الملتقى الدولي: الحق في الخصوصية المعلوماتية بين النصوص القانونية والتحديات التقنية.

جامعة المغيلي الأهلية الدولية ورئيس جامعة الوفاق الدولية بالنيجر ومدير المركز المغاربي شرق أدنى للدراسات الاستراتيجية بالمملكة المتحدة

بتاريخ: 2024/09/06

" الحماية الاليكترونية للخصوصية المعلوماتية في ظل التطور التكنولوجي المعاصر."

«Electronic protection of information privacy in light of contemporary technological development. »

منار طالبي

طالب دكتوراه

جامعة الأمير عبد القادر للعلوم الإسلامية – قسنطينة- مخبر الدراسات الاقتصادية و المالية الإسلامية الايميل: talbimanar8@gmail.com

الملخص :

الخصوصية المعلوماتية أبرز المعضلات التي تسعى التكنولوجيا الحديثة لايجاد سبل و طرق للحفاظ عليها و حمايتها من كل الاختراقات الاليكترونية ، وفي ظل الجرائم المتنوعة اليوم التي تهدد الخصوصية المعلوماتية للأفراد و الجماعات و المؤسسات في مختلف القطاعات الاجتماعية اليوم، حيث تطرقنا في دراستنا هذه إلى سبل مواجهة أهم الأخطار التي تواجه هذه الخصوصيات المعلوماتية من خلال آليات حمائية تعتمد على التطور التكنولوجي المعاصر الذي يشمل مختلف القطاعات و المجالات الاقتصادية و الاجتماعية إبتداءا من تبان الأشكال العامة للتطور التكنولوجي المعاصر في أمن المعلومات و النظم الحمائية، ثمّ نأتي لنوضح دور العلاقة الخاصة بالتطور التكنولوجي المعاصر بحماية الخصوصية المعلوماتية إنتهاءا بمقصودنا من الدراسة بتوضيح كيفية توظيف التطور التكنولوجي الحديث في حماية الخصوصيات المعلوماتية من خلال الانطلاق من إشكالية واضحة توجه لنا طريق الدراسة لماهية سبل التوظيف للتطور التكنولوجي في حماية الخصوصية المعلوماتية و كيفية ذلك.

هذه الدراسة تهدف إلى الوصول لتسليط الضوء على موضوع من مستجدات عصرنا هذا في ظل التطورات التكنولوجية الحديثة و استخداماتها حيث يتمثل في ابراز تشعب التطور التكنولوجي عبر مختلف القطاعات و المجالات و أشكاله، بالإضافة إلى دوره في حماية خصوصية المعلومات فيها.

+الكلمات المفتاحية:

الخصوصية المعلوماتية، التطور التكنولوجي، النظم الحمائية.

Abstract :

Information privacy is the most prominent dilemma that modern technology seeks to find ways and means to preserve and protect it from all electronic breaches, and in light of the various crimes today that threaten the information privacy of individuals, groups and institutions in various social sectors today, where we addressed in this study ways to confront the most important dangers facing these information privacy through protective mechanisms that depend on contemporary technological development that includes various economic and social sectors and fields starting from the emergence of general forms of contemporary technological development in information security and protective systems, then we come to clarify the role of the special relationship between contemporary technological development and the protection of information privacy, ending with our purpose of the study by clarifying how to employ modern technological development in protecting information privacy by starting from a clear problem that directs us on the path of studying the nature of the ways to employ technological development in protecting information privacy and how to do so.

This study aims to shed light on a topic of the developments of our time in light of modern technological developments and their uses, which is represented in highlighting the ramifications of technological development across various sectors and fields and its forms, in addition to its role in protecting the privacy of information therein.

+Keywords:

Information privacy, technological development, protective systems.

المقدمة :

يعتبر التطور التكنولوجي السبيل الوحيد المتعلق بإيجاد الحلول للمشكلات و المعضلات التكنولوجية و الاليكترونية المعاصرة و الحديثة فنظرا لأن التطور التكنولوجي يندرج في مختلف المجالات و القطاعات الاجتماعية في المجتمعات بوسائله و آلياته المختلفة التي تؤطر و تسهل مختلف المعاملات و الأعمال العامة و الخاصة في المجتمع. فمرورا من البرامج الاليكترونية لتخزين المعلومات التي تستعملها المؤسسات و الهيئات القاعدية في الدول إلى المواقع التجارية و

منصات التواصل الاجتماعي للأفراد و الجماعات في حفظ المعلومات و حفظ الخصوصية المعلوماتية للأفراد التي تقع محل خطر محتمل متعلق بالقرصنة و الاختراقات السبيرانية.

