ISSN - 2170- 0656

CERISTNEWS

Bulletin d'information trimestriel
Treizième numéro - Juin 2013

DOSSIER

LES DISPOSITIFS LÉGAUX DE LUTTE CONTRE LA CYBERCRIMINALITÉ

CENTRE DE RECHERCHE
SUR L'INFORMATION
SCIENTIFIQUE ET TECHNIQUE
cerist


CYBERCRIMINALITÉ
LUTTE
UNAUTHORISED
LAW
INTERNET
WEB
TIC
SOCIÉTÉ DE L'INFORMATION
INFORMATIQUE
ATTAQUES
NETWORKS
DROIT
SÉCURITÉ
PRÉVENTION
SERVICES
CRIMINALITÉ
INTERNET
DISPOSITIFS LÉGAUX
COMPUTER
CONSEILS
LÉGAUX
SOCIÉTÉ DE L'INFORMATION
LEGAL DEVICES
RÉSEAUX
CYBERCRIMINALITÉ
SOCIÉTÉ DE L'INFORMATION
COMPUTER
RÉSEAUX
SÉCURITÉ
SERVICES
LUTTE
CRIMINALITÉ
SÉCURITÉ
PRÉVENTION
WEB
LEGAL DEVICES
LUTTE
UNAUTHORISED
INTERNET
WEB
LUTTE

Éditorial

Bouder Hadjira
Attachée de Recherche
Division Recherche et Développement en Sciences de l'Information (CERIST)

Les deux dernières décennies ont été marquées par la dépendance de plus en plus accrue de la quasi-totalité des activités socio –économiques, à travers le monde, de l'outil informatique et des réseaux de télécommunications grâce à la place qu'occupent ces derniers dans le développement des Etats. Néanmoins, toute technologie porteuse de progrès, peut être aussi génératrice de comportements délictuels.

En effet, l'exploitation accrue des réseaux de télécommunication a donné naissance à une nouvelle forme de criminalité, communément appelée « cybercriminalité », « criminalité informatique », « fraude informatique » ou encore « criminalité liée aux TIC ». Cette forme inédite de criminalité menace non seulement l'économie et la sécurité des Etats, mais aussi les citoyens dans leur vie privée et leur patrimoine. Une menace que même les systèmes de sécurité informatique, aussi performants qu'ils soient, peinent à freiner.

Afin de mieux maîtriser cette criminalité, plusieurs Etats à travers le monde, ont procédé, dés les années 70, à l'adoption de dispositifs légaux instituant les différents types de délits relevant de cette catégorie de criminalité, et définissant les mesures procédurales plus adaptées pour leur poursuite .

Toutefois, cette appréhension par les législations nationales de la criminalité informatique s'est heurtée à plusieurs contraintes dont : - L'anonymat (difficulté d'identification de l'auteur de l'infraction) ; - La volatilité des informations numériques (modification ou suppression rapide des preuves numériques); - Le caractère transnational que revêtent souvent les comportements délictuels relevant de la cybercriminalité, et ses conséquences sur la définition légale de ces comportement et leur éventuelle répression.

Face à ces contraintes, une harmonisation du droit pénal matériel et procédural au niveau international, ainsi qu'une étroite coopération judiciaire entre Etats se sont imposées, pour une lutte plus efficace contre des cybercriminels qui tendent à se répandre à travers le monde.

En effet, bon nombre d'initiatives ont été prises dans cette optique, dont certaines ont été couronnées par l'adoption de conventions internationales, notamment au niveau régional, telle que la convention du Conseil de l'Europe sur la cybercriminalité, et la convention de la Ligue des Etats Arabes pour la lutte contre la cybercriminalité.

N'étant pas en reste de cette dynamique mondiale, l'Algérie s'est, dés la fin des années 90, engagée dans l'adaptation de son dispositif pénal national aux exigences de la lutte contre la criminalité informatique.

Ces mesures légales jouent un rôle de plus en plus important dans la lutte contre la cybercriminalité. C'est pourquoi elles méritent d'être mieux explicitées et appréhendées, notamment par les personnes activant dans la sphère de la sécurité informatique et la lutte contre la cybercriminalité.

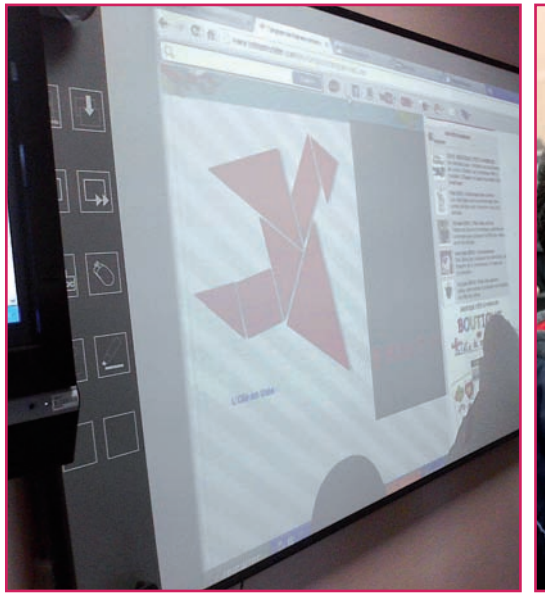
Sommaire

Visite pédagogique de doctorants en informatique du laboratoire LAMOS

Une visite pédagogique a été effectuée au CERIST par des doctorants du Laboratoire de Modélisation et d'Optimisation des Systèmes (LAMOS) de l'université de Béjaia , le jeudi 13 juin 2013. Ces doctorants ont assisté à la présentation de deux projets de recherche à savoir, le projet IRRIG-SENSE sur l'application de réseaux de capteurs sans fil pour l'économie de l'eau d'irrigation et le projet Wise Road sur la gestion du trafic routier, faite par les chercheurs de l'équipe des réseaux de capteurs sans fil. Ces présentations ont été suivies par un riche débat sur le principe de fonctionnement d'un capteur. Par ailleurs les doctorants ont pu voir de près le capteur DZ50 et les différents modules qui le constituent , conçu et réalisé par les chercheurs du CERIST.

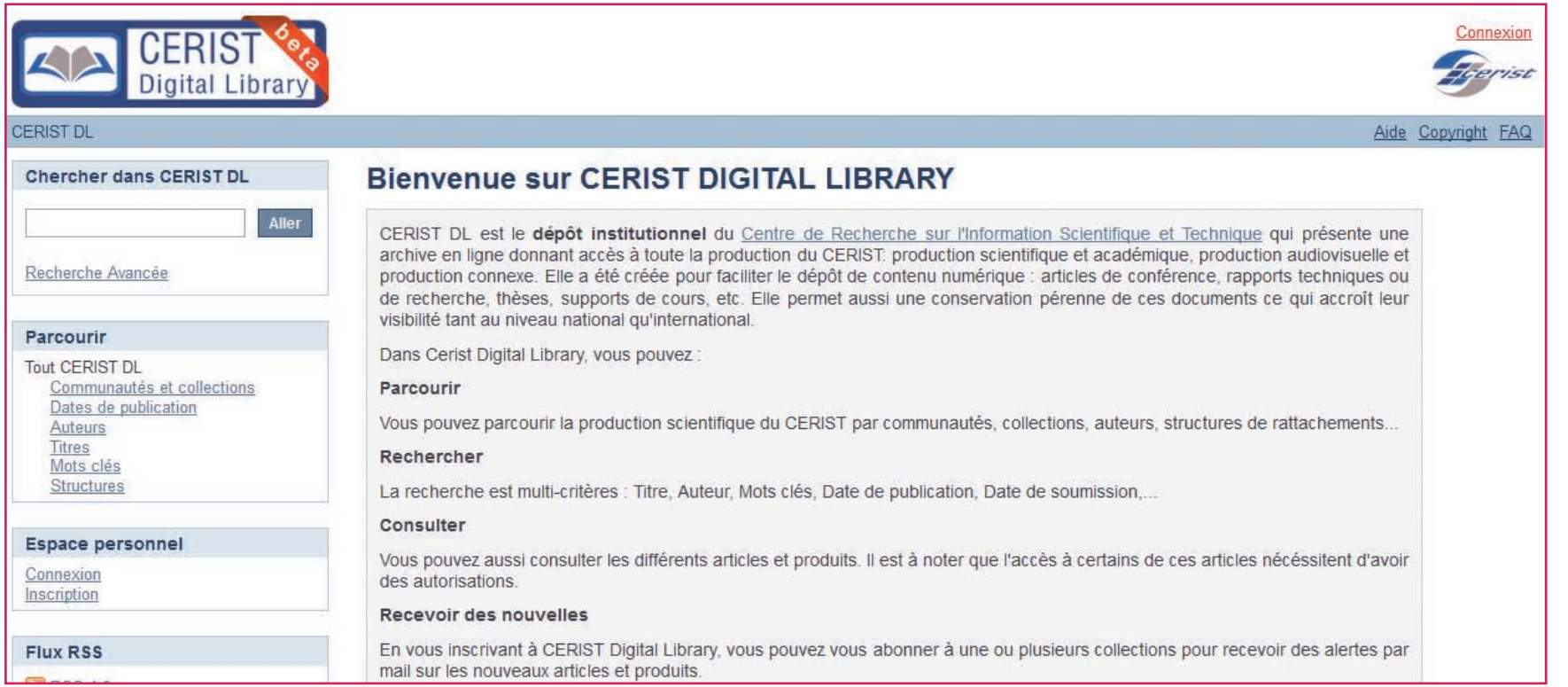
Des élèves de l'école Chafika Mazi de Ben Aknoun en visite au CERIST

Le CERIST a reçu la visite d'une trentaine d'élèves de l'école primaire Chafika Mazi de Ben Aknoun, le mercredi 15 mai 2013. Cette visite rentre dans le cadre de la promotion des nouvelles technologies de l'information et de la communication. Les jeunes écoliers venus visiter le centre ont beaucoup apprécié le bloc pédagogique et toute l'infrastructure de télé enseignement. Ils ont, ainsi, pu tester le tableau blanc interactif avec beaucoup de curiosité. La visite s'est achevée avec des prises de photos souvenirs.



