وزارة التعليـم العالـي والبحث العلمـي

المركـز الجامعـي سي الحواس – بريكـة– الجزائر

معهد الحقوق والعلوم الاقتصاديـة

ومخبر آفاق الحوكمة للتنمية المحلية المستدامة

شهادة مشاركة

يشهد مدير معهد الحقوق والعلوم الاقتصادية بالمركز الجامعي سي الحواس بريكة ورئيس الملتقى :

أن الأستاذة: فريجة مروة، جامعة غرداية، قد شارك (ت) في الملتقى الوطني حول: "الجرائم الماسة بأمن المعلومات في القانون الدولي والوطني"المنعقد بالمركز الجامعي سي الحواس بريكة يوم: 09/ديسمبر/2021، بمداخلة موسومة بـ : المخاطر الرقمية وأمن المعلومات في ظل الذكاء الصناعي.

رئيس الملتقى

الملتقى الوطني: الجرائم الماسة بأمن المعلومات في القانون الدولي والوطني

رئيس الملتقى

د.نويس نبيل

مديرة المعهد

مديرة معهد الحقوق و العلوم الاقتصادية

د.شهيرة بولحية

وزارة التعليم العالي و البحث العلمي

معهد الحقوق و العلوم الاقتصادية

المركز الجامعي - بريكة

وزارة التعليم العالي والبحث العلمي المركز الجامعي سي الحواس بريكة معهد الحقوق والعلوم الاقتصادية مخبر آفاق الحوكمة للتنمية المحلية المستدامة	برنامج الملتقى الوطني بتقنية التحاضر عن بعد **GOOGLE MEET** **الجرائم الماسة بأمن المعلومات في القانونالدولي والوطني** **يوم 09 ديسمبر 2021**

الجلسة الافتتاحية الساعة 08.30

تلاوة آيات بيانات من القرآن الكريم

الاستماع إلى النشيد الوطني

كلمة رئيس الملتقى

كلمة مدير معهد الحقوق والعلوم الاقتصادية

كلمة مدير المركز الجامعي سي الحواس بريكة (الافتتاح الرسمي)

الجلسة الأولى رئيس الجلسة: أ.د. بن سعيد عمر الساعة 09.00 هذه الجلسة تكون لجميع المشاركين على الرابط الأول			
بريشي إيمان	علاقة الأمن المعلوماتي و باقي الجرائم الإلكترونية المشابهة على غرار الأمن السيبيراني و جرائم الإعتداء على الملكية الفكرية	جامعة أبو بكر بلقايد تلمسان	10 د
زناتي محمد السعيد جواج يمينة	الجرائم الماسة بأمن المعلومات في التشريع الجزائري والاتفاقيات الدولية	1-جامعة الحاج لخضر باتنة -جامعة مستغانم	10 د
فيلالي فاطيمة	الجريمة المعلوماتية وخصائصها	جامعة مولاي الطاهر سعيدة	10 د
كربوش أحمد عثماني علي	الجريمة المعلوماتية دراسة نظرية	المركز الجامعي آفلو المركز الجامعي آفلو	10 د
طحرور فيصل	حماية المعلومات والوثائق الإدارية في ظل الأمر 21-09 المتعلق بحماية المعلومات والوثائق الإدارية والأمر 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها	جامعة محمد لمين دباغين سطيف 2	10 د
رقاد حليمة	الخصوصية الرقمية والحق في الأمن المعلوماتي: دراسة في المفهوم والدلالات	جامعة عبد الحميد ابن باديس مستغانم	10 د

زيبار الشاذلي قطاف محمد	دور المديرية العامة للأمن الوطني في مواجهة الجرائم الواقعة على أنظمة المعالجة الآلية للمعطيات	المركز الجامعي بريكة المركز الجامعي بريكة	10 د
عيسى زهية لميز أمينة	صعوبة الإثبات الجنائي في الجرائم المعلوماتية	جامعة أمحمد بوقرة، بومرداس	10 د
تواتي نصيرة	المعاملة الاستثنائية لجريمة المساس بأمن المعلومات في ضوء قانون الإجراءات الجزائية الجزائري	جامعة بجاية	10 د
الجلسة الثانية رئيس الجلسة د.بن الشيخ نور الدين الساعة 10.00 على الرابط الأول للمتدخلين في هذه الجلسة			
زعادي محمد جلول	حماية البيانات الشخصية كوجه من أوجه تكريس الأمن السيبراني: دراسة في ضوء الإتفاقيات الدولية	جامعة آكلي محند أولحاج بالبويرة	10 د
فحيمة إيمان بن بختي عبد الحكيم	الجهود الدولية لحماية الأمن المعلوماتي في ظل تنامي الجريمة الالكترونية العابرة للحدود	جامعة أبوبكر بلقايد تلمسان جامعة أبوبكر بلقايد تلمسان	10 د
الحاج علي بدر الدين مزوري إكرام	الآليات الدولية لحماية المصنف الرقمي	المركز الجامعي مغنية المركز الجامعي مغنية	10 د
بن أحمد نادية ضبع عامر	الإستراتيجيات الدولية والإقليمية في مواجهة الجرائم المستحدثة"الإرهاب الإلكتروني نموذج"	جامعة جيلالي ليابس سيدي بلعباس	10 د
عتيق علي بن بوعبد الله مونية	حماية البيانات الشخصية على ضوء القانون الدولي	جامعة محمد الشريف مساعدية سوق أهراس	10 د
عمراني نادية جماد سمية	جهود الانتربول في مكافحة الجريمة السيبرانية في أفريقيا	جامعة البليدة 2	10 د
عباوي نجاة	دور الهيئات الوطنية والدولية في مكافحة جرائم أنظمة المعلومات	جامعة طاهري محمد بشار	10 د
صابرة شعنبي	مكافحة الجريمة المعلوماتية دوليا– تسليم المجرمين–	جامعة العربي التبسي تبسة	10 د
بوقجوطة فؤاد	الجهود الدولية والإقليمية في مجال مكافحة الجرائم الماسة بأمن المعلومات	جامعة بن يوسف بن خدة الجزائر 1	10 د
سليماني لخميسي بوبشيش رفيق	السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية	المركز الجامعي بريكة جامعة الحاج لخضر باتنة 1	10 د
مقدم الياسين كروش بريكي	مكافحة الجريمة المعلوماتية في ظل اتفاقية بودابست	جامعة محمد بوضياف المسيلة	10 د
لوكال مريم	"قراءة في اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014"	جامعة امحمدبوقرة بومرداس	10 د
بولحية شهيرة حملاوي نجاة	الآليات القانونية لمكافحة الجريمة المعلوماتية في التشريع الجزائري	المركز الجامعي بريكة المركز الجامعي إليزي	10 د
بن سعيد صبرينة قادري نادية	أمن المعلومات الواقعة على النظم البيومترية والمغنطة	المركز الجامعي بريكة	10 د

