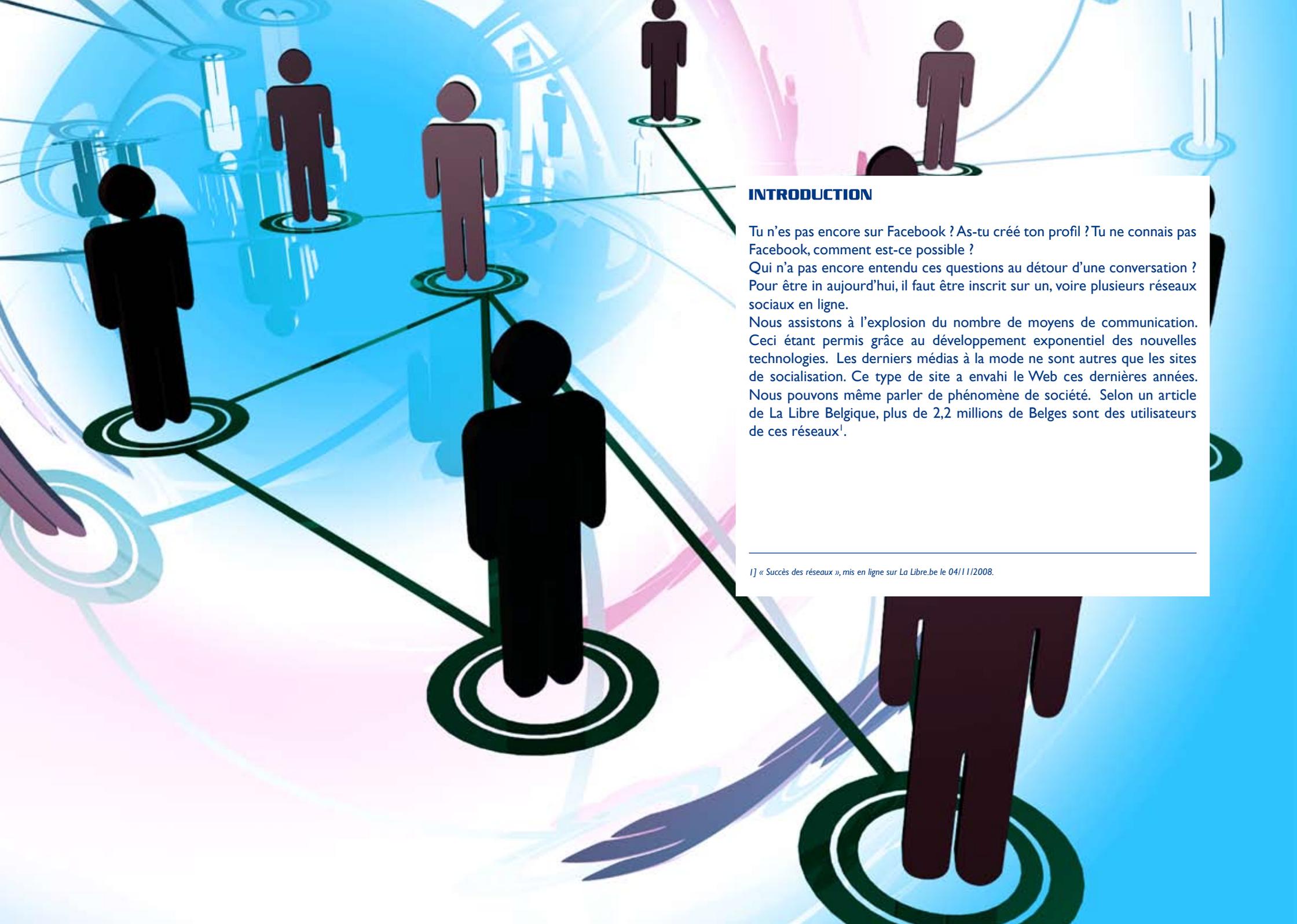




LES RÉSEAUX TISSENT LEUR TOILE





INTRODUCTION

Tu n'es pas encore sur Facebook ? As-tu créé ton profil ? Tu ne connais pas Facebook, comment est-ce possible ?

Qui n'a pas encore entendu ces questions au détour d'une conversation ? Pour être in aujourd'hui, il faut être inscrit sur un, voire plusieurs réseaux sociaux en ligne.

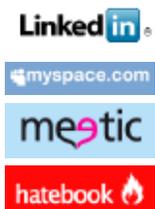
Nous assistons à l'explosion du nombre de moyens de communication. Ceci étant permis grâce au développement exponentiel des nouvelles technologies. Les derniers médias à la mode ne sont autres que les sites de socialisation. Ce type de site a envahi le Web ces dernières années. Nous pouvons même parler de phénomène de société. Selon un article de La Libre Belgique, plus de 2,2 millions de Belges sont des utilisateurs de ces réseaux¹.

