



Réponse du ministre de l'Économie, des PME, de l'Énergie et du Tourisme, Lex Delles, à la question parlementaire n°3811 du 20 mars 2026 de l'honorable député Ben Polidori au sujet de la Cybersécurité des ascenseurs au Luxembourg

Le gouvernement dispose-t-il de statistiques relatives au niveau de cybersécurité des ascenseurs installés au Luxembourg, tant dans les bâtiments résidentiels que tertiaires ou publics ?

Le gouvernement ne dispose pas de statistiques relatives au niveau de cybersécurité des ascenseurs installés au Luxembourg.

Des incidents ou tentatives d'intrusion informatique visant des systèmes d'ascenseurs ont-ils été recensés au Grand-Duché au cours des dernières années ?

Le gouvernement n'a recensé aucun incident ni tentative d'intrusion informatique visant des systèmes d'ascenseurs.

Le gouvernement envisage-t-il de renforcer les normes techniques, les exigences de certification ou les mécanismes de surveillance dans ce domaine afin de prévenir d'éventuels risques pour la sécurité des usagers et le bon fonctionnement des infrastructures ?

La sécurité des usagers et la résilience des infrastructures constituent une priorité pour le gouvernement. Dans ce contexte, l'ILNAS, en tant qu'autorité de surveillance du marché, suit de très près les évolutions réglementaires européennes en matière de cybersécurité des produits connectés et participe activement à leur mise en œuvre au niveau national. Deux législations européennes majeures renforceront de manière significative le cadre applicable dans les prochaines années :

- Cyber Resilience Act (CRA) : Le règlement (UE) 2024/2847 introduit des exigences de cybersécurité harmonisées pour un large éventail de produits comportant des éléments numériques, y compris potentiellement certains systèmes d'ascenseurs connectés. Les obligations de surveillance du marché seront applicables à partir de décembre 2027. Le gouvernement prépare actuellement, sous la coordination du ministère de l'Économie, un projet de loi visant à désigner les autorités compétentes et à organiser la mise en œuvre nationale du CRA. Ce cadre permettra de renforcer les exigences de sécurité et les mécanismes de contrôle, tout en assurant une cohérence avec les pratiques européennes.
- Règlement européen sur l'intelligence artificielle (AI Act) : Le règlement (UE) 2024/1689 établit un cadre pour les systèmes d'IA à haut risque. Certains composants intégrés dans des infrastructures critiques, comme les ascenseurs, pourraient relever de ce cadre lorsqu'ils remplissent des fonctions essentielles à la sécurité. La mise en œuvre nationale de ce règlement est en cours de préparation sous la coordination de la Commission nationale pour la protection des données (CNPD), désignée comme autorité principale. L'ILNAS fera partie des autorités impliquées dans la surveillance du marché des systèmes d'IA à haut risque, dont l'application est prévue à partir d'août 2027.



À travers ces initiatives, le gouvernement confirme sa volonté d'adopter un cadre réglementaire robuste, aligné sur les standards européens, afin de garantir un niveau élevé de sécurité et de confiance pour les usagers.

Une coopération est-elle envisagée au niveau européen pour renforcer les standards de cybersécurité applicables aux ascenseurs et autres équipements connectés relevant de la sécurité des bâtiments ?

La coopération européenne constitue un pilier essentiel de la stratégie luxembourgeoise en matière de cybersécurité. Les équipements connectés, y compris ceux utilisés dans les bâtiments, font déjà l'objet d'une coordination étroite entre les États membres et la Commission européenne. Les règlements CRA et AI Act ont précisément pour objectif d'établir des exigences harmonisées dans toute l'Union européenne, afin d'assurer un niveau élevé et uniforme de cybersécurité. Ils prévoient également des mécanismes renforcés de coopération entre autorités nationales, facilitant l'échange d'informations, la coordination des contrôles et la gestion des risques émergents.

Par ailleurs, la Commission européenne a mandaté les organismes européens de normalisation (CEN, CENELEC et ETSI) pour élaborer les normes techniques nécessaires à la mise en œuvre de ces règlements. En tant qu'organisme national de normalisation et membre de ces organisations, l'ILNAS permet aux acteurs luxembourgeois de participer gratuitement aux travaux de normalisation, afin de défendre les intérêts nationaux et d'anticiper les évolutions réglementaires. Ainsi, le Luxembourg s'inscrit pleinement dans la dynamique européenne visant à renforcer la cybersécurité des équipements connectés et à garantir la sécurité des infrastructures au bénéfice de tous les usagers.

Luxembourg, le 13/04/2026

Le Ministre de l'Économie, des PME, de
l'Énergie et du Tourisme

(s.) Lex Delles