الجلسة الثالثة رئيس الجلسة د. محمودي سماح 10.00على الرابط الثاني للمتدخلين في هذه الجلسة			
بحباح أحمد براهيم	**La politique de la Chine en matière de cyber sécurité**	المعهد الوطني للاتصالات وتكنولوجيات الإعلام والاتصال/INT.TIC Oran	10 د
موساوي سعاد تقرورت محمد	تعزيز الأمن المعلوماتي كآلية لمحاربة الجريمة الالكترونية في الجزائر	جامعة حسيبة بن بوعلي بالشلف جامعة حسيبة بن بوعلي بالشلف	10 د
سوماتي شريفة	الحماية الجزائية لسرية المعلومات من خطر الجريمة الالكترونية على ضوء الأمر 21-09 يتعلق بحماية المعلومات والوثائق الإدارية	جامعة الجيلالي بونعامة خميس مليانة	10 د
بن بوعزيز آسية ميلود بن عبد العزيز	خصوصية المتابعة أمام القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال	جامعة الحاج لخضر باتنة 1	10 د
يتوجي سامية	المنظومة التشريعية لمكافحة الجريمة المعلوماتية في الجزائر	جامعة محمد خيضر بسكرة	10 د
بن حمودة مختار	الجرائم الواقعة على النظام المعلوماتي والعقوبات المقررة لها	جامعة غرداية	10 د
قروي سميرة	الحماية الجزائية للمعلوماتية في التشريع الجزائري	جامعة محمد لمين دباغين سطيف 2	10 د
بلعباس عبد الحميد	الإطار المفاهيمي للجرائم الماسة بأمن المعلومات	جامعة محمد بوضياف- المسيلة	10د
قدة حبيبة	مكافحة الجرائم المعلوماتية في ظل قانون العقوبات الجزائري	جامعة قاصدي مرباح ورقلة	10 د
ماوي فاطمة	الجرائم السيبرانية وتداعياتها على أمن المعلومات.	جامعة الجزائر 1	10د
حلابي عبد القادر	جريمة التحرش الجنسي الالكتروني ضد الأطفال، وكيفية التعامل معه	جامعة غرداية	10 د
بودقزدام سامية	سبل و آليات مكافحة الجرائم الالكترونية: قراءة في التجربة الجزائرية	جامعة بن يوسف بن خدة الجزائر 1	10 د
د. نبيل نويس	إساءة استخدام تكنولوجيا المعلومات من منظور القانون الدولي	المركز الجامعي بريكة	10د
د. العطراوي كمال ط.د. بصوف صديقة	خصوصية التحقيق في الجرائم المعلوماتية.	المركز الجامعي بريكة	10د
زغبيب نور الهدى	تجريم المساس بمبدأ سرية المعالجة الآلية للمعطيات الجينية في البيئة الافتراضية-دراسة في التشريع الجزائري-	جامعة العربي بن مهيدي أم البواقي	10 د
خليفي فتيحة	خصوصية التفتيش في البيئة الرقمية	جامعة بلحاج بوشعيب، عين تيموشنت	10 د
بن دادة سهيلة	جريمة التنمر الإلكتروني، أثارها وسبل مواجهتها في المجتمع الجزائري	جامعة باجي مختار عنابة	10 د
عزوز سارة دقايشية زهور	القصر والجريمة المعلوماتية: جريمة الاستغلال الجنسي للقصر عبر الانترنت -نموذجا-	جامعة الحاج لخضر باتنة 1	10 د
عبد الحميد عائشة	إقرار آلية الترصد الوقائي لجريمة الإرهاب وأمن الدولة في ظل قانوني الإجراءات الجزائية والقانون رقم 09-04.	جامعة الشادلي بن جديد الطارف	10 د
بوقندورة عبد الحفيظ	تدابير التصدي للجرائم المعلوماتية: جهود التكامل البيني والمؤسساتي	جامعة أم البواقي	10 د
ملوك محفوظ	الاعتداء الإلكتروني على الأموال في التشريع الجزائري	جامعة محمد لمين دباغين سطيف 2	10 د
سليماني عبد الحكيم بوريش مهني	حماية وتأمين وسائل الدفع في التجارة الإلكترونية – مع الإشارة إلى حالة الجزائر	المركز الجامعي بريكة جامعة محمد بوضياف المسيلة	10 د
دعاس آسية	الإرهاب الالكتروني ومخاطره على الأمن القومي	الجامعة الإسلامية العالمية بماليزيا	10 د

د. طويرات عبد الرحمان د. برابح منير	القواعد الإجرائية لمكافحة الجريمة المعلوماتية في التشريع الجزائري	المركز الجامعي بريكة	10د
وراني حياة	الحماية الجزائية للأنظمة المعلوماتية من الإعتداءات في قانون العقوبات الجزائري	جامعة الحاج لخضر باتنة 1	10 د
قفاف فاطمة قلات سومية	جرائم المساس بالمعطيات الشخصية – وفقا للقانون 18-07-	المركز الجامعي بريكة جامعة محمد خيضر بسكرة	10 د
الجلسة الرابعة	**رئيس الجلسة د. زيبار الشاذلي الساعة 11.30**	**على الرابط الأول للمتدخلين في هذه الجلسة**	
توتاي غزالة	دور أنظمة الذكاء الاصطناعي في مواجهة جرائم أمن المعلومات	جامعة أبوبكر بلقايد تلمسان	10 د
فريجة مروة	المخاطر الرقمية وأمن المعلومات في ظل الذكاء الصناعي	جامعة غرداية	10 د
عكوش حنان نسراقي محند الزين	المعلوماتية وانعكاساتها على ملكية المؤلف للمصنفات الرقمية	جامعة عمار ثليجيالاغواط جامعة الجيلالي اليابس سيدي بلعباس	10 د
ونوغي نبيل	نظام الملكية الفكرية وعلاقته بأمن المعلومات	المركز الجامعي سي الحواس– بريكة	10 د
محمودي سماح طرشي عبد المؤمن	حق المستهلك الالكتروني في حماية معطياته الشخصية في قانون التجارة الإلكترونية	المركز الجامعي سي الحواس– بريكة	10 د
رحالي سيف الدين	المراقبة الالكترونية إجراء مستحدث للحصول على الدليل الجنائي	جامعة أمحمد بوقرة بجامعة بومرداس	10 د
د. يوسفي علاء الدين ط.د. عزوز صباح	الإطار الايتمولوجي للجريمة المعلوماتية: قراءة في تطور المفهوم والخصائص.	المركز الجامعي بريكة جامعة المسيلة	10د
مباركي إيمان زوقار وفاء	دور الذكاء الاصطناعي في تفعيل الأمن المعلومات	جامعة محمد خيضر بسكرة	10 د
عزيز مختاري	الإطار المفاهيمي للجريمة المعلوماتية	المركز الجامعي بـريكة	10 د
د.باهي هشام د. دهمة مروان	الجرائم المعلوماتية: المفهوم والضوابط القانونية	جامعة ورقلة جامعة غرداية	10 د
حيرش نور الدين بن زيان سعادة	مفهوم الجرائم الماسة بأمن المعلومات في القانون الجزائري	جامعة معسكر جامعة معسكر	10د
ساكري زبيدة حليتيم وناس	الإطار المفاهيمي للجريمة المعلوماتية في التشريع الجزائري	المركز الجامعي بريكة جامعة الأغواط	10 د
رزاق رزيقة	جرائم المكون الرقمي.. من أجل قراءة أنثروبولوجية	جامعة باجي مختار عنابة	10 د
قبايلي محمد	جرائم الملكية الفكرية الرقمية وطرق مكافحتها	المركز الجامعي بريكة	10 د
سعيدي كريم	طرق معالجة الجريمة الالكترونية في التشريع الجزائري	المركز الجامعي بريكة	10 د
الجلسة الخامسة	**رئيس الجلسة د. عباسي سهام الساعة 11.30**	**على الرابط الثاني للمتدخلين في هذه الجلسة**	
قطاف سليمان بن معيزة محمد	مواجهة صعوبات التعاون الدولي في مكافحة الجريمة المعلوماتية	جامعة عمار ثليجي الأغواط جامعة محمد خيضر بسكرة	10 د

