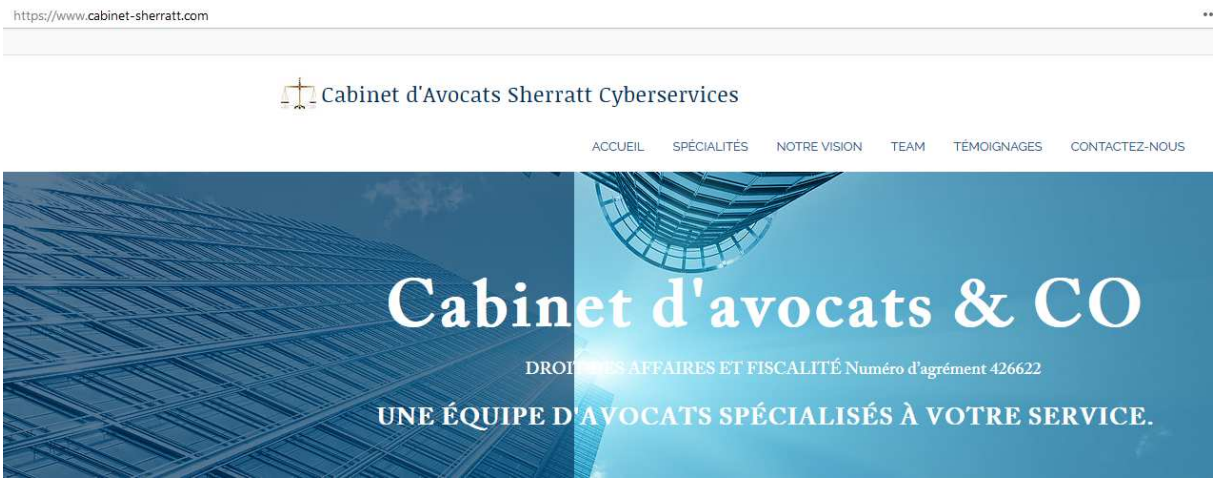
La page accueil du site cabinet-sherratt au 01/02/2019 :



NOS SPÉCIALITÉS

- Avocat Cybersécurité
  Cyberdéfense
- Le Hacking
- Expertise avocat cybersécurité
  cyberdéfense
- Entreprises et Particuliers
  Victimes sur le web

Cybersécurité Cyberdéfense

Le cyberespace est l'espace de communication virtuel dans lequel s'inscrit le droit de la cybersécurité et de la cyberdéfense.
Le cyberespace est devenu le cinquième champ de conflictualité après la terre, la mer, l'air et l'espace.
Le besoin de sécurité globale du citoyen et de l'entreprise entraîne également une augmentation des contrôles et donc une possible violation des libertés individuelles. C'est pourquoi, il est nécessaire d'accompagner toute démarche de cybersécurité et de défense cyber d'un encadrement juridique.

Le droit de la cybersécurité adresse tous les risques et toutes les menaces volontaires d'origine humaine qui sont susceptibles de porter atteinte aux différents patrimoines (technologique, scientifique, économique, image) de l'entreprise. La cybersécurité consiste dans la recherche d'un état pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait donc appel à des techniques de sécurité de systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Le droit de la cyberdéfense investit le champ des exigences de sécurité qui s'impose aux opérateurs de services essentiels (OSE) qui doivent prendre les mesures techniques et organisationnelles nécessaires, proportionnées et adaptées à la gestion des risques menaçant la sécurité des réseaux et systèmes d'informations essentiels au maintien d'activités économiques et sociales critiques. Les modes d'attaques des systèmes d'informations et des réseaux sont de plus en plus ciblés et complexes et sont rendus possibles par l'utilisation de technologies. La France a identifié environ 200 opérateurs d'importance vitale répartis sur 12 secteurs et sous-secteurs.
Les entreprises doivent prendre en compte le risque cybersécurité. Pour ce faire, les entreprises doivent mettre en œuvre une veille spécifique pour identifier les cybermenaces sur leurs activités. C'est à cette condition, que les dirigeants seront en mesure d'anticiper et de réagir aux différentes cybermenaces pesant sur leurs activités.

Le hacking :

« accès et maintien frauduleux dans un système de traitement automatisé de données » va changer. Le 21 janvier 2016, l'Assemblée nationale a adopté, en première lecture, un amendement contenu dans le projet de loi pour une République numérique visant à compléter l'article 323-1 du Code pénal, par un nouvel alinéa :

« Toute personne qui a tenté de commettre ou commis le délit prévu au présent article est exempte de peine si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système de traitement automatisé de données en cause d'un risque d'atteinte aux données ou au fonctionnement du système ».
Cet amendement, nommé « Bluetouff » en référence à l'arrêt de la Cour de cassation du 20 mai 2015 qui avait condamné un internaute pour s'être maintenu frauduleusement dans l'intranet de l'ANSES, prévoit, comme en matière d'association de malfaiteurs, une exemption de peine pour toute personne qui, après avoir constaté, voire exploité, une faille de sécurité en informe immédiatement l'autorité publique ou le maître du système.
Il ne s'agit là que d'une exemption de peine, et non d'une exemption de poursuites, ce qui en d'autres termes signifie que l'auteur du hacking, du piratage pourra être poursuivi et déclaré coupable, mais n'aura pas à exécuter de peines pénales.
Par cet amendement, le Gouvernement entend poursuivre un double objectif. D'abord donner une alternative presque légale au hacker du dimanche qui par défi personnel, et non intention de nuire, est parvenu à s'introduire dans un système d'information. A ce titre, il est regrettable que l'amendement Bluetouff ne prévoit qu'une exemption de peine, l'assurance de ne pas être poursuivi pour hacking aurait, à n'en pas douter, été plus convaincante.
En second lieu, il permettrait de participer à la sécurité du réseau. Garantie en poche de ne pas être pénalisés, nombre d'experts en informatique pourraient collaborer avec les sociétés développant des sites internet, applications ou logiciels pour identifier et corriger les vulnérabilités.