_ فماهي سبل تحقيق الحماية الاليكترونية للخصوصية المعلوماتية في ظل التطور التكنولوجي المعاصر؟

فعلى ضوء الإشكالية السابقة يمكن طرح الفرضيات التالية:

_تختلف و تتنوع نظم حفظ الخصوصية المعلوماتية في ظل التطور التكنولوجي المعاصر

_يرتبط التطور التكنولوجي بحماية الخصوصية المعلوماتية عن طريق أشكال و نظم تكنولوجية حديثة تشكل حاجز لحماية المعلومات.

_يتم توظيف التطور التكنولوجي في حماية الخصوصية المعلوماتية بطرق و أساليب مختلفة نظرا لاختلاف المجالات و القطاعات الموظفة فيها.

حيث تهدف الدراسة لإبراز دور و أهمية التطور التكنولوجي في حماية المعلومات و الخصوصية المعلوماتية في إطار تشعب المجالات و القطاعات الاجتماعية.

و ذلك بالاعتماد على مجموعة من الدراسات السابقة أهمها:

_دراسة منار طالبي حول علاقة الذكاء الاصطناعي بالوقاية من الجرائم الاليكترونية و الاختراقات السبيرانية هدفت الدراسة إلى إبراز الدور الذي يلعبه الذكاء الاصطناعي في تعزيز الوقاية من الجرائم الاليكترونية و الاختراقات السبيرانية و توفير حماية متينة ضدها.

_دراسة نوي أحمد حول الخصوصية المعلوماتية في ظل التطور التكنولوجي و آليات حمايتها هدفت الدراسة لتسليط الضوء على تأثير التطور التقني على الخصوصية المعلوماتية للأفراد و كذا توفير آليات لحماية هاته الخصوصية على الصعيد الدولي و الداخلي.

_دراسة فاضلي سيد علي حول آثار التطور التكنولوجي على حماية الحق في الخصوصية في النظام الأوروبي لحماية حقوق الانسان هدفت الدراسة لتقديم مفهوم للخصوصية المعلوماتية و تبيان الاطار التشريعي القانوني على مستوى النظام الأوروبي لحقوق الانسان في حمايتها.

المبحث الأول : أشكال التطور التكنولوجي المعاصر في أمن المعلومات

لا يمكن لأي دولة من دول النامية على وجه الخصوص ي هذا العصر أن تعيش معزولة عن التطورات التقنية المتسارعة والآثار الاقتصادية والاجتماعية والأمنية الناجمة عنها. وفي ظل الترابط الوثيق بين أجزاء العالم عبر تقنيات المعلومات والات صالات والتطبيقات التي سمحت بانسياب الأموال والسلع والخد مات والأفكار والمعلومات بين مستخدمي تلك

التقنيات، بات من ا الضروري لكل بلد حماية أفراده ومؤسساته ومقدراته وحضارته م ن آثار هذا الانفتاح، ومع إدراك الجميع اليوم للفوائد الجمة لتقنية المعلومات، فإن المخاطر الكامنة في تغلغل هذه التقنية في بيوتنا ومؤسساتنا تتطلب من المجتمع والدولة جميعًا الحيلولة دون ح صول تلك المخاطر بشتى أنواعها، ومن أهم ما يجب توفيره في هذا الصدد حجب المواقع الضارة والتي تدعو إلى الفساد والشر و منها المواقع التي تدعو و تعلم الإرهاب والعدوان والاعتداء على الآخرين بغير وجه حق، فهذا الأسلوب يعد من الأساليب المجدي ة والنافعة.

ولقد سعت بعض الدول إلى حجب المواقع الضارة عن ق تركيب الأجهزة والبرامج التي تقوم بتنقية المواقع وحجب المواقع الضارة ومنع ظهورها 81 وهناك دول عدة إسلامية وغير اسلامية تعمد إلى ترشيح شبكة الإنترنت وحجب المواقع التي ترى أنها ضارة أخلاقيا أو فكريًا.

