a permis à ce dernier d'y accéder et de récupérer les documents attachés.

Des mesures de sécurité simples, tels que le blocage des sites de messagerie personnelle ou la désactivation des ports USB, doivent être mises en œuvre au sein de vos organisations afin d'éviter ce type de mésaventures. Sur la base de ces faits, le Tribunal d'Arrondissement de Luxembourg a retenu que les deux anciens salariés ont notamment commis les infractions de vol domestique, de fraude informatique, de vol, de violation du secret professionnel et du secret d'affaires.

Vol domestique

Le vol domestique exige, pour être constitué, la réunion cumulative des éléments suivants : (i) la soustraction d'une chose, (ii) une chose mobilière, (iii) une soustraction frauduleuse, (iv) une chose soustraite qui n'appartient pas à celui qui la soustrait et (v) l'auteur du fait doit se trouver dans un cas de figure prévu par l'article 464 du Code pénal.

La condition de soustraction d'une chose mobilière est délicate dans le contexte informatique. Les tribunaux luxembourgeois ont, à plusieurs reprises, affirmé que l'infraction de vol ne saurait porter sur des biens incorporels. Le Tribunal d'Arrondis-sement n'a pas retenu cette analyse, se fondant sur un arrêt de cassation du 3 avril 2014 ayant considéré «*que le salarié qui prend, à des fins personnelles, à l'insu et contre le gré du propriétaire, des photocopies de documents appartenant à son employeur et dont il n'a que la détention précaire, fait un acte d'appréhension desdits documents, caractérisant l'élément matériel du vol*».

Le Tribunal correctionnel a considéré en l'espèce que, au vu des actes des deux anciens salariés, l'élément matériel de l'infraction était établi. De même, l'élément intentionnel a été retenu puisque les deux prévenus ont agi en parfaite connaissance de cause. La qualification aggravante de vol «domestique» a également été retenue puisque les prévenus n'étaient en possession des documents soustraits qu'au vu de leur qualité d'employé.

Le vol domestique est sanctionné au Luxembourg d'une peine d'emprisonnement de 3 mois à 5 ans et d'une amende de 251 à 5.000 euros.

Fraude informatique

Outre le vol domestique, le Tribunal a également apprécié si les conditions de l'article 509-1 du Code pénal étaient réunies, disposition réprimant l'accès ou le maintien frauduleux dans tout ou partie d'un système informatique.

Le Tribunal a considéré que, dans le cas du premier salarié, l'accès non autorisé avait été uniquement possible à cause d'une spécificité informatique du système mis en place, ce qui constitue une fraude informatique. Quant au second salarié, l'infraction a également été retenue dans la mesure où celui-ci n'avait aucun droit d'accéder aux déclarations fiscales des clients de son employeur et de les attacher à un brouillon de courriel. Sur ce fondement, les prévenus étaient passibles de peines d'emprisonnement de 2 mois à 2 ans et d'une amende de 500 euros à 25.000 euros (ou de l'une de ces deux peines).

Violation du secret d'affaires

L'article 309 alinéa 1er du Code pénal incrimine celui qui, étant ou ayant été employé, soit dans un but de concurrence, soit dans l'intention de nuire à son patron, soit pour se procurer un avantage illicite, utilise ou divulgue, pendant la durée de son engagement ou endéans les deux ans qui en suivent l'expiration, les secrets d'affaires ou de fabrication dont il a eu connaissance par suite de sa situation.

Ici également, le Tribunal a constaté que l'infraction était constituée puisque (i) les informations dévoilées étaient des secrets d'affaires dans la mesure où elles n'étaient connues que d'un cercle limité de personnes et étaient essentielles pour prospérer dans l'activité commerciale, (ii) la divulgation de ces données a porté atteinte à l'employeur et (iii) les prévenus connaissaient la confidentialité de ces documents et leur démarche avait pour but de nuire à leur ancien employeur. Au titre de cette infraction, les prévenus encourraient un emprisonnement de 3 mois à 3 ans et une amende de 251 euros à 12.500 euros.

Violation du secret professionnel

L'application de l'article 458 du Code pénal a également été analysée par les juges. Aux termes de cette disposition sont sanctionnées les personnes dépositaires, par état ou par profession, des secrets qu'on leur confie, qui, hors le cas où ils sont appelés à rendre témoignage en justice et celui où la loi les oblige à faire connaître ces secrets, les auront révélés.

Les juges ont ici aussi retenu la violation du secret professionnel, considérant que les prévenus étaient soumis au secret professionnel, le savaient et ont, en connaissance de cause et librement, révélé des informations confidentielles. Une telle infraction est sanctionnée par un emprisonnement de 8 jours à 6 mois et une amende de 500 euros à 5.000 euros.

