

Les cinq failles de filtrage.

Si les jeunes enfants sont aujourd'hui bien protégés par l'intermédiaire des contrôles parentaux associés à des listes blanches, il en va tout autrement dans le cas de profils adolescents. Ces derniers sont en effet exposés à la porno-pédophilie, voire même à la pédophilie tout court, via un certain nombre de failles de filtrage.

Cinq grandes failles de filtrage peuvent être identifiées : les sites pédopornographiques, les sites incitant à la pédophilie, les sites communautaires et web 2.0, les contacts directs par email ou messageries instantanées et les réseaux sociaux.

Les sites pédopornographiques sont accessibles directement depuis un navigateur, généralement à partir d'une requête ambiguë sur un moteur de recherche. Il est très facile de bloquer de façon ad hoc ces sites via une liste noire contenant le nom et l'adresse IP du site. L'efficacité réelle de ce blocage restant soumise aux conditions énumérées plus haut.

Les sites incitant à la pédophilie sont particulièrement pernicious, leur but étant de convaincre les préadolescents et les jeunes ados que la pédophilie est une activité normale voire épanouissante. Ils invoquent pour cela la tradition grecque et/ou les idéaux détournés de 1968. Ils sont extrêmement difficiles à détecter car ils nécessitent des techniques d'exploration de sites via des modules d'intelligence artificielle et d'analyse sémantique extrêmement avancés. Comme pour la mise à jour des listes noires, le développement de ce type de module est également hors de portée d'une instance régulatrice.

La prise de contact d'un pédophile avec un adolescent via **des sites communautaires et web 2.0** est impossible à détecter en utilisant des listes noires, sauf à bloquer l'intégralité de ces sites. En effet, les pédophiles excellent à se faire passer pour des adolescents et tentent d'obtenir des informations permettant un contact. Le seul moyen fiable est ici d'empêcher l'adolescent de communiquer des informations confidentielles (email, contact de messageries instantanées, téléphone, adresse postale, etc.). Ce type de contrôle ne peut être réalisé que sur l'ordinateur final.

La sécurisation des informations confidentielles n'empêche pas le contact par l'intermédiaire d'un tiers non sécurisé, typiquement un ami mettant le contact à disposition. Le seul moyen est ici de limiter **les contacts directs par email ou messageries instantanées** à des contacts sûrs. Ceci ne peut être effectué qu'au niveau de l'ordinateur final et pour chaque individu utilisateur.

Les réseaux sociaux où le pédophile peut se faire passer pour un adolescent. La seule protection possible consiste ici aussi à limiter les échanges à des contacts sûrs. Compte tenu du fait que les réseaux sociaux sont la plupart du temps accédés depuis un navigateur, cela suppose des techniques extrêmement lourdes d'analyse dédiées à chaque réseau social. Ces techniques ne peuvent être mise en place que sur l'ordinateur final. Elles supposent également une veille permanente pour adapter les programmes de détection lorsque le réseau social change sa présentation.