منذ أول حالة لجريمة موثقة ارتكبت عام 1958م في ال ت المتحدة الأمريكية بواسطة الحاسوب الآلي وحتى الآن كبر

حجم هذه الجرائم وتنوعت أساليبها وتعددت اتجاهاتها وزادت خسائرها وأخطارها، حتى صارت من مصادر التهديد البالغة للأمن القومي للدول، خصوصًا تلك التي ترتكز مصالحها الحيوية. (غريب، 2017)

حيث تعتبر البرامج الحرة والبرامج مفتوحة المصدر لبنة مهمة لتكوين قاعدة صلبة للتصدي لجميع أنواع تهديدات الأمن المعلوماتي. لذا وجب التنويه بأهميتها ونشر الوعي لدى المستعملين للتعريف بها والتعريف بخطر البرامج المغلقة. وبالتالي اختصار الكثير من الوقت والجهد في مجال الأمن المعلوماتي.

حيث يمكن أن نقول عن برنامج أنه برنامج حر إذا كانت تتوفر فيه الشروط التالية:

حرية استعمال البرنامج لأي غرض، إمكانية دراسته وتعديله ليناسب حاجات المستعمل، إمكانية نسخه، إمكانية تطويره، هذه الشروط لابد أن تكون ممكنة من الناحية التقنية والقانونية، مما يسمح لنا أن نقول بأن المستعمل يراقب البرنامج وليس العكس.

وكأمثلة عن هذه البرامج يمكن أن نذكر برنامج التشغيل لينكس، متصفح الواب: موزيلا فاير فوكس برنامج الصوتيات والمرئيات في أل سي..... و تتمثل مميزات **البرامج الحرة** في:

إتاحة المصدر لكل مستخدم الحق في الحصول على الكود المصدري للبرنامج الذي يريد استعماله، حتى يستطيع تطوير هذا البرنامج وإضافة مميزات جديدة تناسب احتياجاته أو رغباته.

مراقبة المستخدم للبرمجية و تتيح البرامج مفتوحة المصدر المستخدميها تفحص الشيفرة المصدرية والتأكد من مستوى الأمن الذي توفره.

بالإضافة للتنسيق حر لكل المستخدمين أو الذين يتعاملون مع البرامج الحرة الحق في التعاون أو تشارك الخبرات من أجل تطوير هذه البرامج.

مجتمعات حول البرمجية تعتبر البرمجيات الحرة ملكا للجميع، فهي ملك لكل من عمل على بنائها ونشر استخدامها.

حيث يتمثل أمن هذه البرمجيات الحرة بدرع قوي مقارنة بالبرمجيات المغلقة حيث تعتبر معظم المشكلات الأمنية مشاكل عامة تختلف كليا عن تلك التي تظهر في البرمجيات المغلقة، بحيث أنه عند اكتشاف أي ثغرة أو فجوة أمنية يقوم الجميع بحلها بسرعة دون الحاجة إلى العودة إلى المطور الأساس للبرنامج.

أما دور الإبداع فتحفز البرمجيات الحرة المستخدمين على الإبداع في التفكير وتحسين مستوى الإبداع لدى الشباب وتغيير طريقة التفكير التقليدية.

البرامج مفتوحة المصدر

يستخدم المصطلح عادة ليشير إلى شيفرات البرامج المتاحة بدون قيود الملكية الفكرية. وهذا يتيح لمستخدمي البرمجيات الحرية الكاملة في الاطلاع على الشيفرة البرمجية للبرامج، وتعديلها أو إضافة مزايا جديدة لها.

بتميزها بمميزات البرامج مفتوحة المصدر و تتمثل في :

حرية إعادة توزيع البرنامج، توفر النص المصدري للبرنامج، وحرية توزيع النص المصدري.،حرية إنتاج برمجيات مشتقة أو معدلة من البرنامج الأصلي، وحرية توزيعها تحت نفس الترخيص للبرمجيات الأصلية ، عدم وجود أي تمييز في الترخيص لأي مجموعة أو أشخاص،عدم وجود أي تحديد المجالات استخدام البرنامج، الحقوق الموجودة في الترخيص يجب أن تعطى لكل من يتم توزيع البرنامج إليه.

و تهدف هذه البرامج الحرة إلى البرمجيات الحرة ليست مسألة تقنية؛ ولكنها أخلاقية، اجتماعية، وسياسية. فهي

مسألة الحقوق الإنسانية الواجبة لمستخدمي البرمجيات. وبالتالي فإن الحرية والتعاون قيم أساس للبرمجيات الحرة. فعلى عكس البرامج المغلقة والتي هي برامج حكريه تشكل لغزا البرامج الحرة تعمد الى نشر المعرفة البشرية. وفي حين

ان البرمجيات الحكرية تحظر التعليم فان البرامج الحرة تدعم التعليم وتشجعه.