Lancement de CERIST DL

Le jeudi 30 mai 2013 a été lancée la version Beta de la base CERIST Digital Library. La base CERIST DL, accessible sur www.dl.cerist.dz, est le dépôt institutionnel du centre, elle présente une archive en ligne donnant accès à toute la production du CERIST: production scientifique et académique, production audiovisuelle et production connexe. Elle a été créée pour faciliter le dépôt de contenu numérique : articles de conférence, rapports techniques ou de recherche, thèses, supports de cours, etc. Elle permet aussi une conservation pérenne de ces documents, ce qui accroît leur visibilité tant au niveau national qu'international.



Salon International de l'Informatique, de la bureautique et de la Communication (SICOM)

Le CERIST a participé au Salon International de l'Informatique, de la bureautique et de la Communication (SICOM) qui a eu lieu à la Safex (Pins maritimes) d'Alger le 24 avril 2013. Sous le slogan «l'entreprise et les technologies de l'information et de la communication» cette manifestation avait pour objectif de favoriser l'innovation et la création de communautés professionnelles en TIC et consacrer le rôle de ces technologies dans le développement de l'entreprise pour lutter contre la bureaucratie et assurer une meilleure réactivité tant de l'entreprise que d'autres institutions. Lors de ce salon, des conférences sur le programme e-Algérie, sur la cybercriminalité, sur la télévision numérique, et l'ouverture du champ médiatique en Algérie ont été organisées. La conférence sur la cybercriminalité a été animée par Mme Hadjira Bouder, chercheur en droit des TIC au CERIST. Dans sa présentation, Mme bouder a repris tous les textes adoptés dans le cadre de la prévention et de la lutte contre la cybercriminalité, notamment la loi 09-04 du 5 août 2009 portant règles de prévention en matière de surveillance des communications électroniques, d'implication des fournisseurs dans le cas des investigations judiciaires en gardant les contenus des communications pendant un certain temps, la création d'un organe national de prévention et de lutte contre les délits liés aux TIC, la reconnaissance de l'écrit électronique et de la signature électronique basée sur la cryptologie. Cet évènement, devenu un rendez-vous annuel incontournable pour les professionnels nationaux et étrangers a attiré cette année 165 exposants.

Symposium international : « Le LMD D'orthophonie et ses entités de recherche en neurosciences cognitives : Algérie-Etranger ».

Un symposium international, organisé conjointement par l'Université d'Alger 2, la Direction Générale de la Recherche Scientifique et du Développement Technologique (DGRSDT), a eu lieu au CERIST le 26 mai 2013 sous le thème de : « Le LMD D'orthophonie et ses entités de recherche en neurosciences cognitives : Algérie-Etranger ». Cette rencontre, a été une occasion, pour les administrateurs et les Comités Scientifiques décisionnels algériens, qui gèrent le LMD d'Orthophonie, de rencontrer leurs homologues étrangers afin d'aboutir à des recommandations motivées, qui seront proposées au ministère.

Atelier sur les Modalités de mise en œuvre d'un point d'échange Internet

Le CERIST a abrité les 09 et 10 juin 2013 un atelier sur les modalités de mise en œuvre d'un point d'échange Internet. Organisé par le ministère de la Poste et des Technologies de l'information et de la communication (MPTIC), en collaboration avec la commission de l'Union africaine (UA) et l'association Internet society, cet atelier rentre dans le cadre du projet de la commission de l'UA sur le système d'échange Internet africain (Axis) qui vise à garder le trafic de l'Internet

africain au sein même du continent et à contribuer au renforcement des capacités des pays africains, en vue de faciliter l'établissement de points d'échange Internet locaux et nationaux.

Le but de cet évènement est de sensibiliser sur l'intérêt et les avantages de l'établissement d'un point d'échange Internet sur l'écosystème local et régional de l'Internet. L'autre objectif est de permettre aux participants de prendre connaissance des meilleures pratiques utilisées dans le monde pour l'établissement et la gestion d'un point d'échange Internet. La création de centres d'échanges Internet entre les différents fournisseurs d'accès régionaux et locaux permettra d'améliorer la qualité et le débit des connexions, a indiqué, le Pr. Nadjib Badache, directeur du CERIST, lors de cet atelier.

L'avantage de ces points d'échange se situe également sur le plan économique et seront plus rentables pour les fournisseurs d'accès et les utilisateurs. Pr.Badache a fait savoir que le cheminement des informations Internet lors du passage par ces points d'échanges seront plus courts et moins coûteux, relevant que ces informations ne passeront plus par les liaisons internationales mais par les liaisons régionales et locales. Le représentant du Ministère de la Poste et des Technologie de l'Information et de la Communication (MPTIC), M. M'hamed Dabouz, a expliqué que ces centres d'échange seront implantés à Alger, Oran et Constantine. Selon M. Dabouz, un plan national de haut et très haut débit a été mis en place par le MPTIC à travers l'usage de la fibre optique et permettra d'avoir une vitesse de connexion dépassant les 2 mega-bit par seconde, pour chaque utilisateur.

Workshop sur la « bioéthique et la conduite responsable de la science en Algérie »

Le Centre de Recherche sur l'Information Scientifique et Technique (CERIST) a abrité du 16 au 20 Juin 2013 un Workshop sur «La bioéthique et la conduite responsable de la Science en Algérie». Il a été co-organisé par le Centre de Recherche en Biotechnologie (CRBt), le Centre de Développement des Energies Renouvelables (CDER) et the National Academies of Science (NAS) sous le patronage de la Direction Générale de la Recherche Scientifique et du Développement Technologique (DGRSDT). L'objectif de ce Workshop était de rassembler des représentants des différentes universités et centres de recherche algériens provenant de différentes disciplines, afin de discuter des besoins nationaux en matière d'enseignement de la bioéthique. Le résultat attendu était l'élaboration d'une proposition d'un programme national pour l'enseignement de la bioéthique à l'université algérienne. Cette proposition devrait comprendre un contenu détaillé qui fait ressortir les aspects qui transcendent les disciplines et les aspects spécifiques à chaque discipline, ainsi qu'une feuille de route pour l'implémentation de cette proposition en matière de moyens humains et matériels à mobiliser, de partenariat et de formation de formateurs aux techniques pédagogiques d'apprentissage actif.

Cinquièmes Journées d'Etude sur les Bibliothèques Universitaires Algériennes (JEBU' 13)

Le CERIST a organisé les Cinquièmes Journées d'Etude sur les Bibliothèques Universitaires Algériennes (JEBU' 13) sous le thème : « La Politique documentaire du secteur de l'enseignement supérieur et de la recherche scientifique, formation et politique d'acquisition » les 29 et 30 mai 2013.

A l'issue de cette rencontre de deux jours, les participants ont retenu quelques recommandations principales portant essentiellement sur la politique d'acquisition et la formation. Il a été préconisé de mettre en place une commission de documentation au sein de chaque bibliothèque centrale des établissements de l'enseignement supérieur et de la recherche scientifique et d'un comité de réflexion qui sera chargé de la mise en place d'une politique nationale d'acquisition, de gestion et de traitement des documents électroniques. Les documents produits par un établissement de recherche reflètent son dynamisme et son activité scientifique. A cet effet, il a été recommandé pour chaque université d'instaurer le dépôt institutionnel. Par ailleurs, la mise en place d'une politique de formation continue au sein de la commission nationale des ressources documentaires s'avère indispensable, une sous-commission de réflexion devra œuvrer pour mettre en place un cadre institutionnel, recenser les compétences (les formateurs) et élaborer le programme et le financement des formations.

LE DOSSIER

Document spécial de 15 pages : 11/26

LES DISPOSITIFS LÉGAUX DE LUTTE CONTRE LA CYBERCRIMINALITÉ

Un dossier élaboré par :

Bouder Hadjira

Attachée de Recherche

Division Recherche et Développement en Sciences de l'Information

LES DISPOSITIFS LÉGAUX
DE LUTTE CONTRE LA CYBERCRIMINALITÉ

Les dangers sécuritaires liés à la généralisation des Technologies de l'Information et de la Communication (TIC) ne sont plus à démontrer. En effet, l'exploitation de ces technologies à des fins criminelles constitue une forme inédite de la criminalité, que les systèmes de sécurité informatique ne peuvent éradiquer, d'où la nécessité de les renforcer par un autre type de protection, à savoir la protection juridique ou la protection par le droit.