¹ « Succès des réseaux », mis en ligne sur La Libre.be le 04/11/2008.

MAIS QU'EST-CE QU'UN RÉSEAU SOCIAL ?

Le réseau social « est une communauté d'individus ou d'organisations reliés de manière directe ou indirecte entre eux, en fonction de centres d'intérêts, de points de vue ou encore de besoins communs² ». Danah Boyd³ affine cette définition pour les sites de socialisation qui sont « une catégorie de sites Web avec des profils d'utilisateurs, des commentaires publics semi persistants sur chaque profil, et un réseau social public navigable affiché en lien direct avec chaque profil individuel⁴ ». Ces différents sites présentent plusieurs fonctionnalités comme le profil, une liste d'amis et des commentaires. Ils permettent aussi des partages de vidéos, de musique, de photos ...

Il existe différents types de réseaux sociaux :



- professionnel/business (LinkedIn et Viadeo),
- privé/loisirs (MySpace, Bebo, Facebook),
- des sites de rencontres (Meetic...),
- des réseaux pour adultes,
- des sites parodiques (Hatebook, réseau des personnes et des choses que l'on déteste... on ne s'y fait pas que des amis...).
- En bref, il y en a de tous les styles et pour tous les goûts.

Ces sites présentent-ils des risques pour leurs utilisateurs ? Il n'est pas anodin de dévoiler sa vie sur ce type de site. Cela peut entraîner des conséquences auxquelles nous ne pensons pas forcément.

Une petite anecdote ô combien sympathique pour illustrer notre propos. Une jeune fille, voulant profiter de l'absence de ses parents durant un week-end, décide d'inviter ses amies via Facebook. Mal lui en a pris, la petite fête se transforme en gigantesque fiesta avec les 400 « amis » que la jeune fille compte sur le site de réseau social. Nous pouvons facilement imaginer la crise des parents à leur retour⁵...

Dans cet article, nous nous baserons principalement sur Facebook qui connaît une croissance incroyable en Belgique.

2] Définition « réseau social » dictionnaire informatique sur www.dicofr.com

3] Danah Boyd est doctorante en science de l'information à l'université de Berkeley.

4] Affordance.info blog d'Olivier Ertzscheid maître de conférence en science de l'information et la gestion des connaissances.

5] « Sur facebook, pas que des amis » article mis en ligne le 25/10/2008 sur Actu24.be

HARO SUR LA VIE PRIVÉE?

Le principal danger dont découlent les autres risques des sites de socialisation, réside de l'intrusion dans notre vie privée de personnes qui ne nous veulent pas forcément que du bien.

Nous avons tous le droit à la protection de notre vie privée. Et que dire de notre droit à l'image si souvent bafoué ! Comment réagirions-nous si l'un de nos amis commettait l'indélicatesse de publier une photo nous montrant dans une posture compromettante et dont nous ne souhaitons absolument pas la diffusion ? Si cela vous est déjà arrivé, nous sommes persuadés que vous vous êtes empressés d'effacer le « marquage ». Cependant, ces derniers temps, la frontière entre vie publique et vie privée est devenue floue avec l'avènement du Web 2.0⁶. En effet, nous sommes devenus des acteurs du Net. Nous diffusons sur les sites de réseaux sociaux des informations nous concernant, des vidéos, des commentaires... sans penser à d'éventuelles conséquences.

Lorsque nous téléchargeons une application sur Facebook, il nous est demandé d'autoriser l'accès à cette application. Nous ne faisons pas souvent assez attention aux conditions d'adhésion. De fait, accepter l'installation d'une application en lien avec notre profil engendre le partage de nos données personnelles avec le concepteur de l'application⁷. Nos données privées sont notamment revendues à prix d'or à des sociétés de marketing. Pourquoi ? Ces informations permettent de cibler au mieux nos attentes et elles permettent des actions de marketing on-line presque personnalisées. Les Facebook et autres MySpace développent même des outils à destination des publicitaires pour affiner leur ciblage. Lorsque nous surfons sur ces sites, de la publicité est disséminée un

peu partout sur les différentes pages que nous consultons ou encore un bandeau publicitaire interactif y apparaîtrait. Nous pouvons aussi recevoir du



6] Le Web 2.0 est l'internet de nouvelle génération qui permet de l'interactivité.