و يتمثل الفرق بين البرامج الحرة والبرامج مفتوحة المصدر البرامج الحرة والبرامج مفتوحة المصدر هما مفهومان متنافسان لبرامج ذات خصائص متطابقة حيث البرامج الحرة تعطي أهمية كبرى للجانب الفلسفي والسياسي

أما البرامج مفتوحة المصدر : تعنى بطريقة التطوير والنشر. (مخبر الممارسات اللغوية في الجزائر، 2015)

المبحث الثاني : علاقة التطور التكنولوجي بالحماية المعلوماتية

لا شك في أن الأمن السيبراني يمثل الدرع الرقمي الذي يحمي عالمنا المتصل بالإنترنت. وفي عصر تكنولوجيا المعلومات حيث تتداخل حياتنا مع الشبكة العنكبوتية، يصبح الأمن السيبراني أمرا حيويا للحفاظ على خصوصيتنا وأمان بياناتنا.

ويشمل الأمن السيبراني مجموعة من السياسات والتقنيات التي تستهدف الوقاية من الهجمات والحفاظ على سلامة الأنظمة الرقمية وبناء حاجز ضد التهديدات السيبرانية المتزايدة من خلال استخدام برامج مكافحة الفيروسات، وجدران الحماية، وتحديثات البرمجيات.

ويمثل تحقيق التوازن بين التقدم التكنولوجي والحفاظ على الأمن تحديًا مستمرًا يتطلب تطوير وتبني إستراتيجيات فعّالة للدفاع عن العالم الرقمي الذي نعيش فيه، حيث يلعب الأمن السيبراني في هذا العالم الرقمي المعقد دورا حيويا في حماية معلوماتنا الشخصية، وضمان استمرارية العمليات الأساسية للشركات والحكومات.

حيث يعد الأمن السيبراني بمثابة عملية لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية، وتهدف هذه الهجمات عادة إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها، وذلك بغرض الاستيلاء على المال من المستخدمين أو مقاطعة العمليات المعادية.

ويشمل الأمن السيبراني مجموعة واسعة من الإجراءات والتقنيات التي تهدف إلى حماية الأنظمة الإلكترونية والبيانات من التهديدات السيبرانية، بما في ذلك حماية البيانات الشخصية والمعلومات السرية الأخرى من السرقة أو التخريب عبر الفيروسات وبرامج الفدية.

كما يشمل حماية الشبكات والأنظمة ومنع المهاجمين من الوصول إليها، واكتشاف الهجمات السيبرانية ومعالجتها بسرعة، والاستعداد للتعامل مع الهجمات السيبرانية عبر تنفيذ التدابير الوقائية، مثل تحديث البرمجيات بانتظام، وفحص الضعف في الأمان، وتنفيذ سياسات الوصول الصارمة.

التقنيات المستخدمة

توجد العديد من تقنيات الحماية المستخدمة في مجال الأمن السيبراني، وتتنوع حسب الاحتياجات والتحديات الفردية، وإليك بعض التقنيات الرئيسية:

برامج مكافحة البرمجيات الخبيثة: تساعد تكنولوجيا مكافحة البرمجيات الخبيثة في اكتشاف وإزالة البرامج الضارة والفيروسات من الأنظمة.

جدران الحماية: تراقب حركة المرور بين الشبكة الداخلية والشبكة الخارجية، مما يساعد في حماية الأنظمة من التسلل.

التحديثات: يساعد تحديث البرمجيات والأنظمة بانتظام في سد الثغرات الأمنية وتعزيز الأمان.

أنظمة الكشف عن التسلل: تراقب هذه الأنظمة حركة المرور عبر الشبكة وتحاول اكتشاف ومنع التسلل غير المرغوب فيه.

تقنيات التشفير: تساعد في تأمين البيانات عند نقلها عبر الشبكة، مما يحميها من التجسس والاستخدام غير المصرح به.

إدارة الهويات والوصول: تتيح للمستخدمين الوصول إلى الموارد بناءً على صلاحياتهم، وتقلل من مخاطر الوصول غير المصرح به، وتتأكد من أن المستخدمين المتصلين بالأنظمة أو الشبكات هم الأشخاص المصرح لهم.