Outre l'encouragement des activités de recherche et développement en sécurité informatique, de nombreux Etats ont adopté des législations consacrant des crimes informatiques et de nouvelles prérogatives aux entités chargées de leur poursuite.

Toutefois, le caractère planétaire que revêtent les réseaux téléinformatiques, leur dépendance d'un organisme non étatique, l'anonymat qui peut se pratiquer sur les réseaux, ainsi que la volatilité des informations numériques, entravent l'application effective de ces législations, mettant en exergue la nécessité de recourir au droit international afin de garantir une harmonisation internationale du droit matériel et procédural relatif à cette nouvelle criminalité, ainsi qu'une étroite coopération judiciaire entre Etats dans ce domaine.

En effet, bon nombre d'initiatives ont été prises dans cette optique, dont certaines ont été couronnées par l'adoption de conventions internationales, notamment au niveau régional, telle que la convention du Conseil de l'Europe sur la cybercriminalité et la convention de la Ligue des Etats Arabes pour la lutte contre la cybercriminalité .

N'étant pas en reste de cette dynamique mondiale, l'Algérie s'est, dés la fin des années 90, engagée dans l'adaptation de son dispositif pénal national aux exigences de la lutte contre la criminalité informatique.

1. Les dispositifs légaux internationaux

1.1 Travaux de l'ONU

La criminalité liée aux réseaux informatiques a suscité l'intérêt des Etats membres de l'Organisation des Nations Unis dés 1990, à l'occasion de la tenue du huitième Congrès de l'organisation pour la prévention du crime et le traitement des délinquants, qui a eu lieu à la Havane (Cuba) du 22 août au 7 septembre 1990, et qui a recommandé la création d'une commission intergouvernementale pour la prévention du crime et la justice pénale qui serait le principal organe directeur de l'ONU en la matière.

Dés sa création en 1992, ladite commission s'est engagée dans la promotion des efforts internationaux dans le domaine de lutte contre la criminalité informatique, à travers l'élaboration d'un ensemble de principes et de normes destiné à mieux orienter ces efforts. Cet engagement à eu pour premier résultat la publication en 1994 d'un manuel sur la prévention et la répression de la criminalité informatique.

En 2000, un atelier de travail a été consacré aux « délits liés à l'utilisation du réseau informatique », dans le cadre du dixième congrès des Nations Unis pour la prévention du crime et le traitement des délinquants, qui s'est tenu à Vienne (Autriche) du 10 au 17 avril 2000. Il avait pour objectif d'aboutir à une conception commune de la criminalité informatique, à l'échelle internationale, et d'orienter l'élaboration des politiques pénales nationales en la matière.

Le 4 décembre 2000, l'Assemblée Générale des Nations Unis a adopté une résolution à travers laquelle elle a, entre autres, noté avec satisfaction les efforts déployés pour lutter contre l'exploitation des technologies de l'information à des fins criminelles.

A rappeler, que peu avant la tenue du dixième congrès de l'ONU suscité, le Secrétaire Général a été chargé par le Conseil Economique et Social de l'ONU, à travers la résolution 1999/23, de mener une étude sur les mesures efficaces à prendre pour prévenir et lutter contre les délits liés aux réseaux informatiques.

En 2001, le Secrétaire Général a présenté Conformément à la résolution 1999/23, son rapport à la commission pour la prévention du crime et la justice pénale à sa dixième session. Parmi les propositions les plus marquantes de ce rapport, nous citons : l'élaboration d'un instrument international pour la prévention et la lutte contre les délits informatiques, ainsi que la mise en place d'une stratégie mondiale sous l'égide de l'ONU contre ce type de délits.

L'idée d'élaboration d'un instrument international contre les délits informatiques, a été reproposée par de nombreux Etats, notamment dans le

cadre du douzième congrès des NU pour la prévention du crime et le traitement des délinquants qui s'est tenu au Salvador(Brésil) du 12 au 19 avril 2010 ; et où la cybercriminalité figurait en bonne place dans l'ordre du jour, à cause de sa croissance remarquable. Toutefois, cette idée n'a pu, à ce jour, être concrétisée. De son coté, l'Assemblée Générale de l'ONU à chargé, à travers sa résolution 65/230, la Commission pour la prévention du crime et la justice pénale de mettre en place, conformément à la Déclaration de Salvador, un groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité. Le dernier rapport a été remis le 23 janvier 2013.

Les activités de l'ONU dans le domaine de la lutte contre la criminalité informatique restent ainsi limitées à des études, des plans d'actions et des propositions de mesures à mettre en œuvre tant au niveau national qu'international. On ne peut pour autant négliger son impact considérable sur les stratégies de lutte contre la criminalité informatique mises en œuvre notamment au niveau national et régional.

1.2 La convention de Budapest sur la cybercriminalité

La convention de l'organisation du conseil de l'Europe sur la cybercriminalité, communément appelée « Convention de Budapest », est le premier instrument international contraignant en la matière.

Adoptée en 2001 et entrée en vigueur en 2004, cette convention vise pour l'essentiel à :

- Harmoniser le dispositif pénal matériel des Etats membres en énumérant les actes devant être érigés en infractions pénales au niveau national à savoir : l'accès illégal, l'interception illégale, l'atteinte à l'intégrité des données et du système, la falsification informatique, la fraude informatique, etc.
- Renforcer le droit pénal procédural national des Etats membres, à travers l'instauration de pouvoir et procédures adaptés à la nature des cyber-délits et leur environnement immatériel, telle que : la conservation rapide de données informatiques stockées, la conservation et divulgation rapide de données relatives au trafic, la perquisition et saisie de données informatiques stockées, la collecte

en temps réel de données informatiques, l'interception de données relatives au contenu.

- Mettre en place un régime rapide et efficace de coopération et de coordination internationale dans le domaine des enquêtes et des poursuites judiciaires.

En dépit de son caractère régional, cet instrument est considéré comme ayant la plus large portée au niveau international. Puisqu'il permet en vertu de son article 37 aux Etats non membres du conseil de l'Europe d'y adhérer. Il est également reconnu par différentes organisations internationales. Plusieurs pays se sont aussi inspirés de cette convention pour élaborer leur législation contre la cybercriminalité, sans y adhérer officiellement, tels que l'Argentine, le Nigeria, l'Egypte et l'Algérie.

1.3 La convention arabe sur la cybercriminalité

Le monde arabe s'est, à son tour, doté d'une convention pour la lutte contre la criminalité informatique dans le cadre de la ligue des Etats arabes. Adoptée en 2010 , cette convention vise à renforcer la coopération entre les pays arabes dans ce domaine, afin de pouvoir faire face aux conséquences néfastes de ce type de criminalité sur la sécurité et les intérêts de ces Etats et de leurs sociétés nationales.

2- Le dispositif légal national de lutte contre la cybercriminalité

S'appuyant sur l'expérience des états précurseurs des TIC, et tenant compte des priorités et de la réalité nationale, l'Algérie s'est trouvée contrainte de concevoir son propre modèle de lutte contre les risques de croissance du nombre d'actes de délinquance liés aux systèmes informatiques, qui commence à se faire sentir dans la société algérienne (Notamment ceux liés au terrorisme, à l'ordre publique,…). Et ce à travers l'adoption d'une politique pénale évolutive, qui peut constituer à court terme un maillon important dans la chaîne internationale de lutte contre la criminalité liée aux TIC.

2.1 Actes incriminés par le dispositif pénal algérien

Le législateur algérien a attaqué la problématique d'adaptation du dispositif pénal matériel aux exigences des TIC par rapport aux types d'infractions liées à ces technologies (sans s'en tenir à aucune des typologies proposées jusqu'à présent par la doctrine concernant les infractions liées au TIC). Ainsi il a commencé par la consécration de la

protection des biens intellectuels exploitables moyennant les TIC, puis les infractions ayant pour cible les TIC.

- L'action d'actualisation du dispositif pénal matériel algérien a débuté en 1997 avec l'adoption de l'ordonnance n° 97-10 du 06-03-1997 relative aux droits d'auteurs et aux droits voisins, qui traduisait déjà la volonté du législateur algérien d'étendre l'application du droit d'auteur à l'environnement numérique, à travers la consécration explicite de la protection, par le droit d'auteur : des programmes d'ordinateur, bases de données numériques , ainsi que toute création originale représentée ou diffusée sous forme numérique off-line ou on –line; Et en incriminant, à des peines très lourdes, tout acte de contrefaçon portant sur ces types inédits d'œuvres de l'esprit . Cette ordonnance fut modifiée et complétée par l'ordonnance n° 03-05 du 19-07- 2003 relative aux droits d'auteurs et aux droits voisins, qui n'est intervenue que pour mieux préciser la position du législateur algérien vis à vis de la protection des œuvres nées du développement des technologies de l'information, et contre la diffusion de manière générale d'œuvres protégées via des supports numériques, en apportant quelques corrections et compléments, mais sans modifications majeures quant à la qualification pénale des actes de contrefaçon de ces biens ou des peines qui leur sont prévues.
- La deuxième étape du processus d'adaptation du droit pénal matériel algérien aux TIC fut la révision de l'ordonnance n°66-156 du 08-06-1966 portant code pénal.