7] « To be or not to be on Facebook », analyse publiée sur le site de Média animation asbl.

courrier indésirable jusque dans notre boîte mail. C'est aussi la porte ouverte aux spameurs et aux différents hoax⁸. Le problème vient du fait que la législation en vigueur en matière de protection de nos données sur le Web 2.0 en est encore à ses premiers balbutiements. Pire, nos données sont enregistrées dans la base de données de Facebook même après effacement de notre profil. Donc, nous perdons notre « droit à l'oubli » et il est possible de devoir répondre de nos publications sur le Web des années plus tard.⁹

Pour tester leur popularité, les adolescents et même des adultes acceptent un nombre impressionnant « d'amis ». Ils ouvrent leur profil à n'importe qui sans se soucier d'éventuels prédateurs. L'entreprise Sophos qui développe des solutions de gestion de menaces informatiques a réalisé une enquête à ce sujet. Deux cents demandes d'ajouts à une liste d'amis ont été envoyées, résultat 41 % de ces utilisateurs ont accepté l'invitation et sont devenus « amis » avec Freddi Staur. Ce dernier est un profil fictif créé pour les besoins de l'enquête



dont la photo montre une grenouille en plastique¹⁰. Ils ont donné accès à toutes leurs données privées à un parfait inconnu et de surcroît totalement imaginaire. C'est éloquent ! C'est le comportement même des utilisateurs qui est dangereux. Ils laissent accéder trop facilement à leur profil...

Heureusement, il existe maintenant des garde-fous pour protéger un minimum nos informations personnelles. Sur

Facebook, contrairement à de nombreux autres réseaux, nous pouvons sécuriser notre profil en le rendant uniquement accessible à nos amis. Prudence car nous ne sommes jamais à l'abri d'un éventuel « bug » informatique. Une récente faille de sécurité de Facebook a permis la consultation de toutes les photos, pourtant paramétrées « accessibles uniquement aux amis », de certains utilisateurs dont celles du fondateur de Facebook, Mark Zuckerberg¹¹. Si l'un de nos amis est « tagué » dans un album par une personne qui n'est pas notre « ami » nous pouvons quand même accéder à l'album tout entier de cette personne. Lorsqu'un système présente des brèches, il existe toujours des gens pour s'y engouffrer avec de mauvaises intentions... L'accès à nos données personnelles peut engendrer des conséquences plus graves et tout aussi inattendues.

8] Un hoax est un canular sur le Web.

9] Interview d'Alex Türk, président de la CNIL accordée à LCI.

10] « Facebook : la paradis des voleurs d'identité », article sur cases.lu (portail officiel de la sécurité de l'information du Luxembourg)

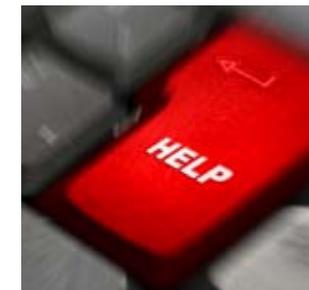
11] « Dérives de Facebook » article sur cases.lu (portail officiel de la sécurité de l'information du Luxembourg)

CYBERCRIMINALITÉ

Il est tentant pour des personnes malveillantes d'usurper votre identité ou celle de vos amis. Le but est de récolter un maximum de données personnelles leur permettant, par exemple, de commettre des délits ou de voler vos codes bancaires ou encore vous jouer un mauvais tour. Pour la petite histoire, Adam Morrisson, un jeune étudiant, s'est retrouvé au poste de police pour un interrogatoire en bonne et due forme. Après lui avoir volé son identité (sa photo et son nom sur Facebook), un petit malin a créé un faux profil. Sur ce dernier, le petit plaisantin a laissé entendre qu'il allait commettre une tuerie similaire à celle de l'école de Columbine. Suite à cela, le jeune homme s'est « effacé » dudit site¹².

Pour faire face aux dérives de ce type de site, certains gestionnaires de réseaux sociaux ont créé des cellules pour intervenir sur les profils criminels et les faux profils. La police fédérale dispose de spécialistes au sein de la Computer Crime Unit afin, notamment, de remonter jusqu'aux auteurs de faux profils. Elle a récemment lancé une campagne de prévention « surfons tranquille » afin de nous aider à accroître notre vigilance sur le Web. Nous pouvons signaler des délits commis sur ou via le Net par le site eCops de la police fédérale.

Les cybercriminels guettent la moindre faille mais d'autres types de personnes peuvent être intéressées par la consultation de notre profil dans un but bien précis auquel nous n'avions peut-être pas pensé.