تقنيات الوقاية من فقدان البيانات: تمنع تسريب البيانات غير المصرح بها.

التحليل السلوكي: يُستخدم من أجل رصد التصرفات غير الطبيعية والاعتداءات السيبرانية باستخدام تحليل سلوك المستخدم والنظام.

الرصد الأمني: يتيح للمؤسسات رصد الأنشطة السيبرانية وتحليل الحوادث للاستجابة السريعة.

الهندسة الأمنية: وهي تصمم الأنظمة والشبكات بطريقة تجعلها أكثر مقاومة للهجمات.

التهديدات السيبرانية في تطور فمن المتوقع أن تستمر التهديدات السيبرانية في التطور والتقدم في السنوات القادمة مع تقدم التكنولوجيا، ويشير خبراء الأمن إلى إمكانية ظهور تحديات وتهديدات جديدة في المستقبل، ومن هذه التهديدات المحتملة:

الذكاء الاصطناعي:

يعد الذكاء الاصطناعي تقنية سريعة التطور ويمكن استخدامها لإنشاء هجمات سيبرانية أكثر تعقيدا وقوة، مما يجعل من الصعب اكتشافها والتصدي لها، حيث يمكن استخدام الذكاء الاصطناعي لإنشاء برامج ضارة أكثر ذكاء يمكنها التهرب من تقنيات الأمان التقليدية، كما يمكن أيضا استخدام الذكاء الاصطناعي لإنشاء هجمات تستهدف البنية التحتية الحيوية، مثل شبكات الطاقة أو نظم النقل.

إنترنت الأشياء:(IoT)

وتُستخدم أجهزة إنترنت الأشياء من أجل إنشاء هجمات حجب الخدمة الموزعة (DDoS) أو سرقة البيانات أو حتى السيطرة على الأجهزة، وقد يزداد التركيز على استهدافها للوصول إلى بيانات المستخدمين أو التحكم في الأنظمة المتصلة.

الهجمات الهجينة:

وتَستخدم الهجمات الهجينة مزيجا من الأساليب التقليدية وغير التقليدية، وتتميز بأنها أكثر تعقيدا وصعوبة في الاكتشاف والحماية منها مقارنة بالهجمات التقليدية.

هجمات الحواسيب الكمومية:

قد تظهر هجمات تعتمد على الحوسبة الكمومية من أجل كسر أنظمة التشفير الحالية، حيث تتميز الحواسيب الكمومية بقدرتها على إجراء العمليات الحسابية بشكل أسرع بكثير من الحواسيب التقليدية، وهذا يجعلها قادرة على كسر أنظمة التشفير الحالية.

الهجمات على الذكاء الاصطناعي:

قد تُستهدف نظم الذكاء الاصطناعي بشكل مباشر لتشويه البيانات أو النتائج، وقد تتسبب هذه الهجمات بتعطيل الأنظمة أو سرقة البيانات أو حتى تعديل البيانات أو إتلافها.

التهديدات السيبرانية للصحة الرقمية:

قد تستهدف أجهزة الرعاية الصحية أو نظم السجلات الطبية، وذلك لأنها حساسة للغاية ويمكن استخدامها لأغراض ضارة، مثل الابتزاز أو التجسس أو حتى إلحاق الضرر الجسدي.

هجمات التحكم في الطائرات المسيرة:

أصبح استهداف الطائرات المسيرة أو أنظمة التحكم فيها محط اهتمام متزايد، وقد تتسبب هذه الهجمات بأضرار جسيمة، بما في ذلك تعطيل الطائرات أو سرقة البيانات أو حتى إسقاطها. (عنتر، 2024)

فهذا كله يمثل علاقة التطور التكنولوجي بالأمن المعلوماتي في مختلف الميادين و المجالات التي يمكن أن تخدمها هذه التطورات التكنولوجية في حماية الخصوصية المعلوماتية باختلاف أشكالها و البرامج المعدّة لذلك من أنظمة و شبكات و تطبيقات ذات خوارزميات و قواعد متينة مهيئة باختلاف أغراضها و أهدافها.