D'abord par la loi 01-09 du 26 juin 2001 qui a introduit dans le code pénal les articles 144 bis, 144 bis1 et 2et 146, où il aux été évoqué pour la première fois l'utilisation du support numérique comme moyen de commission des infractions « d'outrage et violences à fonctionnaires et institutions de l'Etat ».

Ensuite par la loi n°04-15 du 10-11-2004, qui consacrait pour la première fois des dispositions visant la protection des systèmes informatiques ou systèmes de traitement automatisé de données (STAD) (pour s'en tenir à la terminologie adoptée par le législateur pénal algérien). Ces dernières sont classées sous la section 7 bis intitulée « des atteintes aux systèmes de traitement automatisé de données » de ladite loi. Elles érigent en délit la commission ou la tentative de commission de tout acte de :

Accès ou maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données ou système informatique (Ce qui correspond le plus à la notion de «Hacking») ; l'Altération du fonctionnement du système due à l'action d'accès ou de maintien frauduleux ; La suppression ou la modification de données informatiques due à l'action d'accès ou de maintien frauduleux dans un STAD, ou à l'action d'introduction frauduleuse de données dans le STAD; L'abus de dispositif (qui recouvre les actes illicites spécifiques, commis intentionnellement, se rapportant à certains dispositifs ou données d'accès dont il est fait une utilisation abusive aux fins de commettre

des infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes ou données informatiques.)

- Plus récemment, il a été institué en vertu de la loi 08-01 du 23-01-2008 complétant la loi n°83-11 du 02-07-1983 relative aux assurances sociales une nouvelle catégorie d'infractions liées aux TIC (les articles 93quater, 93 quinquiès et 93 sixiès).

2.2 Les moyens procéduraux de lutte contre la cybercriminalité :

L'adaptation du dispositif procédural algérien au développement des TIC est passée par deux étapes qui sont les suivantes :

2.2.1 Le dispositif procédural de lutte contre la cybercriminalité avant la loi 09-04

- L'introduction, en 2004, de dispositions inédites dans le code pénal algérien, à savoir celles relatives à la criminalité liée aux TIC, a certainement suscité l'attention du législateur algérien quant à la nécessité d'adopter des règles procédurales adéquates. Or, les modifications apportées au code de procédure pénale, à la même année, par la loi n°04-14 du 10-11-2004 modifiant et complétant l'ordonnance n°66-155 du 08-06-1966 portant code de procédure pénale, étaient loin d'apporter des solutions claires à tous les obstacles procéduraux que pose la criminalité informatique. Ces modifications consistaient uniquement en l'extension de la compétence territoriale du procureur de la république et du juge d'instruction, en matière (entre autres) d'atteintes aux systèmes de traitement automatisé de données, au ressort d'autres tribunaux par voie réglementaire.

- Deux ans plus tard, une nouvelle révision du code de procédure pénale algérien est intervenue à travers la loi n°06-22 du 20-11-2006 modifiant et complétant l'ordonnance n°66-155 du 08-06-1966 portant code de procédure pénale. Celle-ci visait, notamment, la consécration de règles procédurales plus adaptées à certains types d'infractions nouvelles ou plus répandues, dont les atteintes aux systèmes de traitement automatisé de données. Parmi les nouveautés apportées par la présente loi : « les interceptions de correspondances, des sonorisations et des fixations d'images ».

2.2.2 Le dispositif procédural de lutte contre la cybercriminalité après la loi 09-04

L'esquisse de la nouvelle orientation de la politique du gouvernement algérien en matière de lutte contre la criminalité liée aux TIC, s'est traduite par la loi n°09-04 du 05 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication.

Inspirée de la convention de Budapest sur la cybercriminalité, et du droit pénal comparé, cette loi prévoit des mesures procédurales répondant à trois impératifs majeurs pour le renforcement de la prévention et la lutte contre la cybercriminalité, à savoir :

- Le renforcement des prérogatives des organes d'investigations.
- L'implication des opérateurs techniques.
- Le renforcement de l'entraide judiciaire et de la coopération internationale.

Elle prévoit également un traitement particulier pour certains types d'infractions conventionnelles jugées dangereuses, et désormais facilitées par les TIC, à savoir : les actes de terrorisme ou subversifs et les actes représentant un danger majeur pour la sûreté nationale.

Ainsi la loi pour la prévention et la lutte contre la cybercriminalité était axée en premier lieu sur la précision de ce qui est entendu par certains termes techniques au sens de ladite loi, et la délimitation de son champ d'application. Et de renforcer en second lieu les prérogatives des organes d'investigation à travers l'introduction de règles de procédures plus adaptées aux infractions liées aux TIC, avec l'implication de nouveaux acteurs dans l'administration de ces procédures.

A. Définitions et champ d'application :

- Concernant les définitions des termes techniques employés par le législateur, outre les définitions des termes : « système informatique », « données informatiques » et « fournisseurs de services » qui sont reprises presque intégralement de la convention de Budapest sur la cybercriminalité. Le législateur à introduit à travers la loi 09-04 la définition de deux nouveaux termes, à savoir : « infractions liées aux technologies de l'information et de la communication » et « Communication électronique ».

- Quant au champ d'application de la loi 09-04, ce dernier est bien délimité par l'article 3 de ladite loi, qui tout en rappelant la nécessité de respecter les dispositions légales garantissant le secret des correspondances et des communications, permet le recours dans les limites des règles du code de procédure pénale et de la présente loi à :

- la mise en place de dispositifs techniques pour effectuer des opérations de surveillance des communications électroniques, de collecte et d'enregistrement en temps réel du contenu de ces communications,

- des perquisitions dans un système informatique et des saisies des données informatiques qu'il véhicule.

Ces opérations ne sont permises que pour des impératifs de protection de l'ordre publique ou pour des besoins d'enquêtes ou d'informations judiciaires en cours, tel que précisé dans le chapitre II de la loi 09-04.

B. Renforcement des prérogatives des organes d'investigations :

B.1 Consécration du principe de surveillance des communications électroniques :

En fait, la loi 09-04, à travers son chapitre II, consacre pour la première fois dans l'histoire de la procédure pénale en Algérie le principe de surveillance préventive, et réitère le principe de la surveillance judiciaire qui a déjà été consacré par la loi de 2006 modifiant et complétant le code de procédure pénal de 1966 sous le chapitre IV relative à l'interception de correspondances, des sonorisations et de fixations d'images .

L'article 4 du chapitre II de la loi 09-04, intitulé « surveillance des communications électroniques », vient préciser les cas autorisant le recours aux opérations de surveillance énoncés dans l'article 3, à savoir :

- La mise en place de dispositifs techniques pour effectuer des opérations de surveillance des communications électroniques, de collecte et d'enregistrement en temps réel de leur contenu,
- Les perquisitions et saisies dans un système informatique.

Nonobstant la formulation un peu nuancée du dernier paragraphe de l'article 3, on constate qu'à travers l'article 4 de la loi 09-04, le législateur algérien consacre quatre cas de figure autorisant le recours à la surveillance des communications électroniques, que nous pouvons scinder en deux catégories :

Cas autorisant la surveillance préventive des communications électroniques :

Cette catégorie comprend les cas consacrés dans les points a) et b) de l'article 4, concernant respectivement :

- La prévention des infractions qualifiées d'actes terroristes ou subversifs et les infractions contre la sûreté de l'Etat ;
- Les cas où il existe des informations sur une atteinte probable à un système informatique représentant une menace pour l'ordre public.

Cas de surveillance judiciaire :

Ces cas sont consacrés dans les paragraphes c et d de l'article 4, Ils concernent :

- Les besoins des enquêtes et des informations judiciaires, lorsqu'il est difficile d'aboutir à des résultats intéressant les recherches en cours sans recourir à la surveillance électronique ;
- L'exécution des demandes d'entraide judiciaire internationale.

A souligner que tous ces cas autorisant le recours à la surveillance, préventive ou judiciaire, des communications électroniques sont subordonnés à une autorisation écrite de l'autorité judiciaire compétente.

le législateur algérien a innové en introduisant dans l'article 4 deux conditions auxquelles sont assujetties les opérations de surveillances relevant du paragraphe a). Ces conditions constituent des garanties judiciaires plus ou moins suffisantes et compatibles avec la procédure d'autorisation écrite de l'autorité judiciaire compétente, exigée pour toutes les opérations de surveillances mentionnées dans l'article 4. Ainsi les opérations de surveillance prévues au paragraphe a) doivent impérativement :

- Etre soumises à une autorisation délivrée par le procureur général prés de la cour d'Alger sur la base d'un rapport indiquant la nature du procédé technique utilisé et les objectifs qu'il vise,
- Reposer sur des dispositifs techniques orientés, exclusivement, vers la collecte et l'enregistrement de données en rapport avec la prévention et la lutte contre les actes terroristes et les atteintes à la sureté de l'Etat.

Il ressort également de l'avant dernier paragraphe de l'article 4, que les opérations de surveillance prévues dans le paragraphe a) relèvent exclusivement des compétences des officiers de la police judiciaire relevant de l'organe national de prévention et de lutte contre les infractions liées aux TIC visées à l'article 13 de la loi 09-04.