مجدوب نوال	جريمة الإرهاب الإلكتروني كصورة للجريمة المعلوماتية	المركز الجامعي مغنية	10 د
إخلف سامية	الإطار المفاهيمي للجريمة المعلوماتية	جامعة عبد الحميد ابن باديس مستغانم	10 د
طوير إحسان	الإطار المفاهيمي للجريمة الالكترونية: دراسة في الماهية والأركان والخصائص	جامعة جيلالي ليابس سيدي بلعباس	10 د
أركام جودي الشيخ فريد	النظام الإجرائي للجرائم الماسة بأمن المعلومات في التشريع الجزائري	جامعة آكلي محند أولحاج بالبويرة جامعة آكلي محند أولحاج بالبويرة	10 د
ليراتني فاطمة الزهراء ناصري سفيان	نظام تسليم المجرمين كآلية دولية لمواجهة الجريمة المعلوماتية	جامعة العربي بن مهيدي أم البواقي	10 د
عبد الكافي مريم بورباية صورية	التقسيمات الفقهية والقانونية للجرائم الالكترونية	جـــامعة طاهري محمد بشـــــار	10 د
قنوس إناس	أمام صعوبة كشف الهوية الافتراضية لمرتكبيها، والقوانين الردعية للمشرع الجزائري للحد من استفحال الظاهرة	جامعة دالي إبراهيم الجزائر3	10 د
مرجال عائشة	آليات حماية المعطيات الشخصية في ظل المعاملات الالكترونية بالجزائر	المركز الجامعي بريكة	10د
شراد صوفيا ايناس رقيق	أثر التجسس الالكتروني علي الأمن القومي للدول	جامعة محمد خيضر بسكرة جامعة محمد خيضر بسكرة	10 د
حمدان محمد الطيب	التعاون الأمني السيبراني بين الكيان الصهيوني والمغرب وتأثيره على الأمن القومي الجزائري	جامعة محمد خيضر بسكرة	10 د
قروج رؤوف بشير راضية	مواجهة الجريمة المعلوماتية بين التحديات والعقبات	جامعة الإخوة منتوري قسنطينة 1 جامعة محمد بوضياف المسيلة	10 د

وزارة التعليم العالي والبحث العلمي

المخاطر الرقمية وأمن المعلومات في ظل الذكاء الاصطناعي

طالبة دكتوراه/فريجة مروة

طالبة دكتوراه مسجلة بالسنة الثالثة

كلية الحقوق والعلوم السياسية

جامعة غرادية

جمهورية الجز ائر

معلومات الأستاذ المشارك:

الاسم: مروة

اللقب: فريجة

المؤهل العلمي: دكتوراه

المؤسسة المستخدمة: كلية الحقوق والعلوم السياسية جامعة غرادية/الجزائر

رقم الهاتف: 0794.33.56.22

البريد الالكتروني: fridjamarwa@gmail.com

رقم المحور: المحور الرابع (04) (حماية الأمن المعلوماتي وعغلاقته بالذكاء الاصطناعي)

عنوان المداخلة: المخاطر الرقمية وأمن المعلومات في ظل الذكاء الاصطناعي

مقدمة:

إن العصر الرقمي أفرز إفرازات سلبية تتشكل معاناة يتم العمل على التصدي لها بمجهود ووسائل تنجح أحيانا وتتحقق أحيانا أخرى ولعل من أكثر هاته السلبيات ما أصطلح عليه بـ " أمن المعلومات " حيث عمل على تحقيق وسائل وآليات تضمن الحماية التقنية والإدارية للمعلومات واستراتيجية المعلومات حيث أسهمت الاستخدامات المتزايدة للذكاء الاصطناعي في عدد كبير من المجالات التجارية والصناعية والمعلوماتية والأمنية وغيرها، حيث أن الذكاء الاصطناعي يساهم بشكل كبير في التطور الرقمي مستقبلا وفي جميع المجالات والميادين سواء التجارية أو الاستثمارات الحكومية أو غيرها من المعاملات الإلكترونية والإعلام ولقد بات موضوع الأمن المعلوماتي يؤكد أهمية كبيرة لاعتباره الأداة الفعالة في حماية سرية المعلومات والمحافظة عليها فيقدم التقنيات الرقمية بسرعة كبيرة ساهمت في وقوع مخاطر باحتمال كبير للتهديدات أو الهجمات المعلوماتية حيث أصبح على المقيمين في عالم المعلومات تبين آليات محكمة حماية لعدم تسلسل الفيروسات الحاسوبية أو قرصنة المعلومات التي يقوم بها مجموعة من الأفراد ملقبون بالهاكرز عاثوا فيها فسادا وتخريبا. إذا هل يعتبر الأمن المعلوماتي استراتيجية متطورة لحماية العالم الرقمي من المخاطر والتهديد الإلكتروني بالرغم من استراتيجيات الذكاء الاصطناعي، وكيف ساهمت هاته الاستراتيجيات في عالم المعلومات من أجل التدابير الوقائية؟

من أجل الإجابة على هاته الإشكالية سوف نتناول الخطة التالية وتبيان ذلك في مداخلتنا أمامكم.

- المبحث الأول: الذكاء الاصطناعي والأمن المعلوماتي

  المطلب الأول: مفهوم الذكاء الاصطناعي

  المطلب الثاني: أمن المعلومات ومصادرها ومسؤوليتها
- المبحث الثاني: أمن المعلومات الإلكترونية ووسائل المكافحة التي يمثلها الذكاء الاصطناعي

  المطلب الأول: الإجراءات والتدابير الواجب اتخاذها لحماية المعلومات

  المطلب الثاني: شروط حماية المعلومة والأدلة الرقمية

المبحث الأول: مفهوم الذكاء الاصطناعي والأمن المعلوماتي

قبل تحديد مفهوم للذكاء الاصطناعي نشير إلى أن المبدأ الأساسي الذي يقوم عليه علم الذكاء الاصطناعي لا يكمن في حل الإشكاليات بسرعة أكبر في معالجة المزيد من البيانات أو في حفظ أكبر عدد من المعلومات، ولكن المبدأ الأصح الذي يقوم عليه هذا المجال هو مبدأ معالجة المعلومات مهما كانت طبيعتها وحجمها بطريقة آلية أو نصف آلية وبشكل مناسب ومتوافق مع هدف معين.

المطلب الأول: مفهوم الذكاء الاصطناعي

رغم اختلافات الأكاديميين والفلاسفة في إعطاء تعريف محدد ودقيق لتحديد معنى مصطلح الذكاء الاصطناعي، إلا أنهم اتفقوا على أنه ومنذ ظهور أوائل البحوث في سنوات 1950 أن الذكاء الاصطناعي هو التيار العلمي التقني الذي يضم الطرق والنظريات والتقنيات التي تهدف إلى إنشاء آلات قادرة على محاكاة الذكاء، ويعتبر المتخصصون في علم الآليات والمعلوماتية أن هذا التعريف واضح ويلم بمجالهم، بينما يشير آخرون إلى أن هذا النص غير واضح كتعريف كامل نظرا لطبيعته في حد ذاتها كعلم العصر الحديث معتمد على التجديد والابتكار والتغير.