المبحث الثالث : كيفية توظيف التطور التكنولوجي في حماية الخصوصية المعلوماتية

كما ذكرنا في السابق فالمقصود من الخصوصية المعلوماتية؛ هيا المعلومات الشخصية للافراد أو بياناتهم الخاصة وحقهم في حمايتها، فيمكننا القول بأن موضوع البيانات الشخصية هو نفسه محل الخصوصية المعلوماتية، ويعد من البيانات الشخصية كل معلومة كيفما كان شكلها متى تعلقت بشخص طبيعي معرف أو يقبل التعريف بغض النظر عن دعامتها، فتشمل كل المعطيات الفردية والمدنية والصحية والمالية للأفراد، ويمكن وصف بعضها بالمعطيات الحساسة كالمعطيات التي تظهر وتتعلق بشكل مباشر أو غير مباشر بالأصل العرقي أو الآراء السياسية، المعتقدات الدينية، الانتماء النقابي، وكذا المعطيات المتعلقة بالحياة الجنسية أو بالصحة، إضافة لهذا البيانات المتعلقة بالأحكام الجزائية، والتي تستوجب مستوى أعلى من الحماية.

وتجدر الاشارة إلى أن البيانات الشخصية هيا كل معلومة تتعلق بالشخص وتظهر هويته لكن لا يمكن حصر كل البيانات أو المعطيات التي تعتبر شخصية، فنذكر منها؛

البيانات الفردية نجد منها اسم الشخص وجنسيته، وجنسه وصورته ، وديانته وفصيلة دمه، والسكن والوظيفة والمؤهل الدراسي أو المهني ورقم الهاتف والعنوان، والبصمة الخاصة به، كما توجد بيانات اخرى ... إلخ.

ثمّ البيانات المدنية: وهي من أهم المعلومات الخاصة التي يسعى الإنسان إلى حمايتها وابقائها سرية، كبيانات واقعة الميلاد، التي تحدد تاريخ ومكان ميلاه وجنسه واسم الأب والأم، وأيضا بيانات واقعة الوفاة التي تظهر تاريخ وعمر ومكان وفاته

وسببها، إلى جانب عدة بيانات أخرى منها بيانات الزواج والطلاق، والعنوان و رقم بطاقة التعريف وجواز السفر، وتاريخ دخول ومغادرة البلاد وكذا التأشيرات المتحصل عليها ... الخ .

بعدها البيانات المالية وتتضمن معلومات حول الدخل الشهري للفرد، ومعدل انفاقه وديونه، وأرقام الحسابات والمعاملات المالية الخاصة به ... الخ.

البيانات الصحية: وهي التي تتعلق بالحالة الصحية للفرد، والأدوية الموصوفة له وما سبق من حالاته المرضية، والأمراض المزمنة أو الوبائية وحالة الإدمان أو الأمراض المتنقلة ... الخ . إلى جانب ما تم ذكره مازال نطاق البيانات الشخصية واسعا؛ فنجد مثلا عنوان البريد الالكتروني، والبصمة الوراثية، والرقم الوطني الذي نجده في بطاقة التعريف، ورقم تسجيل المركبة أو السيارة الذي يتواجد في البطاقة الرمادية، ورقم التأمين الصحي، فالبيانات الشخصية متعددة ،وقد كان التطور التكنولوجي سببا زيادتها، وهذا بسبب رقمنة المعلومات وشبكة التواصل التي انشات وجودا افتراضيا للشخص الى جانب وجوده الحقيقي، وقد تفضي إساءة الاستخدام إلى خلق مصادر تهديد للحياة الخاصة رغم اجابيات هذا التطور.

حيث تتمثل صور الاعتداء على الخصوصية المعلوماتية

كما ذكرنا سابقا فالخصوصية المعلوماتية تعد بيانات شخصية أو بالاحرى حماية لها، فيعد الاعتداء عليها إعتداءا على الحياة الخاصة للفرد، ويعتبر من أخطر الاعتداءات كونها تمس بخصوصية الفرد وما يتعلق بكل بياناته، لذلك سنوضح من خلال هذا المطلب أخطر صور هذا الاعتداء، فإرتأينا تقسيمه إلى أربعة فروع، نتناول الاختراق، أما في تجميع البيانات الشخصية، إنتحال هوية المستخدم، وأخيرا الافشاء غير المشروع للبيانات الشخصية

الفرع الأول: الاختراق

الخصوصية المعلوماتية في ظل التطور التكنولوجي وآليات حمايتها في البداية نتعرض لتعريف الاختراق الذي يعد بشكل عام: القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف؛ أي قدرة المخترق على الدخول إلى جهاز شخص ما بغض النظر عن الأضرار التي قد يحدثها فنجد أن الاختراق يشكل التحدي الأكبر الذي يواجه كل الأفراد أو الشركات وكذا أصاحب المواقع الالكترونية. فهو يهدد الجميع كونه يملك القدرة على رصد التحركات الشخصية للافراد وهذا باختراق الأجهزة الالكترونية الخاصة بهم مما يجعلى جميع البيانات الشخصية حتى الدقيقة منها بيد المخترق.