B.2 Les règles de procédures :

Le chapitre III de la loi 09-04 a mis en place des règles procédurales plus adaptées à la nature des délits informatiques, et à la particularité de l'environnement dans lequel ils sont perpétrés, puisque

contrairement à l'article 47 bis de la loi de décembre 2006 modifiant et complétant le code de procédure pénale de 1966, qui consacrait pour la première fois des règles particulières pour la perquisition et la saisie en matière (entre autres) d'infractions d'atteintes aux STAD, les articles de ce chapitre visent la perquisition, la saisie et la conservation des données saisies, effectuées dans un contexte informatique immatériel. Ainsi les dispositions relatives à ces procédures ont été respectivement réparties comme suit :

La perquisition des systèmes informatiques :

Institué par l'article 5 de la loi 09-04, cette procédure ne vise pas la perquisition au sens classique du terme (ex : perquisition d'un local ou une maison sur la base d'un mandat de perquisition), elle désigne plutôt l'accès pour perquisition, y compris à distance, à un environnement virtuelle qui n'est autre qu'un système informatique ou une partie de celui-ci. Ou encore à un support de stockage informatique permettant de stocker des données se trouvant sur le territoire national, en vue de retrouver, parmi des données stockées dans ce système informatique ou dans un support permettant de conserver des données informatiques, des données utiles pour la découverte des infractions ou leurs auteurs.

Par ailleurs, nous remarquons que concernant le cas de perquisition consacré par le paragraphe a) de l'article 5, le législateur algérien prévoit deux cas de figure :

- Le cas, où l'autorité effectuant la perquisition d'un système informatique ou de l'une de ses parties (cas de systèmes interconnectés ou apparentés tels qu'internet le réseau des réseaux), et que ces deux systèmes se trouvent sur le territoire national. L'autorité en question peut étendre rapidement la perquisition au deuxième système informatique ou à une de ses parties, à condition d'en informer, au préalable, l'autorité judiciaire compétente. A rappeler, que cette dernière condition ne fait que conforter les dispositions de la loi 04-14 et celles de la loi 06-22 modifiant et complétant le code de procédure pénale, relatives à la compétence territoriale du parquet, du juge d'instruction et de la police judiciaire, en matière d'atteinte aux STAD.

- Le cas où l'autorité effectuant la perquisition d'un système informatique (ou d'une partie de celui-ci) se trouvant sur le territoire national, a des raisons de croire que les données recherchées sont stockées dans un autre système informatique se trouvant en dehors du territoire national, et que ce dernier est accessible par le système informatique initial (celui situé sur le territoire national). Dans ce cas, l'obtention des données informatiques recherchées se fera avec le concours des autorités étrangères compétentes conformément aux accords internationaux pertinents et suivant le principe de la réciprocité.

Le dernier paragraphe de l'article 5 vient renforcer les prérogatives des autorités judiciaires chargées de la perquisition, en leur donnant la possibilité de réquisitionner toute personne en mesure de les assister et de leur fournir les informations nécessaires à l'accomplissement de leur mission (il s'agit notamment de l'administrateur du système informatique, ou dans certains cas du détenteur des clés de cryptage lorsque la cryptographie est utilisée comme moyen de protection des données informatiques contenues dans le système en question).

La saisie de données informatiques :

Le libellé des articles 6 et 7 de la loi 09-04, confirme encore une fois la volonté, du législateur, d'adapter les règles procédurales classiques à l'environnement numérique. Ainsi, la saisie au sens de cette disposition porte sur les données informatiques qui ont été découvertes, par les officiers de la police judiciaire ou par les personnes dûment habilitées, dans un système informatique, et qui pourraient être utiles pour la constatation de l'infraction ou l'identification de son auteur. Selon ces mêmes articles, la saisie des données informatiques peut être effectuée suivant trois scénarii :

- La saisie du support informatique (disquette, CD-Rom, disque dur externe ou interne, ordinateur) contenant les données informatiques utiles pour la découverte des infractions ou leurs auteurs, en le plaçant sous scellé conformément aux conditions prévues par le code de procédure pénale
- Lorsque la saisie du support n'est pas nécessaire (exemple : fichier non volumineux) , la saisie des données informatiques utiles, ainsi que celles nécessaires à leur compréhension, s'effectue en copiant ces données sur des supports de stockage informatique pouvant être saisis et placés sous scellés dans les mêmes conditions prévues pour les objets matériels conformément aux règles générales de procédures pénales.
- S'il est impossible, pour des raisons techniques, de saisir l'intégralité du système ou de copier les données informatiques utiles et les données permettant leur compréhension sur un support (cas précédent), l'autorité habilitée est autorisée à recourir à la « saisie par l'interdiction d'accès aux données », qui consiste à utiliser les techniques adéquates pour empêcher l'accès à ces données ou aux copies de celles-ci qui sont à la disposition des personnes autorisées à utiliser le système informatique visé.

A souligner que concernant le deuxième scénario de saisie de données informatiques, il a été tenu compte des éventuelles altérations du contenu des données saisies, pouvant être occasionnées par l'utilisation de moyen technique de copiage ou de remise en forme des données saisies. C'est pourquoi, il a été rappelé dans le deuxième et le troisième paragraphe de l'article 6 : « …qu'en tout état de cause,

l'autorité effectuant la saisie doit veiller à l'intégrité des données du système informatique en question ».

A noter que dans le deuxième paragraphe de l'article 6, le législateur insiste sur la nécessité de veiller à l'intégrité des données, que ça soit à l'occasion d'une procédure de perquisition ou de saisie de données informatiques. Ceci nous amène à nous interroger sur l'intérêt d'inclure le respect de l'intégrité des données lors d'une perquisition dans cet article, alors qu'il aurait été préférable de l'aborder dans la partie de la loi relative à la procédure de perquisition (article 5). D'autant plus que les possibilités d'altérations des données, dues aux manipulations techniques, se présentent de la même manière aussi bien dans la procédure de perquisition que lors d'une procédure de saisie partielle des données (opération de conservation de données saisies dans un autre support de stockage). A relever aussi, qu'il n'est nullement précisé dans cette loi le responsable des éventuels dommages pouvant être causés de façon non intentionnelle, par les personnes requises pour la perquisition et la saisie informatique, au système informatique ou aux données qu'il véhicule.

Outre ces dispositions, le dernier paragraphe de l'article 6 vient apporter une réponse à une situation particulière de saisie informatique, à savoir : la saisie portant sur des données intangibles, telles que des données cryptées. Dans ce cas de figure le législateur permet à l'autorité effectuant la perquisition et la saisie de recourir aux moyens techniques requis pour mettre en forme ou reconstituer (décrypter) les données en question, en vue de les rendre exploitables pour les besoins de l'enquête. Ceci à condition que cette mise en forme ou reconstitution des données n'en altère pas le contenu sans définir, le cas échéant, les responsabilités.

Données saisies au contenu incriminé :

En vertu de l'article 8 de la loi 09-04, l'autorité ayant effectué la perquisition se voit dotée de nouvelles prérogatives, lorsque les données relatives à l'infraction en cours de recherche ou à ses auteurs sont contraires à l'ordre public ou aux bonnes mœurs, ou constituent un danger pour l'intégrité des systèmes informatiques ou des données stockées, traitées ou transmises par le biais de tels systèmes. Elle peut de ce fait ordonner les mesures conservatoires nécessaires, notamment en désignant toute personne qualifiée pour employer les moyens techniques appropriés pour rendre ces données inaccessibles.

A noter, que cette disposition a été fortement contestée, par certains membres, lors des travaux de la commission chargée de la rédaction de la présente loi, pour le fait qu'on ne peut reconnaître aux services chargés des investigations un pouvoir presque absolu d'appréciation des faits sans contrôle d'un juge.

B.3 Implication des fournisseurs de services dans la procédure d'investigation

Tenant compte du rôle que peuvent jouer les opérateurs de télécommunications et les fournisseurs de services Internet dans la recherche des infractions relatives aux TIC et leurs auteurs, la commission chargée de la rédaction de la loi en question a choisi d'adopter le principe d'implication de ces partenaires techniques dans les procédures d'investigations.

Inspiré des législations européennes, notamment la législation française, ce principe consiste à amener les partenaires techniques de télécommunications à apporter leur concours aux autorités chargées de l'application de la présente loi, en leur fournissant les informations qui pourraient leur être utiles dans leurs investigations. Et ce en répondant à l'obligation de sauvegarder certains types de données pendant une durée déterminée.

Après les longs débats qui ont eu lieu au sein de la commission autour du contenu des obligations qui allaient incomber aux opérateurs de télécommunications et aux fournisseurs de services Internet, notamment en ce qui concerne la nature des données à conserver, les partenaires techniques visés par cette conservation, la durée et le coût de cette conservation, il a été décidé de consacrer le chapitre IV de la loi 09-04 aux « obligations des fournisseurs de services ». Ces obligations sont réparties en deux catégories :

Des obligations incombant à tous les fournisseurs de services

En vertu de l'article 11 de la loi 09-04, les fournisseurs de services, au sens de la présente loi, sont tenus de conserver les données relatives au trafic, telles que définies par la convention de Budapest sur la cybercriminalité et reprise par le législateur algérien, pour une durée d'un an , à compter du jour de leur enregistrement. A ce titre, ils ont l'obligation, selon la nature et les types des services fournis, de conserver dans les conditions prévues par cette disposition : « toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent. ».

