

ASSEMBLÉE NATIONALE

27 octobre 2022

D'ORIENTATION ET DE PROGRAMMATION DU MINISTÈRE DE L'INTÉRIEUR - (N° 343)

Tombé

AMENDEMENT

N ° CL250

présenté par

M. Rimane, Mme Faucillon, Mme K/Bidi, Mme Bourouaha, M. Brotherson, M. Castor,
M. Chailloux, M. Chassaigne, M. Dharréville, M. Jumel, M. Le Gayic, Mme Lebon, M. Lecoq,
M. Maillot, M. Monnet, M. Nadeau, M. Peu, M. Roussel, M. Sansu, M. Tellier, M. William et
M. Wulfranc

ARTICLE 4

À l'alinéa 4, substituer aux mots :

« 24 heures »

les mots :

« quinze jours ».

EXPOSÉ SOMMAIRE

En 2020, chaque individu a produit 1,7 Mo de données par seconde. Et 90 % des données disponibles sur Internet ont été créées au cours des deux dernières années.

Cette tendance massive à la digitalisation de notre société, accélérée par l'augmentation du télétravail, a pour conséquence logique l'accroissement des risques cyber.

Toutefois, le manque de sensibilisation à ces risques, l'absence de maîtrise des systèmes d'information, le non-respect des mesures d'hygiène informatique, la pénurie d'experts en cybersécurité et l'augmentation de la surface d'attaque du fait de la généralisation du télétravail, sont autant de faiblesses exploitées par les cybercriminels que de raisons ne pas pénaliser les victimes en les soumettant à un délai lilliputien qui conditionnera leur capacité à être protégées.

À titre d'exemples :

- En décembre 2021, l'étude "Les Français et les risques numériques" menée par Harris Interactive pour Assurance Prévention, dévoilait que 51 % des Français s'estimaient mal informés sur ces risques cyber et méconnaissaient les mesures permettant de les limiter.

- En décembre 2021 toujours, l'enquête "Les TPE / PME et la cybersécurité" menée par l'Ifop indiquait que seule un tiers des TPE/PME déclaraient avoir un spécialiste informatique en charge de la cybersécurité dans leur entreprise, signe d'un enjeu encore peu mature.

C'est pourquoi, si la procédure de pré-plainte devait initialement permettre aux victimes de bénéficier d'un gain de temps en effectuant une pré-déclaration en ligne qu'il faudra ensuite simplement venir signer au commissariat pour qu'elle soit enregistrée en plainte, la temporalité de mise en oeuvre de cette déclaration ne nous semble pas adaptée.

Face à des cyber-risques encore relativement nouveaux, le manque d'acculturation de la population, l'inaptitude d'une partie d'entre elle à utiliser les outils numériques du quotidien (en 2019, 17 % de la population se trouve en situation d'illectronisme, selon l'INSEE) ainsi que le manque de cyber-robustesse des entreprises françaises (et plus particulièrement des TPE, PME et ETI), le délai imposé de 24 heures est une pression supplémentaire qui risque de laisser sur le bord de la route une partie des victimes et d'en décourager une autre de s'emparer du dispositif, alors même qu'ils cotisent pour bénéficier d'une assurance.

Face à une contrainte temporelle excessivement restreinte, et alors qu'il arrive bien souvent que l'attaque ait été lancée bien avant sa découverte, cet amendement vise ainsi à augmenter le délai laissé aux assurés pour justifier du dépôt d'une plainte pour éviter de pénaliser trop fortement les victimes, qui sont par ailleurs souvent des petites entreprises ou des administrations publiques.