Outsourcing

Vers un encadrement légal plus rigoureux de l'externalisation IT

La transformation digitale et la crise actuelle poussent les acteurs du secteur financier vers une externalisation plus prononcée de la fonction IT. Déjà strictement encadrée au Luxembourg, l'externalisation IT a fait l'objet d'initiatives récentes qui instaurent, au niveau de l'UE, des règles allant au-delà de celles actuellement en vigueur.

Le secret bancaire au Luxembourg

Historiquement, la réglementation sur l'externalisation IT au Luxembourg était axée sur le principe sacro-saint du secret professionnel (ou «secret bancaire»), qui était ancré dans la loi de 1993 sur le secteur financier, et que l'on retrouve également dans le secteur des assurances et des services de paiement. Ce cadre visait avant tout à préserver la confidentialité des données des clients bancaires, interdisant les externalisations qui donneraient lieu à une divulgation de données en dehors du territoire national. Cette réglementation fut renforcée en 2003 par la création des professionnels du secteur financier (PSF) de support IT, ces professionnels pouvant se voir confier par les institutions de crédit et d'autres acteurs du secteur financier certaines fonctions IT sans violer le secret professionnel.

Le changement du focus réglementaire vers le principe de bonne gouvernance

Même si le secret professionnel reste toujours important au Luxembourg, plusieurs exceptions y ont été prévues au fil du temps, notamment concernant l'externalisation. Après une flexibilisation progressive de la position de la CSSF, un changement de la loi en 2018 a explicitement introduit une exception permettant aux institutions du secteur financier d'externaliser sur la base du consentement de leurs clients. Le centre de gravité de la réglementation CSSF s'est déplacé du respect du secret professionnel vers les principes réglementaires de l'administration centrale et de bonne gouvernance. Une attention particulière est portée à la prise de décision responsable basée sur une politique d'externalisation prédéfinie et une analyse des risques, ainsi qu'au contrôle que l'institution financière doit exercer sur les activités et la chaîne de sous-traitance. Ce basculement est aussi visible dans la circulaire CSSF de 2017 sur l'externalisation IT basée sur une infrastructure *cloud* qui met en avant l'*accountability* en introduisant l'obligation de tenir un registre des externalisations basées sur le *cloud* et la nécessité de pouvoir changer de prestataire si nécessaire.

Le modèle luxembourgeois repris à l'échelle européenne

L'Autorité bancaire européenne (ABE) a établi en 2019 des lignes directrices pour des institutions de crédit, des entreprises d'investissement et des prestataires de paiement. Elles concernent tous types d'externalisation et établissent des règles très strictes sur la prise de décision et la gouvernance des opérations d'externalisation. Ainsi, l'ABE a instauré une réglementation se rapprochant de celle de la CSSF, mais plus précise sur certains points, ou allant au-delà des règles du régulateur luxembourgeois. L'ABE a ainsi créé un *level playing field* entre les acteurs locaux et les acteurs dans le reste de l'UE, qui étaient souvent soumis à un régime moins strict. L'Autorité européenne des assurances et des pensions professionnelles et l'Autorité européenne des marchés financiers ont très récemment adopté des lignes directrices qui sont, malheureusement, limitées au *cloud*.

> «Le secret professionnel reste toujours important au Luxembourg.»

Même si la CSSF s'attend à ce que les institutions financières concernées se conforment déjà aux règles de l'ABE, elle adoptera sous peu une nouvelle circulaire, consolidant ses règles en la matière, basée sur les lignes directrices de l'ABE, tout en maintenant les spécificités locales résultant de sa circulaire *cloud* et en étendant sa circulaire aux sociétés de gestion dans le domaine des fonds.

Vers une réglementation au sein de l'UE qui aborde l'IT de manière plus holistique

Entre-temps, l'ABE a également établi des exigences relatives à la gestion des risques liés aux technologies de l'information et à la sécurité. Via sa circulaire 20/750, la CSSF a étendu ces exigences à tous les professionnels au sens de la loi de 1993 sur le secteur financier et de la loi de 2009 sur les services de paiement. Ces exigences doivent être prises en compte lorsque les institutions financières externalisent des fonctions IT, voire lorsqu'elles s'appuient sur une infrastructure ou une solution *cloud*.

La Commission européenne vient de publier une proposition de règlement sur la résilience opérationnelle digitale dans le secteur financier au sens large. La proposition consolidera les règles de gestion de risques IT et de sécurité et en introduira de nouvelles, le tout dans l'objectif d'assurer, d'une manière plus holistique, la résilience IT. Ces règles concernent, entre autres, la gestion des prestataires tiers de services IT (donc également des services qui ne constituent pas une externalisation au sens strict du terme!). La plupart des acteurs du secteur financier au Luxembourg pourront s'y conformer rapidement, car ces règles se rapprochent de celles de la CSSF et de l'ABE (même s'il y a évidemment quelques différences). Nous prévoyons le plus de difficultés pour les sociétés de gestion dont la gestion des risques IT n'a pas été extensivement réglementée jusqu'à présent. *Last but not least*, la proposition prévoit aussi de réglementer directement des prestataires «critiques» ayant une importance systémique dans le secteur financier, tels que les Amazon Web Services et Microsoft. ▬

VINCENT WELLENS
Partner, IP/ICT
NautaDutilh Avocats Luxembourg

Photo → NautaDutilh Avocats Luxembourg