وفي معظم الأحيان يلاحظ على الذكاء الاصطناعي أنه علم معرفي وليس علم تقني ويرجع ذلك لتاريخه كونه بدأ بأعمال بحث لمجموعة من باحثين في علم الأعصاب الحسابي والمنطق الرياضي قبل نسخها كفرع من علوم الحوسبة، نظرا لتعميم استخدام الخوارزميات لكن ما اتفق عليه الجميع هو أن دورها الأساسي يقوم على البحث عن طرق حل للإشكاليات ذات التعقيد المنطقي الحسابي أو الخوارزمي العالي قبل ظهور البيانات الضخمة، ولقد كان طموح الذكاء الاصطناعي يكتفي بتقليد الإنسان في تطبيقات معينة من وظائفه المعرفية لكن مع التسارع المشهود على أمل الوصول إلى الاستخدامات المختلفة.

إذن من خلال مفهوم وتعريف الذكاء الاصطناعي تظهر لنا أهداف الذكاء الاصطناعي حيث تعطي لنا أربعة أهداف مختلفة:

1/ نظم تفكر مثل الإنسان

2/ نظم تفكر بشكل عقلاني

3/ نظم تعمل مثل الإنسان

4/ نظم تعمل بشكل عقلاني

الفرع الأول: تطبيقات الذكاء الاصطناعي:

للذكاء الاصطناعي عدة تطبيقات نذكر منها ما يلي:

1) التفاعل مع النظام المرئي: يقصد به تطبيقات الذكاء الاصطناعي التي تستطيع أن تفسر وتحلل ما يتم إدخاله لها من صور كبرامج التعرف على الوجه وتحليل الصور للتعرف إلى الموقع.
2) التفاعل مع الكتابة اليدوية: مثل تطبيقات التعرف إلى الخط المكتوب باليد سواء كانت عملية الكتابة على الورق أو على شاشة الجهاز نفسه.
3) الروبوتات الذكية: تقوم الروبوتات الذكية بالأعمال التي يقوم بها البشر وتتميز بقدرتها على الإحساس بالعوامل المحيطة كالضوء والحرارة والصوت والحركة وذلك عن طريق مستشعرات خاصة وأهم ما يميز هذه الروبوتات أنها قادرة على التعلم من تجاربها السابقة والاستفادة من الأخطاء.

4) التفاعل مع الصوت المنطوق: تستخدم بعض تطبيقات الذكاء الاصطناعي للاستماع إلى الكلام وفهم معانيه، حتى لو كانت الصوت في جو من الفوضى أو منطوق باللهجة العامية.

5) تطبيق سيري (SIRI): هو عبارة عن خدمة صوتية تتيح للمستخدم التعامل مع الهاتف من خلال الأوامر الصوتية، يعمل على أجهزة (آبل)، حيث يحول الصوت إلى كلمة ويبحث عنها على الأنترنت ليلبي طلبات مستخدميه.

6) موقع أمازون: يحدد اذكاء الاصطناعي البضائع التي تثير اهتمام المستهلك ويقترحها عليه من خلال تعلم الحاسوب الأنماط التي يتبعها المستهلك عند البحث أو التصفح وبفضل هذا البرنامج زادت مبيعات الموقع فأكثر من ثلث مبيعاته تأتي من هذه التوصيات، يستخدم أمازون تقنية الذكاء الاصطناعي منذ أكثر من 20 سنة.

7) نتفلكس: تقدم منصة (NETFLIX) اقتراحات للمشاهدة بناء على معرفتها ما يفضله وما يعجبه، وذلك بفضل الذكاء الاصطناعي، إذ تحليل (نتفلكس) ما يفضله المشاهد وبناء على ذلك تقترح عليه الأعمال والأفلام.

8) الألعاب الإلكترونية: باتت الألعاب الإلكترونية منتشرة بشكل كبير وكل يوم يتم اختراع لعبة جديدة أو تطوير لعبة قديمة، ويتم استخدام أنظمة الذكاء الاصطناعي، حيث تتطلب هذه الألعاب تفكيرا استراتيجيا، كلعبة البوكر ولعبة الشطرنج.

9) مواقع التواصل الاجتماعي: تستخدم شبكة التواصل الاجتماعي تطبيقات الذكاء الاصطناعي مثل فيسبوك للكشف عن وجود اختراق لصور المستخدم.

الفرع الثاني: مجالات الذكاء الاصطناعي

مع التقدم السريع لتكنولوجيا الحاسبات وبفضل كون الحواسب مصممة أصلا لتحميل وتخزين ومعاملة واستخدام المعلومات من المتوقع أن تصبح تقنيات وتطبيقات الذكاء الاصطناعي جزءا هاما من حياتنا مثل الشبكات العصبونية، Expert Systems وتنقسم إلى عدة أجزاء النظم الخبيرة AI.

- الشبكات العصبونية:

وهي عبارة عن نظم تقوم بتمثيل الذكاء بواسطة مجموعة من عناصر المعالجة تشابه العصبونات في الدماغ، وتتمثل هذه العناصر مع بعضها البعض من خلال شبكة من الوصلات الموزونة بحيث تتم معايرة هذه الأوزان من خلال التعليم كما يحدث عادة مع الإنسان، وهذه الوصلات في التقنيات الحالية قليلة جدا مقارنة مع ما هو متوفر في الدماغ، حيث يوجد بلايين الموصلات (تطبيق نظم الشبكات العصبونية في مجال محدد مثل التعرف على الأشكال).

- المنطق العائم:

وهو منطق يستخدم _ بالإضافة إلى المستويين المنطقيين المعروفين: صح/ نعم أو خطأ/لا – مستويات وسيطة مستمرة بينهما مثلا أكثر حرارة، بارد نوعا ما، وهو بذلك محاولة لتطبيق طريقة تفكير أكثر شبهًا بالإنسان في برمجة الحواسب.

- العميل:

تتصرف لصالح شخصيات أخرى غالبا Computational Enityوهو عبارة عن شخصية حاسوبية بشرية بشكل مستقل، مثلا يمكن لشخص أن يملك عميله الخاص الذي يراقب له المقالات الحديثة وينتخب له المقالات المفضلة لديه Usenet.

*** مكونات النظم الخبيرة: يتألف النظام الخبير عادة من:**

1) واجهة ربط مع المستثمر :End User Interface معلومات، حقائق، قواعد، خبرة يقوم المستثمر باستشارة النظام من خلال واجهة الربط التي تحدد الطلبات واللغة المطلوب استخدامها، ويقوم النظام بالاستفسار من المستثمر بواسطة نفس الواجهة ليحصل على المعلومات اللازمة لأخذ القرار.
2) قاعدة معرفة Knoledge Base: تحتوي قاعدة المعرفة على كل " المعارف " التي يستخدمها الخبير البشري لحل مشاكل المجال المحدد.