Des obligations spécifiques aux fournisseurs d'accès Internet

Au sens de la présente loi, les obligations consacrées dans l'article 12 incombent particulièrement aux fournisseurs d'accès à Internet nationaux. Elles visent, d'une part, à faciliter la tâche aux services chargés de la lutte contre les infractions informatiques qui se rapportent au contenu, et d'une autre part, à impliquer ces prestataires de services dans les opérations de lutte contre les contenus illicites. De ce fait, ces prestataires auront, outre les obligations d'assistance aux autorités et de conservation des données relatives au trafic, l'obligation :

«[…] a) d'intervenir, sans délai, pour retirer les contenus dont ils autorisent l'accès en cas d'infractions aux lois, les stocker ou les rendre inaccessible dés qu'ils en ont pris connaissance directement ou indirectement ;

b) de mettre en place des dispositifs techniques permettant de limiter l'accessibilité aux distributeurs contenant des informations contraires à l'ordre public ou aux bonnes mœurs et en informer les abonnés. »

B.4 Création de l'organe national de prévention et de lutte contre la criminalité liée aux TIC :

En fait, l'institution de cette organe et la fixation de ses missions furent à l'origine de la présente loi, qui devait fournir l'encrage juridique des opérations de surveillance préventive prises en charge par le centre national pour la lutte contre la cybercriminalité relevant de la gendarmerie nationale, et de fixer ses relations avec les autres corps chargés de la lutte contre ce type d'infractions, tant au niveau national qu'international.

La création d'un tel organe devrait avoir pour principal objectif le regroupement des efforts des autorités chargées de la poursuite et de la lutte contre la criminalité informatique et d'éviter les redondances.

Ainsi cette loi est venue instituer l'organe national pour la prévention et la lutte contre la criminalité liée aux TIC, qui a pour missions notamment :

- La dynamisation et la coordination des opérations de prévention et de lutte contre la criminalité liée aux TIC .
- L'assistance des autorités judiciaires et des services de la police judiciaire en matière de lutte contre la criminalité liée aux TIC, y compris à travers la collecte de l'information et les expertises judiciaires
- L'échange d'informations avec ses interfaces à l'étranger aux fins de réunir toutes données utiles à la localisation et à l'identification des auteurs des infractions liées aux TIC

Quant à la composition, l'organisation et les modalités de fonctionnement de cet organe, ils devraient être fixés par voie réglementaire. Mais aucun texte réglementaire n'a été adopté à ce jour dans ce sens.

C. Renforcement de la coopération et de l'entraide judicaire internationales

L'intégration de ce volet dans la présente loi, traduit une prise de conscience de la nécessité de renforcer l'entraide internationale en matière de lutte contre la cybercriminalité, afin de palier aux difficultés d'investigations et de poursuites des auteurs de ces infractions, liées principalement au caractère transnational des réseaux de télécommunication.

Ainsi un chapitre a été réservé dans la loi 09-04 à la coopération et l'entraide judiciaire internationales, qui tout en rappelant les règles de compétences prévues par le code de procédure pénale, consacre les suivantes règles de coopération spécifiques à la lutte contre la cybercriminalité :

- L'élargissement de la compétence des juridictions algériennes en matière de lutte contre la criminalité informatique, qui désormais s'étend aux infractions liées aux TIC commises par un auteur étranger en

dehors du territoire national, lorsqu'elles ont pour cible les institutions de l'Etat algérien, la défense nationale ou les intérêts stratégiques de l'économie nationale (article.15).

- La fixation des cas autorisant le recours à l'entraide judiciaire internationale en vue de recueillir des preuves sous forme électronique, en l'occurrence les investigations et les informations judiciaires menées pour la constatation des infractions liées aux TIC et la recherche de leurs auteurs (article 16 paragraphe 1). Ces demandes, qui en temps normal doivent obéir à un certain formalisme procédural, sont recevable en cas d'urgence si elles sont formulées par des moyens rapides de communication (télécopie, courrier électronique,…) pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (article 16.parag 2)

La consécration de restrictions aux demandes d'entraides émanant des autorités étrangères, qui sont les suivantes :

- les demandes tendant à l'échange d'informations ou à prendre toute mesure conservatoire sont satisfaites conformément aux conventions internationales pertinentes, aux accords bilatéraux et en application du principe de réciprocité (article 17) ; - la satisfaction des demandes d'entraide peut être subordonnée à la condition de conserver la confidentialité des informations notifiées, ou de ne pas les utiliser à des fins autres que celles indiquées dans la demande (article 18. Paragraphe2) ; la demande d'entraide de nature à porter atteinte à la souveraineté de l'Etat ou à l'ordre public est rejetée (article 18.paragraphe 1).


LES CONSEILS
DE DZ-CERT

Protéger son site web des attaques Sql Injection

Les attaques de type injection sont considérées comme l'une des attaques les plus critiques. Dans les documents OWASP TOP10 des années 2007, 2010 et 2013, ce type d'attaque occupe toujours les toutes premières positions.

Une injection SQL fait en général référence à une attaque qui cible les applications web qui interagissent dynamiquement avec une source de donnée, dans le cas usuel, une base de données.

Cette attaque est réalisée en injectant du code SQL dans une entrée utilisateur dans le but de former une nouvelle requête SQL et qui est non prévue par le programmeur. Cela permet à un attaquant de récupérer des données sensibles à partir de la base de données (récupérer des mots de passe par exemple).

Une telle attaque cible une faille dans une application web. Ce type de faille peut exister si les entrées utilisateur (formulaires, URL ou tout entête HTTP) ne sont pas filtrées correctement et sont utilisées comme paramètres pour récupérer des informations à partir de la base de données.

Exemple de faille : page d'authentification

```php
<?php

...

mysql_connect(...);
mysql_select_db(...);

...

//récupération des paramètres
$utilisateur=$_POST['user'] ;
$password   =$_POST['password'] ;

//construction de la requête SQL
$requete='SELECT * FROM user WHERE user='. $utilisateur . 'AND password='. $password ;

//exécution de la requête
$result = mysql_query($requete);
...

?>
```

Nous illustrons un exemple de faille par une page d'authentification. Cette page contient deux champs : le champ utilisateur et le champ mot de passe. Ces deux données sont passées à un code PHP qui va vérifier leur légitimité par-rapport à une base de données:

texte :

< ?php

…

mysql_connect(...);

mysql_sqlectdb(..) ;

…

//récupération des paramètres

```
$utilisateur=$_POST['user'] ;
$password=$_POST['password'] ;
//construction de la requête SQL
$requete='SELECT * FROM user WHERE user='. $utilisateur . 'AND
password='. $password ;
//exécution de la requête
mysql_query($requete) ;
...
?>
```

Ici, la requête SQL est construite à partir des données envoyées par le formulaire. Aucune modification ou traitement sur ces données n'est effectué.

Exemple d'exploitation : contournement du mécanisme d'authentification

Le code précédent contient une vulnérabilité de type SQL injection. Les paramètres du formulaire sont envoyés tels quels. L'attaquant peut injecter du code SQL dans l'un des champs du formulaire. Il peut par exemple insérer:

Utilisateur : admin
Mot de passe : ' or 1=1 --
La requête devient après construction :
SELECT * FROM user WHERE user='admin' AND password='' or 1=1
--

La condition sur le mot de passe est toujours évaluée à vraie. L'attaquant peut donc se connecter avec l'identifiant admin sans vraiment connaître le mot de passe.

Classification des injections SQL :

Outre l'exemple précédent, plusieurs variantes des attaques par injection SQL existent, elles peuvent être classées comme suit :

Tautologies : le principe ici est d'injecter un code pour que les instructions conditionnelles soient toujours évaluées à vraie (exemple du contournement du mécanisme d'authentification).

Requête avec union : le but est d'exploiter un paramètre de la requête pour extraire des données d'une table (autre que celle normalement utilisée dans la requête).

Requête Piggy-Backed : l'attaquant essaie avec ce type d'attaque d'injecter une nouvelle requête sans modifier la requête originale.

Requête incorrecte : elle consiste à causer intentionnellement une erreur dans la requête afin de récolter des informations importantes sur le système, l'application web ou la base de données.

Procédures stockées : le principe est d'exécuter les procédures stockées fournies par le SGBD. Dans les SGBD modernes, ces procédures permettent même l'interaction avec le système d'exploitation.

Inférence : consiste à modifier la requête pour simuler un mécanisme de réponse vrai ou faux. Comme le site ne retourne aucun message, l'attaquant doit observer le changement des pages du site web afin d'en déduire la réponse.

Encodage alternatif : est utilisé conjointement avec les autres techniques. Son but principal étant d'éviter la détection par les mécanismes de défense existants.

Techniques de protection :

Plusieurs techniques existent pour mitiger le risque des attaques par injection SQL. Leur utilisation est grandement recommandée voir même obligatoire. Il est très important de prendre l'habitude de les utiliser notamment pour les développeurs.

