



Politique de filtrage Internet pour les établissements de la scolarité obligatoire et du secondaire II

1. Préambule

Internet et les technologies de l'information et de la communication sont devenues incontournables dans le cadre scolaire et leur usage est porteur d'une potentielle plus-value pédagogique.

Cependant, la facilité d'accès à une multiplicité de sites pouvant présenter un contenu préjudiciable, voire illégal, pour les élèves mineurs, les étudiants, les apprentis (ci-après les élèves) ou l'ensemble de la communauté éducative, pose le problème de la maîtrise de l'outil dans un contexte pédagogique.

Aussi, afin de permettre aux enseignants de développer sereinement les usages et de mettre en œuvre une protection des élèves vis-à-vis des contenus illicites ou inappropriés, le Département de l'économie et de la formation (ci-après : le Département) demande aux établissements de la scolarité valaisanne d'être équipés d'un outil de filtrage des contenus Web et de promouvoir un usage responsable des accès à Internet.

2. Filtrage

Les établissements doivent disposer d'une solution technique professionnelle de filtrage des connexions Internet, permettant de garantir, a minima, le blocage des catégories de contenus définies ci-dessous :

2.1 **Pornographie, érotisme et nudité**

Appartiennent à cette catégorie, les sites Web à caractère pornographique, les contenus montrant une activité sexuelle explicite, ainsi que les sites orientés sexuellement ou érotiques avec nudité partielle ou intégrale.

2.2 **Activités criminelles**

Appartiennent à cette catégorie, les sites Web, dont les données sont du domaine des activités illégales ou criminelles (appels ou conseils au meurtre, au suicide, au sabotage, à la fabrication de bombes, au cambriolage ou au vol, ...) ou diffusant des données illégales, tout comme les sites Web se rendant coupables, encourageant ou permettant directement la tromperie ou la fraude des consommateurs.

2.3 **Haine et Discrimination**

Appartiennent à cette catégorie, les sites Web appelant directement ou implicitement à la discrimination ou à l'exclusion d'un certain groupe de personnes par la diffusion d'avis se référant à la race, à la religion, à la nationalité, au genre, à l'âge, à un handicap ou à une orientation sexuelle, ainsi que les sites Web défendant de tels contenus.

2.4 **Sectes**

Appartiennent à cette catégorie, les sites Web avec un contenu relatif à des sectes ou mouvements sectaires et potentiellement dangereux, comme le satanisme, l'occultisme, etc.

2.5 Drogues et stupéfiants

Appartiennent à cette catégorie, les sites Web avec des informations sur la culture, la vente, l'utilisation et la consommation de drogues, de stupéfiants, de médicaments et substances psychotropes ou en lien avec l'atteinte à la santé personnelle (scarification, boulimie, anorexie, comportements sexuels).

2.6 Violence

Appartiennent à cette catégorie, les sites Web avec différents types de représentations de violence, les images et les textes réels ou proches du réel montrant, décrivant et glorifiant des actes de violence, de torture ou de cruauté sont inclus dans cette catégorie. La violence peut se diriger envers les hommes, les femmes, les enfants, les animaux, les choses ou les institutions et peut également comprendre la représentation et la glorification de la mort, du terrorisme et de la guerre.

2.7 Contenus choquants

Appartiennent à cette catégorie, les sites Web contenant des données de mauvais goût, choquantes ou cruelles, notamment les plaisanteries de mauvais goût, les illustrations ou les photos par exemple d'excréments, d'accidents, d'opérations médicales, ou même des bijoux étranges pour le corps et également la description ou l'illustration de mauvais traitements sur les animaux.

2.8 Jeux d'argent

Appartiennent à cette catégorie, les sites Web contenant des informations sur les jeux d'argent, les jeux de hasard, les loteries et les sociétés de paris, ainsi que des sites proposant de jouer en ligne.

2.9 Criminalité informatique et piratage

Appartiennent à cette catégorie, les sites Web contenant des instructions pour la manipulation d'appareils électroniques, de réseaux de données, de décryptage de mots de passe, des manuels pour la programmation de virus et de logiciels potentiellement dangereux, ainsi que les sites proposant le téléchargement de contenus illégaux.

2.10 Contournement du filtrage

Appartiennent à cette catégorie, les sites Web proposant des solutions de contournement des limitations définies par les filtres et autres moyens de sécurisation de l'Internet et des outils informatiques, ainsi que les dispositifs proposant de surfer anonymement notamment via proxy, TOR.

2.11 Réseaux sociaux

L'accès aux réseaux sociaux est bloqué, à moins que celui-ci soit absolument nécessaire à la formation dispensée. Le cas échéant, l'enseignant formulera, au préalable, une requête écrite d'accès auprès de la Direction d'établissement.

Remarques :

Le Département se réserve le droit de mettre à jour ces catégories en tenant compte de l'évolution du contenu présent sur le Web.

3. Usage responsable

Aussi performant soit-il, chaque dispositif de filtrage comprend des limites et doit s'accompagner d'un usage responsable d'Internet. C'est pourquoi un règlement d'usage fixe les grands principes et informe des comportements à adopter.

En cas de doute, il convient de s'adresser au Centre de compétences ICT-VS du Département.

4. Considérations techniques

Lorsqu'un site inapproprié (par exemple jeux dangereux) est signalé comme accessible malgré l'application des filtres mis en place, un dispositif doit permettre de l'exclure spécifiquement et rapidement. De même, lorsqu'un site présente un intérêt pédagogique et est indûment bloqué, un dispositif doit permettre d'en libérer l'accès, après vérification et validation de la Direction.

De plus, la part du trafic qui utilise un cryptage de l'appel et des contenus de l'accès Internet (https) ne cesse d'augmenter et ce trafic crypté doit également faire l'objet d'une surveillance et d'un filtrage adéquat dans le respect de la présente politique.

Pour ce faire, le filtrage et la protection contre les logiciels malveillants exigent que les requêtes sur Internet soient traitées à l'aide d'une inspection SSL, à savoir décryptage - inspection – recryptage, afin de permettre le blocage des contenus indésirables.

5. Responsabilité des établissements

Les établissements de la scolarité obligatoire et du secondaire II sont rendus attentifs au fait que le respect des minima, fixés dans le présent document, ne leur garantit pas la conformité légale, le respect de celle-ci leur incombant.

De surcroît, des décisions judiciaires concrétisant d'avantage les dispositifs de filtrage à mettre en place pourraient également accroître les exigences quant au niveau de protection requis, de sorte qu'un réexamen régulier de la conformité est conseillé. Le principe de précaution doit donc trouver application et en cas de doute l'accès au contenu doit être purement et simplement prohibé.

Les violations des obligations figurant dans la présente Politique de filtrage Internet pourront faire l'objet de procédures judiciaires et/ou de mesures administratives.

Ce document annule et remplace la Politique de filtrage Internet pour les établissements scolaires valaisans du 29 juin 2012. Il entre en vigueur le 17 août 2020.

Sion, le 25 août 2020



Christophe Darbellay
Conseiller d'Etat