المطلب الثاني: أمن المعلومات ومسؤوليتها ومصادرها

تعتبر المعلومات في الوقت الراهن سلعة أو خدمة وهي مصدر قوة سياسية وعسكرية واقتصادية لأنها ترتبط بمختلف مجالات النشاط الإنساني وتتداخل معه في جوانب الحياة العصرية حيث أصبح الوعي بها مظهرا لتقدم الشعوب.

ولقد أصبحت المعلومات في بنية اليوم ترتبط بشتى مجالات الحياة وتشكل ركيزة أساسية في نشاط الإنسان الاقتصادي والاجتماعي والثقافي والسياسي ... وتتيح المعرفة بالواقع ومشكلاته وأبعاد هذه المشكلات ومع هذا أصبح لها إمكانية اتخاذ القرارات في كافة المجالات تقريبا.

إن المعلومة هي تعبير يستهدف جعل رسالة قابلة للتوصيل إلى الغير، ثم إن قابليتها للتوصيل بفضل علامة أو إشارة من شأنها أن توصل المعلومة للغير فواقعة معينة أو فكرة ما لا تعتبر معلومة طالما أنها لم تأخذ شكل إشارة ملموسة فهي بطبيعتها تتطلب وجود وسط لتقوم فيه بتخزين المعلومات وقد يكون هذا الوسط عبارة عن ذبذبات كهربائية في الفضاء كموجات الراديو أو قطع وصل إلكتروني كالإشارات الرقمية في الحاسبات الآلية Electronique Switches وهذا التلاعب هو الذي يحدث في هاته الوسائط والذي من شأنه أن يعرض المعلومة للخطر، وعلى هذا هناك عدة شروط يجب توافرها في المعلومة وتتمثل هاته الشروط في:

أ) التحديد والابتكار: إن المعلومة المحددة والمبتكرة هي خصيصة أولى تفرض نفسها دائما، فالمعلومة التي تفتقر إلى التحديد لا يمكن أن تكون معلومة حقيقية، فإذا كانت المعلومة هي تعبير وصياغة محددة تجعل رسالة ما قابلة للتبليغ عن طريق علامات أو إشارات معينة فهذا يتطلب أن تكون محددة ويصبح هذا التحديد ضروريا، وبصفة خاصة في مجال الاعتداءات على الأموال فهذه الاعتداءات تفترض دائما وجود شيء محدد، أما فيما يتعلق بالابتكار فهذه صفة أساسية في المعلومة فمعلومة غير مبتكرة هي معلومة شائعة متاحة للكافة وغير مرتبطة بشخص أو أشخاص معينين.

ب) أن يتوافر في المعلومة السرية أو الاستئثار: السرية لازمة للمعلومة لأنها تحصر حركة الرسالة وتحمل المعلومة في دائرة محددة من الأشخاص، ولا يمكن تصور الجرائم الخاصة بالسرقة والنصب وخيانة الأمانة وإذا انعدم هذا الحصر لأن المعلومة غير السرية تقبل التداول.

وتكتسب المعلومة وصفها إما بالنظر إلى طبيعتها أو بالنظر إلى إرادة الشخص أو بالنظر إلى الأمرين معا، كما في حالة الرقم السري الخاص باستعمال بطاقات الائتمان، ويقلل الطابع السري وفي هذه الحالات المختلفة من استخدام المعلومات ويقصرها فقط على دائرة المؤتمنين عليها والذين يجدون أنفسهم هكذا منتفعين بحث الاستثمار عليها.

وضوابط سرية المعلومات هي ثلاثة أمور:

1-الجدية: ويقصد بها هنا الجدية النسبية وليست المطلقة، لأن المعلومة قد تكون معروفة لعدد من الأشخاص مع ذلك محتفظة بطابع السرية، فحدود سرية المعلومات فيما يتعلق بالجدية يتوقف على عدم التعاون في تعريفها وكشفها للعامة.

2-أن يكون للمعلومات قيمة معتبرة في مجالها: فقيمة هذه المعلومات تعكس حاجتها للحماية، ولا شك أن قيمة المعلومات ترتبط بسريتها وبصعوبة التوصل إليها وكلما كانت من الصعب الوصول إليها زادت قيمتها.

3-أن تتخذ تدابير للمحافظة على سريتها: لا يكفي لاعتبار السرية في المعلومات التعامل معها بجدية وأن يكون لها قيمة معتبرة في مجالها، بل لا بد من اتخاذ تدابير وإجراءات معقولة من قبل الحائز الشرعي للمعلومات للمحافظة على سريتها.

أ-مجالات الأمن المرتبط بالمعلومات:

هناك عدة أنواع ومجالات متنوعة للأمن المرتبط بنظم المعلومات نذكر منها:

1-أمن المعلومات Information Security

وهو المرتبط بالمعلومات التي هي أساس أ هدف نظام المعلومات القائم والذي يشكل عصب أو حياة المنشأة الحديثة أو الكيان أو النظام على اختلاف صيغتها اقتصادية أو إدارية وهو يعمل على حماية المعلومات ذاتها وأيضا العمل وبنفس الدرجة على حماية المخازن للمعلومات والبيانات بمعناه الفني أو الاصطلاحي.

2-أمن الوصول إلى الأنظمة Access Control

يعني عملية التأمين المعلومات المرتبطة بالأساس بعمليات العامل مع البيانات والمعلومات القائمة عليها النظام المعلوماتي، وتشمل تلك الإجراءات تأمين أو عمليات التحكم في الدخول لنظام المعلومات ذاته والتحكم في التطبيقات التي يعمل عليها نظام المعلومات وهو غالبا ما يكون على عدة مستويات طبقا للمستوى الوظيفي لمستخدم هذا النظام ودرجة احتياجه للمعلومات المراد التعامل معها بالنسبة لتخصصه الوظيفي أو للصلاحية الشريعة المسموحة له.

3-أمن برمجيات نظم المعلومات Software Security

وهي العملية التي تستهدف حماية البرامج التي تشغل أو يقوم عليه نظام المعلومات ذاته، وهي البرامج التي تحدد مسار البيانات وكيفية التعامل بها وبالمعلومات، وكيفية الاستفادة منها وتوظيفها وهي تشمل عمليات التأمين ضد القرصنة والتأمين ضد السطو من الخارج أو الداخل أو أعمال التخريب أو الاتلاف المتعمد لها.

4-أمن الاتصالات Communication Security

وهي عمليات تأمين وسائل الاتصال التي تعتمد عليها في أعمالها الوظيفية وتشمل تأمين وسائل الاتصال السلكي من خطوط تليفونية وخطوط ومسارات وكوابل نقل المكالمات وأجهزة نقل وتداول الاتصالات وأيضا محطات الاتصالات المركزية أو الرئيسية الداعمة أو المقوية للاتصالات التليفونية، كما تشمل عمليات التأمين وسائل الاتصال اللاسلكي سواء كانت وسائل اتصال لاسلكي أو وسائل اتصال لاسلكي ملحة بأجهزة أخرى.