Rejet de faits justificatifs

L'un des prévenus a argué de l'état de nécessité et du statut de lanceur d'alerte, sans succès. Sur l'état de nécessité, il a ainsi été avancé que le prévenu pouvait bénéficier de l'état de nécessité dans la mesure où la commission des infractions susmentionnées était légitime «*eu égard à une valeur largement supérieure et fondamentale, soit l'intérêt général d'un bien public, soit celui des contribuables européens*».

Ce fait justificatif, qui pour être retenu par les tribunaux doit répondre à certaines conditions strictes, n'a pas été accueilli par les juges. Il a en effet été considéré que le prévenu ne faisait pas face à un péril imminent et avait d'autres choix. Au titre de ces choix, le Tribunal a notamment énoncé la divulgation d'informations sans soustraction de documents (ce qui semble néanmoins constituer une violation du secret professionnel et/ou de secrets d'affaires) ou la remise au journaliste d'un nombre restreint de documents (ce qui ne change *a priori* par la qualification des infractions susmentionnées).

Quant au fait justificatif du lanceur d'alerte, le Tribunal a constaté que le prévenu ne bénéficie, pour les faits qui lui sont reprochés, d'aucune protection en droit luxembourgeois. En droit européen, le constat est le même. Le Tribunal évoque à cet égard la directive sur le secret d'affaires qui entend resserrer le cadre de la protection des lanceurs d'alerte en limitant la protection pour l'exercice de la liberté d'expression et d'information, la révélation d'une faute, d'un acte répréhensible ou d'une activité illégale ou aux fins de protection d'un intérêt légitime reconnu par le droit de l'Union ou le droit national (art. 5 de la Directive 2016/943 du 8 juin 2016).

Cette directive, qui n'a pour l'instant pas encore été transposée en droit luxembourgeois mais doit servir de grille de lecture aux prétoires pendant le délai de transposition jusqu'au 9 juin 2018, n'aurait donc *a priori* pas non plus offert l'impunité aux prévenus de l'affaire LuxLeaks. A ce sujet, il est intéressant de se tourner vers la France, où le projet de loi Sapin II - actuellement en débat - prévoit l'introduction d'une protection des lanceurs d'alerte. Le projet initial a toutefois été amendé par le Sénat et est l'objet d'âpres discussions.

Enfin, le Tribunal a également rejeté le moyen tiré de l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales protégeant la liberté d'expression. Les juges ont en effet considéré que le prévenu aurait parfaitement pu critiquer les pratiques d'optimisation fiscale «*moralement douteuses*» au Luxembourg et ailleurs, et a dépassé les limites de la critique en soustrayant à son employeur des milliers de pages de documents confidentiels pour les transmettre ensuite à un journaliste. Dans la mesure où le prévenu - qui était tenu d'un devoir de loyauté, de réserve et de discrétion envers son employeur - n'a pas dénoncé des conduites ou des actes illicites, il ne peut bénéficier de cette protection.

De lourdes peines … inappliquées !

Dans le cas présent, plusieurs infractions ont été constatées par le Tribunal. Lorsque le même fait constitue plusieurs infractions, le Code pénal prévoit que seule la peine la plus forte sera prononcée, peine qui peut même être élevée au double du maximum, sans toutefois pouvoir excéder la somme des peines prévues pour les différents délits. La peine la plus forte en l'espèce était celle prévue en cas de vol domestique : 3 mois à 5 ans d'emprisonnement et 251 à 12.500 euros d'amende. Les juges n'ont pas fait application des peines maximales, bien au contraire…

Après avoir constaté que la gravité des infractions retenues à charge des deux prévenus est indéniable, le Tribunal a pris en compte le fait que (i) les prévenus n'avaient pas été rémunérés pour avoir transmis au journaliste les documents confidentiels soustraits et que (ii) suite aux révélations «LUX-LEAKS» et leur impact politique mondial important, les prévenus ont contribué à une plus grande transparence et équité fiscale.

Considérant que les deux prévenus avaient agi «*dans l'intérêt général et contre des pratiques d'optimisation fiscale moralement douteuses*», le Tribunal d'Arrondissement a condamné les deux prévenus à des peines très allégées. Le premier a écopé d'une peine d'emprisonnement de 12 mois avec sursis et d'une amende de 1.500 euros, le second d'une peine d'emprisonnement de 9 mois avec sursis et d'une amende de 1.000 euros. Ils ont en outre été condamnés solidairement à payer à leur ancien employeur 1 euro symbolique au titre du préjudice moral.