Les procédures stockées : en utilisant cette technique, les données entrées par l'utilisateur sont transmises comme paramètres, sans risque d'injection.

Les expressions régulières : utiliser ces dernières permet de s'assurer que les données entrées par l'utilisateur sont bien de la forme souhaitée.

Principe moindre privilège : utiliser le principe du moindre privilège afin de limiter les droits des utilisateurs de l'application web ainsi que ceux de la base de données et ainsi limiter les risques ou les dégâts en cas d'intrusion.

Les requêtes paramétrées : en utilisant une requête paramétrée, c'est le SGBD qui se charge d'échapper les caractères selon le type des paramètres.

Les fonctions d'échappement : utiliser les fonctions d'échappement (exemple des fonctions mysql_real_escape_string et addslashes dans PHP) afin de filtrer les caractères spéciaux.

Zoom Sur Un Projet

Bouder Hadjira
Attachée de Recherche

Division Recherche et Développement en Sciences de l'Information

« Le Droit à l'épreuve des Technologies de l'Information et de la Communication : Conséquences sur l'Algérie »

Introduction :

La généralisation des réseaux téléinformatiques à travers le monde, favorisée par la démocratisation des technologies de l'information et de la communication, a donné naissance à un nouveau concept incarnant la parution d'une nouvelle société humaine, communément appelée «société de l'information». Cette dernière revête certaines caractéristiques authentiques: c'est une société fondée sur l'immatériel, à caractère transnational, ne relevant officiellement d'aucune entité étatique. Cependant, les effets des activités exercées en son sein dépassent l'espace virtuel sur lequel elle se développe, créant de nouveaux défis pour le Droit.

En fait, l'émergence de la société de l'information a donné lieu à de nouvelles situations juridiques, qui ont démontré les limites des systèmes juridiques existants et la nécessité de leur actualisation.

Afin de répondre à cet impératif, beaucoup de pays ont procédé au renforcement de leurs dispositifs juridiques à travers l'adoption de dispositions adaptées aux TIC, en vue de garantir un meilleur encadrement juridique aux pratiques nées de l'utilisation des réseaux de télécommunication et leurs impacts sur l'économie, la culture et la sécurité de ces Etats.

Toutefois, le caractère planétaire que revêtent ces réseaux et leur dépendance d'un organisme non étatique, entrave l'application effective de ces législations, mettant en exergue la nécessité de recourir au droit international pour mettre en place un cadre légal international pour la société de l'information.

En effet, bon nombre d'initiatives ont été prises dans cette optique, dont certaines ont été couronnées par l'adoption de conventions internationales universelles et régionales. Quant au niveau universel, outre les chantiers ouverts par les Nations Unies et ses organisations spécialisées autour des problématiques : de la criminalité informatique, du commerce électronique et de la propriété intellectuelle, le sommet mondial sur la société de l'information dans ses deux phases (Genéve en 2003 et Tunis en 2005), témoigne de la prise de conscience de la

communauté internationale de la nécessité de soumettre la société de l'information au droit international.

N'étant pas en reste de cette dynamique mondiale, l'Algérie a procédé en 2004 puis en 2008 à l'adoption de stratégies nationales pour le développement d'une société algérienne de l'information. Où «la mise à niveau du cadre juridique national » occupe une place majeure.

Dans cette optique, plusieurs chantiers ont été ouverts en vue d'adapter le dispositif juridique national à la révolution numérique. Certains ont abouti à l'adoption de textes plus ou moins actualisés, notamment ceux concernant la lutte contre la cybercriminalité et le renforcement de la protection de la propriété intellectuelle dans l'environnement numérique. D'autres ont moins bien avancé, pour des considérations multiples, tel que le e-commerce et la certification électronique.

Néanmoins, force est de constater que ces efforts tardent à apporter leurs fruits. D'où la nécessité de s'interroger sur les contraintes d'ordre juridique qui empêchent notre pays de tirer profit de l'ensemble des opportunités offertes par les TIC. Ainsi, les textes juridiques adoptés jusqu'à présent sont-ils suffisants ? répondent-ils aux besoins du terrain ? Ont-ils permis d'accélérer l'intégration des TIC dans la société algérienne ? Ont-ils contribué à l'instauration de la confiance tant nécessaire pour le développement de la société de l'information, ou plutôt ils ont créé de nouvelles contraintes ? Que reste-t-il à faire en Droit des TIC en Algérie, pourquoi et comment ?

Objectifs du Projet :

Ce projet consiste à dresser un bilan des mesures entreprises par les autorités algériennes pour la mise à niveau du cadre juridique national relatif aux TIC, en vue de mesurer leur impact sur le développement de la société algérienne de l'information, et d'en dégager les contraintes et les opportunités. Et ce, à la lumière des expériences juridiques étrangères dans le domaine. Il vise ainsi à :

- Contribuer aux réflexions menées autour des incidences du développement des TIC sur le Droit.

- Définir les enjeux juridiques de la société de l'information dans les pays en développement, à travers le cas de l'Algérie.
- Evaluer les mesures juridiques entreprises par l'Algérie dans le cadre de sa stratégie d'adhésion à la société mondiale de l'information.

Impacts Scientifiques, Socio-Economiques et Techniques du Projet :

- La valorisation des résultats de ce projet, à travers les manifestations scientifiques et les publications au niveau national et international, a permis de démontrer l'importance de notre travail sur les problèmes juridiques occasionnés par l'intégration des TIC en Algérie. Puisque le Cerist a été sollicité, à plusieurs occasions, par des institutions de l'Etat pour participer à des travaux portant sur des problématique ayant fait l'objet de notre réflexion dans le cadre de ce projet, ainsi que par des entreprises économiques et même des particuliers. Nous citons pour exemple : l'invitation de participation en 2011 au séminaire international organisé par le centre de recherches juridiques et judiciaires relevant du ministère de la justice, et ce suite à la participation du cerist à la rédaction de la loi de 2009 pour la prévention et la lutte contre la cybercriminalité. Ou plus récemment l'invitation du Groupe de Travail Chargé du Rôle de l'Autorité Racine Autonome en matière de Certification Electronique, relevant des Services du Premier Ministre, pour sa réunion du 11 juin 2013. Afin de représenter une communication déjà faite dans le cadre d'un séminaire de l'ARPT sur la signature et la certification électronique, et qui portait sur la cadre juridique de cette matière en Algérie.

- L'objet du présent projet est également inscrit en tant que thèse de doctorat au niveau de l'université d'Alger. Sa soutenance permettra d'offrir un outil de travail, retraçant et analysant les plus importants problèmes juridiques nés de l'exploitation des TIC notamment au niveau national, à toute personne concernée par ces questions (étudiants, chercheurs, juristes, magistrats, institutions de l'Etat,..),

- Un séminaire national a été organisé, dans le cadre de ce projet, les 16 et 17 mai 2012 au CERIST sur : **«Le cadre juridique des TIC en Algérie : Entre opportunités et contraintes ? »**. Il a été animé par des experts étrangers et nationaux venant du secteur académique, judiciaire et professionnel (notamment les banques). Ce séminaire à suscité l'intérêt d'un nombre important de personnes activant dans la sphère des technologies numériques, ou s'intéressant aux questions juridiques relatives (Institutions de l'Etat (ministères, parlement, corps constitués), entreprises publiques et privées, chercheurs en Droit et informatique ou autres disciplines concernées (professionnels des TIC, juristes spécialisés, magistrats, avocats, étudiants, etc.)

FORMATION

Une formation sur JAVA ,et précisément sur l'introduction à JAVA : Un langage orienté objet adapté à Internet ainsi que Java et les bases de données a été donnée aux personnels de la SONELGAZ, de l'Union des Coopératives de céréales de l'algérois, de l'Université de Yahia Fares de Médéa, de l' Institut de télécommunication d' Oran, et de l' Université de Batna.

Deux autres formations ont été aussi données, l'une portant sur la « Conception de sites web niveau I et II » aux personnels de la SONELGAZ et l'ENSSMAL et l'autre sur « La gestion de l'information dans l'entreprise » au profit de l' ENSSP. Par ailleurs, Pr Saddek Bensalem de l'université de Grenoble a animé une formation sur la conception des systèmes basée sur des modèles, pour les chercheurs du centre, du 14 au 17 avril 2013.

Cycle de conférences / **www.cerist.dz/conf**

Mme Imane Benkhelifa attachée de recherche au CERIST : « Overview on projects using Wireless Sensor Networks in Disaster Management » , 28 mars 2013.

Dr malika Silhadi Mehdi CERIST : « Méta heuristiques hybrides sur GPU-Applications à des problèmes réels »,04 avril 2013.

M. Madjid Sadallah attaché de recherche au CERIST : « Un modèle de traces pour la reconception de documents multimédia », 18 Avril 2013.

M. Nouredine Tonkin chargé D'étude au CERIST : « Une approche d'adaptation de documents multimédia à base de contraintes », 18 Avril 2013.

Dr. Madjid Dahmane Chef de la division Recherche et Développement en Sciences de l'Information : « Les contenus nationaux sur Internet », 16 avril 2013.