الفرع الثاني: المسؤولية في مجال المعلومات ومصادرها:

يرى بعض الفقهاء أن المسؤولية التي تبث عبر شبكات الأنترنت هي مسؤولية موضوعية تقوم على أساس الخطأ المفترض من واقع الحيازة للمعلومات وحراستها والتي يحكمها نص المادة 138 من القانون المدني الجزائري. وهذه المسؤولية قد توجد بشقين:

- الشق الأول: يتعلق بالمسؤولية عن حراسة المعلومات وذلك بعد الاتفاق على اعتبار المعلومة شيئا غير مادي يدخل في مفهوم المادة 138 من القانون المدني الجزائري وفي هذا السياق جاء المادة 138 من القانون الفرنسي وبذلك يكون حارسها والذي يكون غالبا هو المورد المسؤول عن الأضرار التي يسببها بث المعلومة عبر الشبكة للغير ولا يعفى من المسؤولية إلا بإثبات السب الأخير.

-أما الشق الثاني فهو يتعلق بمسؤولية المتبوع عن التابع وهو يحقق في مجال الأنترنت في حالة أن تتولى شركة القيام بجميع مراحل بث المعلومة ويسأل في مواجهة الشخص المضرور في جميع هذه المراحل ويعد كل متدخل في أي مرحلة على الشبكة تابعا له ويسأل عن فعله.

ومن جهة أخرى تتنوع مصادر المعلومات فقد تكون تقليدية، وقد تكون ورقية، وقد تكون غير ورقية مخزنة إلكترونيا على وسائط ممغنطة أو ليزرية بأنواعها وبنوك المعلومات متاحة للمستفيدين عن طريق منظومة الأقراص المكتنزة (CD Rom) والمتطورة الأخرى مثل الأقراص المتعددة وأقراص (DVD).

وتتنوع مصادر المعلومات الالكترونية حسب التغطية والمعالجة الموضوعية فهناك التي تكون حسب الوسط المستخدم مثل (الأقراص الصلبة والأقراص المرنة والأقراص والأشرطة) وهناك من تكون حسب نقاط الاتاحة وطرق الوصول وهي الشبكات المحلية، قواعد البيانات الداخلية أو المحلية وشبكة الانترنت، أما المعلومات الإلكترونية التي تكون حسب التغطية والمعالجة الموضوعية والتي تكون ذات التخصصات المحددة والدقيقة، وتتناول موضوعا محددا أو موضوعات ذات علاقات مترابطة مع بعضها والتخصصات الشاملة، وهنالك التي تكون ذات توجهات إعلامية وسياسية والعامة بعد النظر عن تخصصاتهم ومستوياتهم العلمية والثقافية ومصادر المعلومات التلفزيونية وهذا النوع يعتبر من الأنواع الحديثة لمصادر المعلومات.

إن الهدف من جميع مستخدمي الأنترنت هي الحصول على المعلومات ونقلها بشكل آمن فظهرت مجموعة من التحديات التي يجب أخذها في الحسبان لضمان نقل أمن المعلومات بين الأطراف المشتركة وتنحصر هذه التحديات في ثلاث محاور هي: الخصوصية (privacy)، وسلامة المعلومات (Integrity)، والتحقق من هوية الأطراف الأخرى (peer authentication).

إن المعلومة أصبحت منفعة ومصدر قوة والحصول على المعرفة وحسن استخدامها، لكن هناك تخوف من تدني المعلومات حول مؤشرات حقوق الإنسان، خصوصا في ظل التطورات التكنولوجية المتلاحقة لموجات التطور التقني لمعالجة المعلومات وباتت مؤسسات المعلومات تهتم بالترويج للمعلومة باعتبارها سلعة وليس باعتبارها خدمة ومن هذه المؤشرات:

1-الاتجاه نحو تركيز خدمات المعلومات في عدد من شركات تقنيات المعلومات التي تهتم بالربح في المقام الأول.

2-تركيزها لدى الشركات التجارية بهذا الشكل، قد يوفر أرضا خصبة لضياع حقوق الفرد من المعلومات وذلك لحكرها على ذوي اليسار مما يلحق الضرر بالفرد.

3-استفادة المناطق الريفية ببطء وفي ذلك عدم عدالة في التوزيع بالمقارنة بالمناطق ذات الاهتمام البؤري التي تتركز فيها عناصر الخدمة، صحيح أن الاتصالات بعيدة المدى قد وفرت الكثير من الخدمات لمثل هذه المناطق النائية إلا أن لمثل هذه الأبعاد الكثير من الانتقادات.

إن مجموع القواعد التي يضعها مسؤولو الأمن يجب أن يتقيد بها جميع الأشخاص الذين يمكنهم الوصول إليه فمفهوم الأمن واسع، يشمل قواعد أصول ضبط الاتصال وانتقال المعلومات وتخزينها وحفظها، وأمن الأنظمة الالكترونية وعمليات استثمارها إضافة إلى أمن الاتصالات.

المبحث الثاني: أمن المعلومات ووسائل المكافحة التي يمثلها الذكاء الاصطناعي

أمن المعلومات هو عبارة عن دراسة وتدابير حماية وسرية وسلامة المحتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال أنظمتها في ارتكاب الجريمة وهذا هو الهدف والغرض من تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها.

ولربما يكون الهدف الأساسي لأمن المعلومات وراء حماية الموجودات المعلوماتية للمؤسسات الحكومية والأفراد من الهجمات والاختراقات التي تستهدف استخداما غير مشروع لمواردها او إحداث خال في هيكلتها أو محتواها.

هذا وتنبثق السياسة الأمنية لمؤسسة من مجموع السياسات الفنية والاقتصادية التي تنتجها في تسيير دقة أنشطتها وتصنف على ضوئها البيانات التي تقيم في نظامها المعلوماتي وسبل المحافظة عليها من الانتشار والاعلان وحمايتها من جميع أشكال الخلل والتلف.

المطلب الأول: الإجراءات والتدابير الواجب اتخاذها لحماية المعلومات

- هناك مجموعة من الإجراءات الإدارية والفنية التي يمكن استعمالها في هذا الصدد لتحقيق أمن المعلومات.

الفرع الأول: الإجراءات الإدارية لأمن المعلومات

على الحكومات التي تتبنى تقديم خدماتها الالكترونية للمواطنين القيام بعدة مهام اتجاه أمن المعلومات كالرقابة والاشراف على أمن المعلومات وسوف نذكر منها ما يلي:

أ-توفير أمن الأجهزة: لتأمين الأجهزة لا بد من تأمين المبنى كعدم السماح لغير المصرح لهم بالدخول إلى غرفة الحاسب الآلي، ومخزن وسائط التخزين وبفضل استخدام التكنولوجيا الحديثة للدخول على الأنظمة مثل: بصمة الأصبع، بصمة الوجه، البطاقة الممغنطة ... الخ.

ب-توفير أمن البيانات: يتوجب على الإدارة توزيع الصلاحيات والمسؤوليات حسب الهيكل التنظيمي بما يضمن رفع المستوى الأمني وتقليص الجرائم ووضع آلية يتم تنفيذها للقيام بالنسخ الاحتياطي وتأمين وسائط الحفظ الخارجية بما يكفل أمنها وتحديثها ويجب صياغة الضوابط المنظمة لعمليات التشغيل ولمبرمجي قواعد البيانات ومدراءها، ولإدارة الشبكات وخطوط الاتصال، والضوابط الأمنية لبناء وتشغيل البرامج التطبيقية.