Les peines prononcées sont donc extrêmement douces au regard de ce que les deux prévenus encouraient. Se pose la question de l'impact des médias sur l'appréciation des juges. Comme l'a indiqué la Cour européenne des droits de l'homme dans son arrêt Worm c. Autriche du 29 août 1997, «*si l'on s'habitue au spectacle de pseudo-procès dans les médias, il peut en résulter à long terme des conséquences néfastes à la reconnaissance des tribunaux comme les organes qualifiés pour juger de la culpabilité ou de l'innocence quant à une accusation pénale*». Appartenait-il au Tribunal d'Arrondissement de juger les infractions commises à la lumière de leurs conséquences dans la sphère politico-médiatique ? Le pouvoir d'appréciation du juge pénal est en l'espèce allé très loin, trop loin ? C'est ce qu'il appartiendra à la Cour d'Appel de trancher, un appel ayant été interjeté par les deux anciens salariés, ces derniers considérant avoir été reconnus coupables à tort. Affaire à suivre…

Vincent WELLENS (cf. portrait)
Avocat à la Cour
Partner NautaDutilh Avocats Luxembourg S.à r.l.
vincent.wellens@nautadutilh.com

Anne-Sophie MORVAN
Avocat au Barreau de Paris (Liste IV)
Associate NautaDutilh Avocats Luxembourg S.à r.l.
annesophie.morvan@nautadutilh.com

A Few Quotes on Fintech at the General Meeting of the Belgian Association of Stock Exchange Members (BASEM)

Chaired by Umberto Arts, executive committee member at KBC Securities, the Belgian Association of Stock Exchange Members (BASEM) organized a debate on «The Threats and Opportunities of the Global Digitalization on the Ecosystem of Investment Firms», presented by Paul Huybrechts, former general manager of Belgian financial daily De Tijd and chairman of the Vlaamse Federatie van Beleggers (the Flemish association of investors).

Agefi Luxembourg editor, Adelin Remy who is also a member of BASEM, grasped a few interesting quotes:

- "While the tech-savvy millennial generation is the initial target for automated investment advice, we believe there is a much broader, and in some cases untapped, market for these firms, given their ability to deliver a cost-effective solution direct-to-consumer…. Furthermore, the **greatest wealth transfer in history** is currently underway and will continue over the next decades as baby boomers pass along wealth to their heirs, creating more pressure on the traditional model." (EY, «Advice Goes Virtual», Winter 2015).

- "New uses of data analytics span the spectrum from institutional trading and risk management to small notional retail wealth management. The increased sophistication of data analytics is reducing the asymmetry of information between small- and large-scale financial institutions and investors, with the latter taking advantage of automated financial services solutions. Sophisticated analytics also uses advanced trading and risk management approaches such as behavioral and predictive algorithms, enabling the analysis of all transactions in real time." (PwC, «Blurred Lines», March 2016).

- Frictionless trading. Smart algorithms that are increasingly better at predicting the behaviors of markets and humans will not only become more common but more powerful. With sufficient investment in the technology infrastructure, these trading machines will be capable of analyzing risk in real time and in a holistic fashion, fully leveraging both institutional knowledge and external data sets. …There are only a few barriers for real-time trading even now, but **clearing will take** a few years; while for settlement, **T+2** will happen **by end of 2017**, and T+1 possibly in about 10 years. **Blockchain** will change that…" (Deloitte, «Banking Reimagined», Outlook 2016);

- "Accenture recently released a study of 24,489 customers in 33 countries and across 11 industries. According to that research: 83% of U.S. consumers prefer dealing with human beings. 65% agree in-store service is the best channel for personalized experiences. Clearly, technology will have a continually important role in service delivery, as evidenced by Accenture's finding that 73% of study participants expect customer service to be easier and more convenient, and 61% expect it to be faster. In essence, **the more machines resemble humans the less acceptable those machines become to us.**";

- "Fintech may not be as aware of regulation," says Moven CEO Brett King, "until they get slapped down by it." Fintech appears to understand this—and to accept the future need for experience in managing risk and maintaining regulatory compliance. "**A Fintech** that competes head on with banks **needs a compliance and regulatory team bigger** than any other division in the company" according to Erik Engellau-Nilsson, marketing director for the Swedish start-up Klarna.

"Trust for new organisations does not occur at the speed of technology"_says Eugene Danilkis, co-founder and CEO of Germany-based Mambu, a cloudbased alternative to traditional banking platforms. "**You can build technology in a year or two but trust takes as long as human behaviour requires**." Fintech will be challenged to gain customer trust as they move beyond the early adopters.

We expect to see many of the same banking names in 5-10 years, but the way we receive banking services will have shifted. As is the case in so many disruptive events, **the winner will be the consumer, who will receive lower prices, more innovative products and better service** in a transformed banking world. (The Economist Intelligence Unit, June 2015).

- "We always **overestimate** the change that will occur in the next **two** years and **underestimate** the change that will occur in the next **ten**. Don't let yourself be lulled into **inaction**." (Bill Gates)