Législateur et secteur privé s'acheminent progressivement vers un droit au hacking. En attendant, le Code pénal nous rappelle qu' « accéder ou se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 euros d'amende ».

Entreprises et Particuliers Victimes sur le web

Les entreprises et les Particuliers sont quotidiennement victimes de nouvelles formes de vulnérabilités :

• acte contrevenant aux traités internationaux ou aux lois nationales effectué dans le cyberespace ou au moyen d'un système informatique : cybercriminalité ;

• piratage informatique qui permet d'accéder à des informations tenues secrètes. L'objectif est d'en tirer un avantage personnel, économique, patrimonial : cyberespionnage ;

• acte de terrorisme utilisant des systèmes informatiques ou la technologie des ordinateurs comme une arme ou comme une cible (...). Le cyberterrorisme a des motivations politiques, sociales ou religieuses, il vise à semer la peur ou la panique dans la population civile ou à déstabiliser l'appareil militaire et civil. : cyberterrorisme ;

• risque de guerre informatique exposant les entreprises qui sont sur le territoire d'Etat étranger dans lequel un conflit classique dont au moins une des composantes, dans la réalisation, les motivations et les outils (armes au sens large du terme) s'appuie sur le champ informatique ou numérique. Il est évoqué le terme de « cyberattaque » (Source : Eric Filiol, auteur et expert en sécurité informatique et ancien militaire). Si l'objectif de cette guerre informatique est politique : sa cible les militaires, un Etat (et ses infrastructures) ou une société et ses équipements informatiques.

De nombreuses installations industrielles fonctionnent grâce à des systèmes de contrôle et d'acquisition de données (SCADA en anglais). Quel que soit le secteur d'activité de l'entreprise, l'énergie, les transports, la santé, et jusqu'à ce que les dispositifs de contrôle et d'acquisition de données soient conçus en adoptant une logique de « Secure by design », ces dispositifs font naître des vulnérabilités face aux enjeux de cybersécurité ou de cyberdéfense.

Expertise avocat cybersécurité cyberdéfense

Notre expertise et nos compétences nous permettent d'anticiper, d'analyser et d'évaluer les risques, afin de vous permettre de pérenniser et renforcer votre stratégie de cybersécurité mais aussi de défendre contre les conséquences dommageables sur les patrimoines et l'image de votre entreprise, en cas de dommages portés aux réseaux et systèmes d'information de votre entreprise.

Le cabinet est distingué Law Firm of the Year pour l'année 2017 dans la catégorie Technologies de l'Information pour la France par la revue américaine « Best Lawyers« . Cette distinction fait suite à la désignation M sherratt comme Lawyer of the Year de 2011 à 2015 dans les catégories Nouvelles Technologies et Droit des Technologies.

NOTRE VISION

Pénal et Cybercriminalité

Faire face à vos côtés et défendre avec vigueur vos intérêts dans un monde en mouvement et digitalisé où plus que jamais associer compétences juridiques et technologies est primordial.

Le cabinet assiste des particuliers et des entreprises, auteurs présumés d'infractions ou parties civiles, à tous les stades de l'enquête et devant les juridictions pénales. Il a développé une expertise particulière et

reconnue en matière de cybercriminalité, de preuve numérique et d'investigations dans l'environnement digital et les systèmes informatiques. Notre équipe se compose également d'experts techniques.

RGPD

- Respect de la vie privée : tout traitement susceptible d'entrainer des risques élevés sur la vie privée devra faire l'objet d'une étude d'impact,
- Transparence : l'individu a le droit de savoir à quoi servent ses donnée
- Droit à l'oubli : sur demande le consommateur peut réclamer la suppression de ses données,
- Contact inactif : tous contacts inactifs depuis plus de 3 ans doit être retirés des traitements.

Honoraire

Comment travaillons-nous ?

Honoraire facturé uniquement sur le résultat

Comment calculons nous nos honoraires , nous prenons un % sur nos résultats .

Le % de nos honoraires vous sera valide par mail.

M.J.Sherratt

Sherratt est l'un des fondateurs de notre cabinet d'avocats .

Diplôme à Genève puis a fait un master à Londres.

Depuis plus de 6 ans, il s'occupe des Cyber Attac.

Notre Team

Isabelle Martin Bureau de Varsovie

Avocate et sont Team

Isabelle travaille dans notre bureau de Varsovie depuis plus de 8 ans.

Diplôme à Genève puis à Varsovie.

Marc Vidal bureau de Bruxelles et sont Team

Responsable suivi des clients

Master en économie, a développer un système de suivi de clients avec nos différents collaborateurs en Europe.

Notre Team Financier

Tatiana Viloduvitch

Service Juridique.

Localisé à Varsovie

John Hamilton

Service financier

Localisé à Londres

Hilda Baumann

Service Financier / Contentieux

Localisé à Berlin

Contactez-nous

Cabinet d'Avocats Sherratt Cyberservices

Nos Bureaux

Rondo ONZ 1, 00-124 Warszawa -Pologne

Piccadilly Street 79 - London w1j8eu - England

Service Financier

TD Grosshandels Gmbh i.G

Uetzer Str 5 - 38536 Meinersen - Germany

E-mail : avocats@cyberservices.com

Téléphone 00 33 (0)1 70 77 24 99 - 00 33 (0)1 70 77 24 99