ج-توفير أمن الأفراد: في حالة أرادت الإدارة حماية المعلومات عليها اتباع الإجراءات الإدارية في مجال أمن الأفراد بالشكل التالي:

- منع التوظيف المؤقت نهائيا ومراعاة إجراءات انهاء خدمة الموظف بطلب تسليم كل ما كان بحوزته كالمفاتيح والبطاقات، وتغيير كلمة المرور قبل مغادرته.
- متابعة العاملين ونقلهم إجباريا بين الأقسام في الإدارة.
- عقد ندوات ومؤتمرات ومحاضرات بشكل دوري في مجال أمن المعلومات وعرض النشرات الداخلية وتعليمات الإدارة التي تتضمن إطلاع الأفراد على المعلومات المهمة في مجال الأمن المعلوماتي.
- منح التحفيزات وربط الترقية والدورات بمدى التقيد بأمن المعلومات.
- دفع العاملين لحضور المعارض العالمية للأجهزة والبرامج، وإرسالهم إلى الدورات المتخصصة بأمن المعلومات ليكون لديهم خلفية قوية بما يكفل تحقيق أمن المعلومات.

د-توفير قسم متخصص بأمن المعلومات: تقوم المؤسسة الكبيرة بتعيين مدير أمن نظم المعلومات يرتبط بالإدارة العليا مباشرة لأهمية التقارير التي يعدها. مع تخصيص فريق مختص في مجال أمن المعلومات ومن ذوي الخبرة الفنية والأمنية في مجال البيانات

والبرمجة ونظام التشغيل ولغات البرمجة وقواعد البيانات المستخدمة في المؤسسة ومدربين على التنسيق الأمني ولديهم القدرة الكافية على التعامل مع جرائم النظام المعلوماتي والحالات الطارئة.

الفرع الثاني: الإجراءات الفنية لأمن المعلومات

أ-**توفير الحماية الإلكترونية:** تخضع الحماية الإلكترونية للإعدادات الخاصة بالحاسب الآلي وأجهزته الملحقة به ويمكن تبيانها كما يلي:

- حذف الملفات غير المهمة ولو كانت المعلومات التي تحتويها ضئيلة وعديمة الفائدة والتأكد من عدم إبقائها في سلة المحذوفات؛
- الكشف على الحاسب الآلي بعد الغياب عن طريق المستكشف وتركيب برامج تمنع مسح المعلومات منه، أو استخدام برامج تحتفظ بالعمليات التي يتم إجراؤها لعدد كثير من (Password) كنظام حماية للمرور؛
- استغلال برنامج الملفات وحمايتها بكلمة المرور؛
- التأكد من عدم وجود برامج تجسس في حالة الارتباط بشبكات في الحاسب الآلي؛
- في حالة استخدام البريد الإلكتروني يجب عدم فتح الملفات المرفقة إلا بعد التأكد منها؛
- يجب تركيب البرامج المضادة للفيروسات على الجهاز وتشغيلها طوال فترة استخدام الجهاز، ومن الضروري تحديث برنامج مستكشف الفيروسات بصورة دورية مستمرة.

ب-تأمين جميع مكونات الشبكة: في حالة استخدام الشبكات، فإن الحماية في هذه الحالة تعتمد على التحقق من الشخصية، للدخول إلى الشبكة، وعلى وسائل أمن الشبكة والتي يجب فحصها، وتقييم إمكانية اختراق نظام الحماية وتحديد تلك المخاطر المتعلقة بالتصميم والإدارة.

ج-استخدام التشفير: إرسال البيانات عبر الشبكة يجعل من السهل التنصت عليها والطريقة الوحيدة لمنع هذا هي استخدام التشفير، لأنه عملية تحويل المعلومات إلى شفرات غير Encryption يعرف التشفير مفهومة غير ذات معنى لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات أو فهمها ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مشفرة وتشكل الأنترنت الوسط الأضخم لنقل المعلومات الحساسة، قصد الحفاظ على سلامتها وأمنها فلا بد من تشفيرها.

وللتشفير ثلاثة طرق كالتالي:

-الشهادات الرقمية: تصد الشهادات الرقمية المانحة الموثوق بها التي توقع عليها وتستخدم هذه الشهادات للتحقق من موثوقية المفاتيح العامة التي أصدرت -البصمة الإلكترونية-والتي تعد بصمة رقمية يتم اشتقاقها وفقا لخوارزميات معينة تدعى دوال أو اقتران التمويه.

-التوقيع الرقمي: يستخدم التوقيع الرقمي رسالة قد جاءت من مصدرها دون تعرضها لأي تغيير أثناء عملية النقل ويمكن للمرسل استخدام المفتاح الخاص لتوقيع الوثيقة الكترونيا، أما المستقبل فيتم من التحقق من صحة التوقيع عن طريق استخدام المفتاح العام المناسب، وباستخدام التوقيع الرقمي يتم تأمين سلامة الرسالة والتحقق من صحتها وفوائد هذا التوقيع أنه يمنع المرسل من التنكر للمعلومات التي أرسلها.

-استخدام كلمات المرور: يتطلب أمان نظم المعلومات استخدام كلمات مرور معقدة لتسجيل الدخول إلى شبكة أو حاسب آلي، وتكون كلمات المرور القوية مهمة على اعتبار أن أدوات اكتشاف كلمات المرور مستمرة في التحسن وعلى

اعتبار أن أجهزة الحاسب الآلي المستخدمة لاكتشافها أصبحت أكثر فاعلية من قبل وأصبح بالإمكان اختراق كلمات المرور لكل شبكة.

إلى جانب هاته التحديات هناك بعض الوسائل لأمن المعلومات التي تهدف إلى مكافحة الجرائم المعلوماتية ويمكن تصنيف هذه الوسائل إلى:

1- الوسائل التي تتعلق بالتعرف بشخص المستخدم وموثوقية الاستخدام ومشروعيته Identification and Authorization
2- الوسائل التي تهدف إلى منع افشاء المعلومات المصرح لهم بذلك
3- وسائل حماية التكاملية وسلامة المحتوى
4- الوسائل المتعلقة بمنع الإنكار
5- وسائل مراقبة الاستخدام وتتبع سجلات النقاد والأداء

المطلب الثاني: شروط حماية المعلومة والأدلة الرقمية

هناك شروط يجب توافرها حتى تكون الحماية كافية للمعلومات الإلكترونية وتضمن نقلها بشكل آمن بين الأطراف المتصلة

الفرع الأول: الشروط الواجب تو افرها لحماية المعلومة

-السرية CONFIDENTIALITY

من الضروري حماية سرية المعلومات وإيجاد وسيلة لنيل ثقة الناس وتوفير الضمانات لهم حيال ذلك وحيال استخدام الحكومة الإلكترونية وهي من العوامل الهامة جدا بل والأساسية لنجاح الحكومة الإلكترونية لأن الأنترنت بطبيعتها هي عبارة عن عالم مفتوح من عمليات الحاسوب وبالتالي فإنها معرضة للعديد من المخاطر المتعلقة بالحماية وسرية المعلومات ومن أكثر الأساليب التي يتبعها الهاكرز أو المخترقون للنظام المعلوماتي هي البرمجيات الخبيثة والبرمجيات التجسسية.