M. Yalaoui Billal attaché de recherche au CERIST : « La nouvelle version Web de la revue RIST », 16 avril 2013.

Dr Djamel Lakhal (CEO de la société suisse ASCOMP spécialisé dans le développement de logiciels de simulation pour le domaine dynamique des fluides &transfert de masse et de chaleur) : « Presentation of the CFD code TransAT of ASCOMP Switzerand », 22 avril 2013.

M.Messaoud Chaa attaché de recherche au CERIST : « Apprentissage d'ordonnancement en recherche d'information structurée », 07 mai 2013.

Dr Ahcene Bendjoudi CERIST : « Hybridation de Méthodes Exactes Arborescentes etApprochées sur GPU », 02 mai 2013.

M. Nadir Bouchama attaché de recherche au CERIST : « Sur l'Amélioration des Performances de la VoIP dans les réseaux Ad hoc »,16 mai 2013.

M. Abderazek Seba attaché de recherche au CERIST : « Sur l'Amélioration des Performances de la VoIP dans les réseaux Ad hoc », 06 Juin 2013.

Pr Hassan Ait-Kaci l'université de Lyon : « Présentation du projet chaire d'excellence ANR CEDAR , 12 Juin 2013.

Melle Nadia Aliouali attachée de recherche au CERIST : «Les enjeux de la diffusion des thèses en ligne», 12 juin 2013.

Melle Lydia Chalabi attachée de recherche au CERIST : « Open Access in developing countries: African Open Archives »,25 juin 2013.

RAPPORTS DE RECHERCHE INTERNES

(http : // www.cerist.dz/publications)

Samira Bouchama, Latifa Hamami, Hassina Aliane, Error Drift Compensation for Data Hiding of the H.264/AVC. Alger: CERIST: 2013. ISRN CERIST-DTISI/RR--13-000000012—dz

http://dl.cerist.dz/handle/CERIST/224

Khaled Chait, Omar NOUALI, Designing Energy Efficient Virtualized Web Servers. Alger: CERIST: juin 2013. ISRN CERIST-DTISI/RR--13-000000016--dz

http://dl.cerist.dz/handle/CERIST/366

Fouzia Bourai, Hassina Aliane, L'Ingénierie des Ontologies et Modèles de Connaissances. Alger: CERIST: 2013. ISRN CERIST-DTISI/RR--13-000000017—dz

http://dl.cerist.dz/handle/CERIST/225

Djamel Djenouri, Antoine Bagula, On the Relevance of Using Interference and Service Differentiation Routing in the Internet-of-Things. Alger: CERIST: 2013. ISRN CERIST-DTISI/RR--13-000000018—dz

http://dl.cerist.dz/handle/CERIST/228

Rachid Aliradi, Classification of color textured images using linear prediction errors and support vector machines. Alger: CERIST: 2013. ISRN CERIST-DSISM/RR--13-000000019-1—dz

http://dl.cerist.dz/handle/CERIST/229

Fatma Zoha Bessai, Toward a neural aggregated search model for semi-structured documents. . Alger: CERIST: juillet 2013. ISRN CERIST-DTISI/RR--13-000000021—dz

http://dl.cerist.dz/handle/CERIST/367

Imane Benkhelifa, Nadia Nouali- Taboudjemat, Sensor Technologies for Disaster Management Information Systems. Alger: CERIST: juillet 2013. ISRN CERIST-DTISI/RT--13-000000023--DZ

http://dl.cerist.dz/handle/CERIST/213

CERIST

Bases de données documentaires

Accessibles sur : www.cerist.dz

SYSTÈME NATIONAL DE DOCUMENTATION EN LIGNE

Le CERIST permet l'accès à une documentation électronique nationale et internationale couvrant tous les domaines scientifiques et techniques grâce au Système National de la Documentation en Ligne (SNDL).
Ce système concerne les chercheurs, les enseignants chercheurs et les étudiants.

De plus amples informations sont disponibles sur le site
www.sndl.cerist.dz

Directeur de publication

Pr. BADACHE Nadjib

Dossier : LES DISPOSITIFS LÉGAUX DE LUTTE CONTRE LA CYBERCRIMINALITÉ

Réalisé Par : **Bouder Hadjira**
Attachée de Recherche
Division Recherche et Développement en Sciences de l'Information

Rubrique : Les Conseils de DZ - CERT

L'ÉQUIPE DZ-CERT

Rubrique : Zoom sur un Projet

Bouder Hadjira

Comité de communication et de rédaction

BEBBOUCHI Dalila

BENNADJI Khedidja

DJETTEN Fatiha

Photographies

ALIMIHOUB Dahmane

Réalisation graphique

BOUKEZOULA Mohamed Amine

BENABDERRAHIM KAHINA

Publié par le CERIST

5, rue des 3 Frères Aissou. Ben Aknoun. BP 143, 16030 - Alger

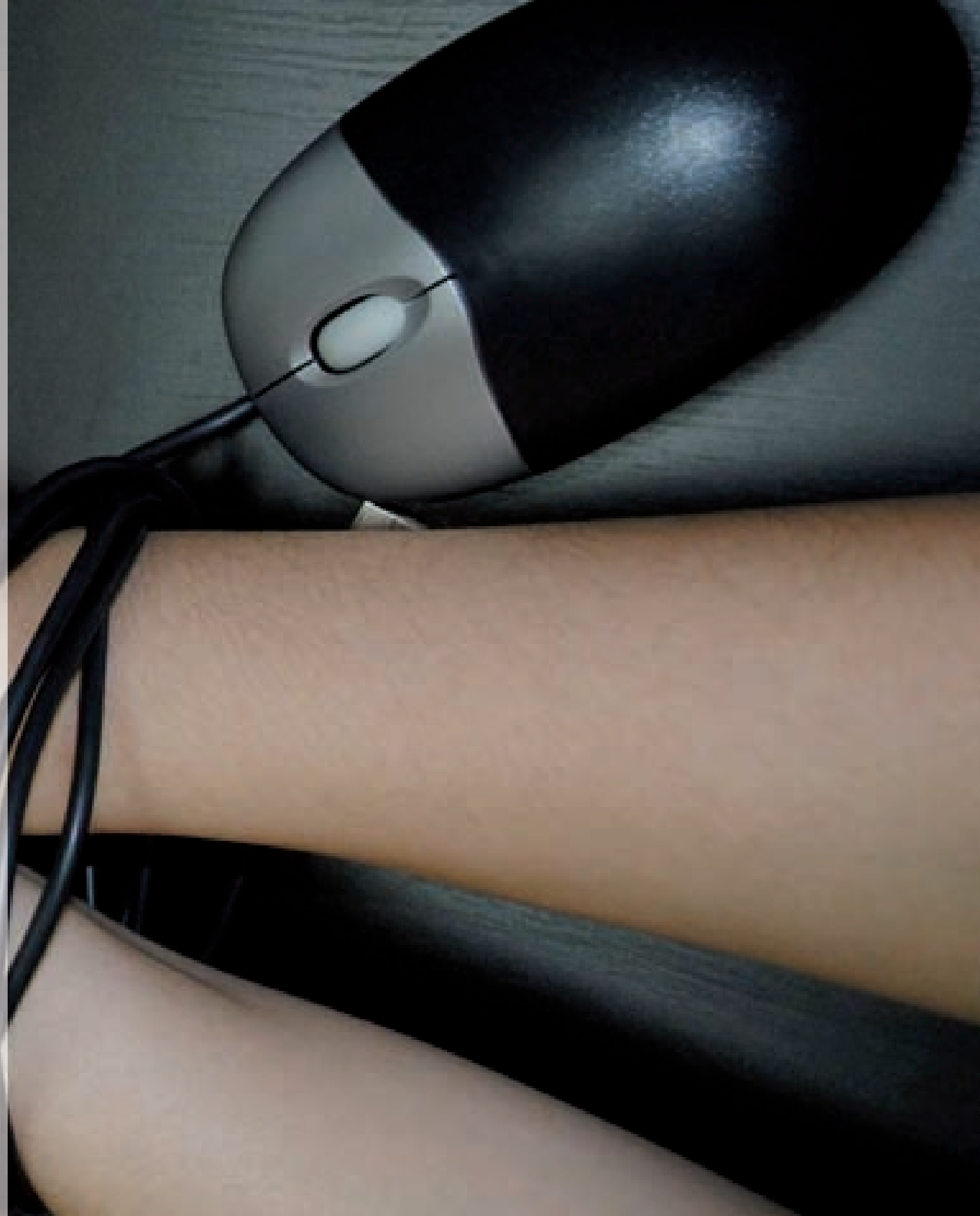
Tél : +213 (21) 91 62 05 – 08 / Fax : +213 (21) 91 21 26

E - mail : vrr@mail.cerist.dz
www.cerist.dz

Impression

ANEP

ISSN : 2170-0656 / **DÉPÔT LÉGAL :** 2690-201



Le Bulletin CERISTNEWS

CENTRE DE RECHERCHE SUR L'INFORMATION SCIENTIFIQUE ET TECHNIQUE - CERIST
5, Rue des Trois Frères Aissou, Ben - Aknoun - BP 143. 16030 - Alger
Tél : +213 (21) 91 62 05 - 08 / Fax : +213 (21) 91 21 26
www.cerist.dz