الفرع الثاني: تجميع البيانات الشخصية

يجب أن يتم تجميع البيانات الشخصية لغرض مشروع وهذا بعد اخذ إذن أصحابها، فيعد تجميع هاته البيانات دون رضا المستخدم من صور الاعتداء على خصوصيته وهو فعل غير مشروع، وهذا ما أكدته محكمة النقض الفرنسية التي اعتبرت تجميع عناوين البريد الالكتروني دون علم أصحابها تجميعا غير مشروع للبيانات، كذلك نجد اللجنة القومية

للمعلوماتية والحريات قد أكدت على ضرورة رضا صاحب البيانات الشخصية قبل أن تتم عملية تجميعها، وذلك من خلال فرض غرامة 100 ألف يورو على شركة جوجل بسبب قيامها بجمع بيانات المحتوى من هويات و كلمات مرور .

الفرع الثالث: انتحال هوية مستخدم أخر

يمكننا تعريفها بأنها : " الظهور امام الغير بمظهر الذي انتحلت شخصيته بحيث الناظر إليه والمتعامل معه يعتقد دون شك انه يتعامل مع من انتحلت شخصيته.

و يقصد بانتحال الهوية سرقة البيانات الشخصية للغير والتعامل بها وقد انتشرت هاته الصورة من الجرائم خاصة فيما يتعلق بالتجارة الالكترونية وتتمثل في استخدام هوية شخص آخر للاستفادة منها أو إخفاء هوية المنتحل ليقوم بالاحتيال على الزبائن باسم من قام بانتحال شخصيته، وكذا تسهل من ارتكابه الجرائم أخرى كما أن عملية انتحال الهوية من أخطر صور الاعتداء على البيانات الشخصية كونها قد تفضي إلى انتهاك الجانب المالي والشخصي للافراد.

الفرع الرابع: الإفشاء غير المشروع للبيانات الشخصية

تعد هاته الصورة من الاعتداء على الخصوصية المعلوماتية قديمة نوعا ما، إلا أنها توسعت بتفشي التكنولوجيا في جميع الميادين والمجالات التي تمس بالحياة الخاصة بالافراد خاصة بظهور مواقع ووسائل التواصل الاجتماعي، وكذا الاستعمال الواسع لها، كما انها لا تقل عن ما سبقها من الصور في الجسامة، حيث تعتبر هذه الصورة قريبه جدا من صورة إفشاء الأسرار والتي تعاقب عليها أغلب التشريعات. (أحمد، 2023)

حيث تتمثل وسائل تحقيق عناصر أمن المعلومات من خلال عناصر أمن المعلومات وأهمية توافر جميع هذه العناصر حتى يمكن الحصول على معلومة آمنة. لكن السؤال المطروح هو: كيف يجري تطبيق أو تحقيق كل عنصر من هذه العناصر ؟ والجواب هو أنه يوجد وسائل (أو تقنيات يمكن من خلالها تحقيق هذه العناصر، ويمكن استخدام الوسيلة نفسها لتحقيق أكثر من عنصر في الوقت نفسه ، ويلزم في بعض الأحيان استخدام أكثر من وسيلة معا لتحقيق عنصر واحد من عناصر أمن المعلومات. هناك ثلاث تقنيات رئيسة يمكن استخدامها كوحدات بناء أساسية لتحقيق بعض عناصر أمن المعلومات وهي: التشفير (Encryption) بنوعيه المتناظر وغير المتناظر، والتصديق الرقمي (Digital Signature)، والبصمة الرقمية .(Hash Value) فيمكن استخدام هذه الوسائل كوحدات بناء أساسية لتحقيق بعض عناصر أمن المعلومات وهي: التحقق من الهوية. والتحكم بالوصول، والسرية، وسلامة المعلومة وتكاملها، فيمكن تحقيق عنصر السرية باستخدام التشفير المتناظر أو غير المتناظر أو بهما معا. ويمكن تحقيق عناصر : التحقق من الهوية، والتحكم بالوصول (للمنشآت الصغيرة) ، وعدم الإنكار باستخدام التشفير غير المتناظر والتصديق الرقمي معا. ويمكن تحقيق عنصر سلامة المعلومة وتكاملها باستخدام البصمة الرقمية. كما يمكن استخدام التصديق الرقمي للتحقق من هوية الشخص Entity Authentication) ، ويستخدم مع البصمة الرقمية للتحقق من) Data Origin Authentication(هوية الرسالة أو المعلومة يمكن استخدام تقنيات تسجيل الدخول الواحد، ومصفوفات قوائم التحكم، وأنظمة كشف