-الموثوقية وسلامة المحتوى INTEGRITY

وهو التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله، وهنا يتم تأمين المعلومات من خلال مجموعة من الأساليب توفرها نظم قواعد المعطيات كقوائم النفاذ والصلاحيات، وفي هذا السياق لا يكون المهم الحفاظ على سرية المعلومة بل الجانب الأهم هو الحفاظ على سلامة المعلومة من التزوير والتغيير بعد إعلانها على الملأ، فقد تقوم هيئة ما بالإعلان على معلومة مالية أو غيرها تخص الهيئة وهنا يجب المحافظة على سلامة المعلومة كإعلان الجامعات عن أسماء مقبولين للعمل بها وتتمثل في حماية تلك القوائم من التزوير والتغيير.

-استمرارية توفر المعلومات AVAILABILITY

يقصد بها ايصال المعلومات والبيانات الى الاشخاص المناسبين في الوقت المناسب وضمان وصول المعلومة إلى الأشخاص المصرح لهم من خلال توفير القنوات والوسائل الآمنة والسريعة للحصول على تلك المعلومات، واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وأن مستخدم المعلومات لن يتعرض لمنع استخدامها ودخوله إليها.

-المقاومة والمرونة

وهي قدرة النظام على الحفاظ على نفسه من العمليات التي تجعله غير متاح للمستخدمين المخولين باستخدامه، أما المرونة فتتملل في توفير الإمكانيات والأدوات التي تمكن من إدارة النظام دون أن يستدعي ذلك إلى توقفه وسهولة الاستخدامCase of Use

الفرع الثاني: الأدلة الرقمية وكيفية التعامل معها

لقد انتشر في الآونة الأخيرة مفهوم الأدلة الرقمية التي تعرف بأنها القرائن والشواهد التي توجد على شكل معلومات مخزنة أو منقولة في شكل رقمي وتكون طبيعة هذه المعلومات أنها معلومات ثابتة وإثباتية يمكن من خلالها الاستدلال بها أو التأكد من قيام المستخدمين بعمل ما ومن الأمثلة على ذلك انشاء ملف في تاريخ معين به معلومات معينة ومهمة تخص القضية أو الجريمة، وإرسال بريد الإلكتروني أو وجود صور فوتوغرافية رقمية أو مخرجات أو مقاطع الصوت والفيديو الرقمية، وعادة ما يتم الحاسب الآلي ومحتوياته عن مستخدميه خاصة في عصرنا الحالي الذي أصبح فيه استخدام الحاسب الآلي في إنجاز الكثير من الاعمال والمراسلات أمر عاديا.

إن التحديات التي يقوم عليها الأمن الرقمي معقدة ويحتاج التصدي لها ضرورة توفر الإرادة السياسية اللازمة لتصميم وتنفيذ استراتيجية لتطوير البنية التحتية والخدمات الرقمية تشمل استراتيجيات متطورة للأمن المعلوماتي تكون متماسكة وفعالة، وقابلة للتحقق من إرادتها ويجب أن تكون هاته الاستراتيجيات الأمينة جزءا من نهج متعدد التخصصات ويمكن كذلك الاستجابة القوية للأبعاد البشرية والقانونية والاقتصادية لاحتياجات أمن البنية الأساسية الرقمية أن تبني الثقة، وأن تولد النمو الاقتصادي المرغوب فيه والذي يفيد المجتمع.

وعليه فإن التحكم في زمام رصيد المعلومات الرقمية وتوزيع السلع غير الملموسة وإضافة القيمة إلى المحتوى، وسد الثغرة الرقمية كلها مشاكل ذات طبيعة اقتصادية واجتماعية تستلزم شيئا أكثر من مجرد اتباع نهج وحيد البعد وتكنولوجي تجاه الذكاء الاصطناعي.

وفي هذا الفلك الرقمي أقدم المشرع الجزائري إلى سن قوانين تنصيب في إطار الأمن الرقمي، والانخراط في معاهدات إقليمية ودولية لتعزيز التعاون الدولي في هذا المجال، وتعزيز الجهود الدولية في مجال الأمن المعلوماتي.

خاتمة:

ما نلاحظه بصورة جلية أن قضية الأمن المعلوماتي أصبحت من التحديات الكبرى على الصعيدين الإقليمي والعالمي لا سيما في ظل تنامي التهديدات الإلكترونية سواء من ارتفاع الجرائم أو الأضرار الناجمة عنه ، نتج عنها خلق تحديات كثيرة أمام النظام القانوني القائم في العديد من المول، خاصة ما يتعلق بمكافحة هذه الظاهرة، وهذا الأمر الذي دعا الفقه والقضاء على البحث فيما اذا كانت النصوص القائمة كافية لمواجهة هاته الجرائم بشتى أنواعها أم أن الأمر يستدعي استحداث قوانين ونصوص خاصة قادرة على احتوائها ومراعاة طبيعتها وخصوصيتها، وانتظار التعديل التشريعي، بتضعيف قوة الصنع والتقاعس عن قدح الذهن لتطوير النصوص.

وما نستنتجه من هاته الدراسة المتعلقة بالأمن المعلوماتي أن:

- المعلومة في هذا العصر تعد كنز عظيم وهام، لاسيما في وجود تكنولوجيا المعلومات والتي ساهمت بشكل فعال في معالجة وتخزين وبث المعلومات.
- إضافة إلى المعلومات برز الأمن المعلوماتي الذي يشكل مجموعة الوسائل والطرق التي تسيطر على كافة أنواع المعلومات وحمايتها.
- أهمية العنصر البشري الذي لعب دورا هاما وفعالا في حماية المعلومات باعتماده على التقنيات الأجنبية الخاصة بأمن المعلومات.

وفي ختام دراستنا هذه نقترح بضرورة تدخل المشرع بإقرار نصوص تشريعية لمواجهة الجرائم المعلوماتية والنص على الصور المتحدثة من الأجرام المعلوماتي كتلك التي لم تكن معروفة من قبل كجرائم البريد الالكتروني.

-كما يجب أن تنهض الجهات الوطنية المسؤولة عن صياغة القوانين بإصدار وتنفيذ القوانين والضوابط التي تضمن سلامة البيئة الالكترونية، وأن تسعى بلادنا الجزائر مع بقية الدول العربية الى انشاء منظمات تهتم بالتنسيق في مجال مكافحة الجرائم المعلوماتية عبر الأنترنت، وتفعيل دور الشرطة، وتشكيل مجموعات عمل في جميع الدول العربية وزيادة الجهود الدولية في مجال مكافحة الجريمة المعلوماتية.

-وأيضا عقد دورات تدريسية مشتركة بين رجال القضاء والنيابة العامة والشرطة والخبراء المختصين بالجريمة المعلوماتية، من أجل تحقيق الهدف المتفق عليه والمتمثل في إقامة مجتمع معلومات شامل ومؤمن ومكفول للجميع.

قائمة المراجع المعتمدة:

- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، 2008.
- ذيب بن عايض القحطاني، أمن المعلومات، المملكة العربية السعودية الرياض، 2015، الفصل العاشر.
- درار نسيمة، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني، دراسة مقارنة، أطروحة دكتوراه في القانون الخاص، جامعة أبو بكر بلقايد -تلمسان-2016/2015.
- هشام فريد رستم، جريمة الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة، بحث مقدم لمؤتمر الأمم المتحدة لمنع الجريمة والذي عقد خلال 29 أفريل، مجلة الأمن، العدد151.
- نادلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية، منشورات الحبلي الحقوقية، 2005.