12] « Dérives de Facebook » article sur cases.lu (portail officiel de la sécurité de l'information du Luxembourg)

QUESTION DU RECRUTEMENT / POSITIONNEMENT DES ENTREPRISES

Pour se passer de publier des annonces coûteuses de recrutement, certaines entreprises se sont lancées à la recherche de nouveaux talents via les réseaux en ligne. Les employeurs font des recherches avant de nous engager, ils pistent nos traces sur le net. Découvrir notre profil et nos états d'âmes sur un site de réseau social est un bon moyen pour les employeurs de mieux nous cerner. Ensuite, une personne des ressources humaines dresse notre profil psychologique.

Quid si notre potentiel futur employeur tombe sur des commentaires peu reluisants de sa société ou sur des photos ne nous présentant pas sous notre meilleur jour ? Des employés de Virgin se sont faits licencier suite à des propos critiques à l'encontre de leur société. Les établissements se posent des questions quant à leur image et à ce que leurs employés peuvent en dire sur des réseaux en ligne. Un quart des entreprises belges pensent bloquer l'accès au site Facebook, c'est ce qui ressort d'une enquête menée par Vacatures-References et Koppen¹³. Par contre, certaines firmes voient dans ces sites un excellent moyen publicitaire. C'est l'occasion d'annoncer leurs événements, de se faire connaître et de tisser des liens. Comme nous l'avons fait remarquer, il existe des sites entièrement dédiés au business comme LinkedIn avec des intentions tout à fait louables.

¹³] « Un employeur sur quatre envisage de bloquer l'accès à Facebook » mis en ligne sur LaLibre.be le 18/12/2008.

CONCLUSION

L'usage des sites de socialisation doit faire l'objet de bon sens et de précautions. L'éducation aux médias, surtout auprès des jeunes, semble primordiale.

Le problème majeur que nous avons soulevé dans cet article réside dans l'utilisation que nous faisons des sites de socialisation. Nous agissons généralement sans prudence. Si nous poussons à l'extrême, il est préférable de ne rien publier de personnel sur le Web pour être sûr de préserver sa vie privée car il en reste toujours une trace quelque part.

Nous nous sentons protégés derrière notre ordinateur or comme nous l'avons démontré il n'en est rien. Bien que nous vivions à l'ère du virtuel, nous devons nous ancrer dans la réalité. Nous pensons que ces relations sur la toile et ces échanges dans un espace fictif ne remplaceront jamais une vraie discussion autour d'un verre ou d'un bon repas.

Soyons vigilants, agissons sur le Net comme nous agirions dans la vie réelle. Nous ne donnons pas notre nom, notre adresse ou notre numéro de téléphone à un parfait inconnu dans la rue. Pourquoi alors le faire sur la toile ? Gardons-nous des espaces de discussions et de rencontres bien réels où nous pouvons contrôler nos échanges.

Cependant tout n'est pas négatif non plus. Ces sites de socialisation permettent de retrouver d'anciennes connaissances, de partager de la musique ou des vidéos avec ses amis, de se créer un réseau qui peut être utile dans le cadre du travail...



SOURCES

« Succès des réseaux », mis en ligne sur La Libre.be le 04/11/2008.

« Un employeur sur quatre envisage de bloquer l'accès à Facebook » mis en ligne sur LaLibre.be le 18/12/2008.

« Sur facebook, pas que des amis » article mis en ligne le 25/10/2008 sur Actu24.be

« To be or not to be on Facebook », analyse publiée sur le site de Média animation asbl.

« Facebook : le paradis des voleurs d'identité », article sur cases.lu (portail officiel de la sécurité de l'information du Luxembourg)

« Dérives de Facebook » article sur cases.lu (portail officiel de la sécurité de l'information du Luxembourg)

« MySpace : la puissance du réseau social au service du marketing », Guillaume Devaux, article mis en ligne sur le journaldunet.com le 17/07/2006.

« Facebook, le défi de la confidentialité et de la productivité » article sur Sophos.fr

Interview d'Alex Türk, président de la CNIL accordée à LCI.

Affordance.info est le blog d'Olivier Ertzscheid qui est maître de conférence en sciences de l'information et la gestion des connaissances.

Le dictionnaire informatique <http://www.dicofr.com>

Auteur : Frank Marchal
juillet 2009

DÉSIREUX D'EN SAVOIR PLUS !

Animation, conférence, table ronde... n'hésitez pas à nous contacter,
Nous sommes à votre service pour organiser des activités sur cette thématique.



Centre Permanent pour la Citoyenneté et la Participation

Rue des Deux Eglises 45 - 1000 Bruxelles

Tél. : 02/238 01 00

info@cpcp.be