ومنع التطفل لتحقيق عنصر التحكم بالوصول (Access Control) للمنشآت الكبيرة والمنشآت التي تحتاج إلى أنظمة تحكم بالوصول قوية متخصصة في ذلك.

أما عنصرا التوفر والتدقيق فيحتاجان إلى وسائل وتقنيات أخرى، حيث يمكن تحقيق عنصر التوفر (Availability) باستخدام تقنيات الأجهزة والبرامج الرديفة وأنظمة الحماية ضد الهجمات التي تعطل الخدمة-Denial of Service) (DoSويمكن تحقيق عنصر التدقيق باستخدام تقنيات متابعة وتسجيل الأحداث، سواء تلك التي ترد رفق أنظمة التشغيل أو التي يتم بنائها من قبل شركات متخصصة في ذلك. (أمن المعلومات، 2015)

و هذا كله تمثل أساليب و تقنيات الحديثة للتطور التكنولوجي من آليات و غيرها التي يتم توظيفها و استغلالها في حماية الخصوصيات المعلوماتية في شتى القطاعات و المجالات المتخصصة.

خاتمة :

فللوصول للحماية الاليكترونية الشاملة للخصوصية المعلوماتية في ظل التطور التكنولوجي المعاصر و باستخدام التكنولوجيات الحديثة المختلفة و المتنوعة ذات التقنيات وصولا لعناصر أمن المعلومات ، فيجب الوصول للقواعد الأساسية لأشكال التطور التكنولوجي المختلفة التي تتلائم مع مختلف المجالات الاجتماعية مرورا بربط علاقتها بتقنيات التطور التكنولوجي المعاصر وصولا لكيفية توظيف هذه التقنيات و الأساليب في حماية الخصوصية المعلوماتية لتحقيق عناصر أمن المعلومات المختلفة.

النتائج و التوصيات:

_ تتعدد أشكال التطور التكنولوجي المعاصر بما يخدم مختلف القطاعات في المجتمع من تقنيات و آليات و عناصر تشكل و تحمي نظم معلوماتية ذات أساس متين يمثل مركز للمنشآت و الأفراد.

_ ترتبط حماية الخصوصية المعلوماتية بالتطور التكنولوجي عن طريق تحقيق التوازن بين أشكال التطور التكنولوجي و خطورة إختراقات الخصوصية المعلوماتية.

_لتوظف أفضل للعلاقة بين التطور التكنولوجي و حماية الخصوصية المعلوماتية يجب دعم التطور التكنولوجي بكافة تقنياته المختلفة بأنظمة مجهزة بقوالب متخصصة بمختلف القطاعات بما يحقق عناصر أمن المعلومات المطلوبة,

قائمة المصادر و المراجع :

- **باللغة العربية :**

ذ .ب .القحطاني (2015). Dans *أمن المعلومات* .(p. 107_108)الرياض :مدينة الملك عبد العزيز للعلوم و التقنية.

مخبر الممارسات اللغوية في الجزائر. (2015). ملتقى الوطني: الأمن المعلوماتي مهدداته و سبل الحماية. تيزي وزو: منشورات مختبرالممارسات اللغوية في الجزائر.

غريب ,ح .(2017) .محاطر مواقع التواصل الاجتماعي على الأمن المجتمعي :الرهانات و الاستراتيجيات .*الندوة الدولية (عولمة الاعلام السياسي و تحديات الأمن القومي للدول النامية* .(16_ 15 .p) (الجزائر :المدرسة الوطنية للعلوم سياسية الجزائر.

أحمد ,ن .(2023) .الخصوصية المعلوماتية في ظل التطور التكنولوجي و آليات حمايتها .*التحديات القانونية و التطور التكنولوجي* p. 8) إلى .(10قسنطينة :جامعة قسنطينة 1.

عنتر ,أ .(2024, 08 22) .*الجزيرة*. Récupéré sur موقع الجزيرة .https://www-aljazeera-net.cdn/ :