حماية البيانات الشخصية و الأمن السبراني

تحليل من منظور القانون الدولي

رفرافي عبد الرحمان ، جامعة الوادي

refrafi-abderrahmane@univ-eloued.dz

تاريخ الاستلام: 2025/04/06 تاريخ القبول: 2025/06/10 تاريخ النشر: 2025/06/19

ملخص

عندما يتعلق الأمر بتطبيق القانون الدولي في مجال الفضاء السيبراني، ومن أجل مواجهة هذه الهجمات السيبرانية، هناك خياران .يمكن اللجوء إلى القواعد القائمة في القانون الدولي، من خلال التكييف المناسب .أو البدء في صياغة معاهدات جديدة .كان الخيار الأول هو ذلك الذي تدعمه الولايات المتحدة وحلفاؤها الغربيون، فاستراتيجيات الأمن السيبراني لهذه البلدان واضحة للغاية في هذا الصدد، ومن جانبها، تمكنت الجمعية العامة للأمم المتحدة، في إطار اللجنة الأولى، من التوصل إلى الحد الأدنى من توافق الآراء، من خلال "فريق الخبراء الحكوميين المعني بالتقدم في مجال المعلومات والاتصالات في سياق العلاقات الدولية".

تهدف المقالة لتقديم الخلفية العامة للقارئ حول الحق في حماية البيانات الشخصية؛ تحليل القيمة الاقتصادية والاجتماعية لمعلومات العملاء والمستخدمين التي تحتفظ بها الشركات؛ تحديد الإطار القانوني المطبق في المسألة المذكورة؛ وضع تصور للحق في حماية البيانات الشخصية وتحديد مبادئ تفسيره؛ وأخيرا، تحليل التحديات التي يواجهها القطاع في معالجة البيانات الشخصية، فضلا عن اقتراح آليات الامتثال للوائح المتعلقة بهذا الشأن.

مقدمة

تعتبر الهجمات السيبرانية مشكلة متنامية ومستمرة .على سبيل المثال، كان فيروس برامج الفدية ، والذي وضع نصف العالم تحت المراقبة في عام 2017، لا يزال أحد أكثر الفيروسات عدوانية. ويمكن أن يكون للهجمات الإلكترونية أصل عام أو خاص ففي الحالة الأولى تدخل في نطاق استخدام القوة، الذي ينظمه القانون الدولي في إطار ميثاق الأمم المتحدة، الذي خصص فصله السابع للأمن الجماعي .وفي حالة

الهجمات السيبرانية ذات المنشأ الخاص، فمن الضروري اللجوء إلى مختلف آليات التعاون القانوني الدولي، والتي سيتم ذكر بعضها أدناه.

تم إعداد المقالة بناءً على المنهج التحليلي، من أجل تحليل الإطار القانوني الذي يمكن تطبيقه على حماية البيانات الشخصية للعملاء ومستخدمي شركات الخدمات .وهذا يسمح لنا بقياس القيمة الاقتصادية والاجتماعية لهذا النوع من المعلومات، وتصور الآثار المترتبة على هذا الحق ومبادئ تفسيره، وتحديد التحديات الرئيسية والمقترحات للامتثال للتشريعات المتعلقة بهذا الشأن.

إشكالية الدراسة: نظراً لهذه الموجة من الهجمات، من المفيد أيضاً أن نتساءل: إلى أي مدى تأثرت المنظمات الخاصة؟ ما هو مستوى تأثير هجمات *برامج الفدية* بين الشركات؟ .وتسلط هذا الدراسة الضوء فقط على الحاجة الملحة إلى وجود تنظيم عام مناسب فيما يتعلق بالأمن السيبراني.

المبحث الأول: تأطير القانون الدولي للفضاء السبراني

في تقرير فريق الخبراء العالمي (ONU, 2013) 2013 ، تم التوصل إلى اتفاق بشأن إمكانية تطبيق القانون الدولي الحالي على الفضاء الإلكتروني، وتحديدًا ميثاق الأمم المتحدة وحقوق الإنسان، فضلاً عن القواعد الأساسية المتعلقة بالمسؤولية الدولية ، وبالمثل أصر تقرير فريق الخبراء العالمي (ONU, الدورة 70, 2015) على إمكانية تطبيق بعض مبادئ القانون الدولي الإنساني (مثل التناسب أو التمييز) في الفضاء الإلكتروني، فضلا عن الالتزام بالعناية الواجبة .وقد دعمت بعض المبادرات الخاصة المهمة هذا الخيار (OTAN, 2013-2017) .

أما الخيار الثاني، والذي يتمثل في وضع معاهدات دولية جديدة، فقد أيدته روسيا والصين ودول أخرى، والتي قدمت مقترحات مثل مدونة قواعد السلوك لأمن المعلومات لعام 2011. وقد تم تسليط الضوء على التناقض بين هذين الخيارين (في تقرير GEG لعام 2017 ، والذي تم اعتباره فاشلاً)..

والواقع أن قضايا مثل اللجوء إلى الدفاع عن النفس، أو التدابير المضادة، أو الاعتراف الصريح بقواعد معينة في القانون الإنساني الدولي، لقيت رفضاً من قِبَل دول مثل روسيا أو الصين أو كوبا، على أساس أن

الدول الغربية تسعى إلى عسكرة الفضاء الإلكتروني (ولكن مفهوم الجريمة الإلكترونية لم يتم تعريفه قانونيا، على الرغم من أن أكثر من 470 جريمة مرتبطة بأنظمة المعلومات). تأتي البادئة "سايبر" من الكلمة اليونانية kubernêsisوالتي تعني "الحكم أو فعل التوجيه."

قد يدفع هذا الفشل إلى الاعتقاد بأن الطريق المتعدد الأطراف مغلق، وأن الدول ستلجأ إلى الطريق الأحادي أو الإقليمي (ONU, 2021) في نهاية عام 2018، تم إنشاء فريقي عمل في إطار الجمعية العامة للأمم المتحدة .فمن ناحية، تم إطلاق مجموعة GEG جديدة برعاية الولايات المتحدة (مع 25 ممثلاً للحكومة).(otan, 2022)

ومن ناحية أخرى، تم إنشاء مجموعة عمل مفتوحة تروج لها روسيا، وهي لا تتعارض مع المجموعة السابقة ومن المفترض أنها أكثر شمولاً (ويمكن أن تشمل جميع أعضاء الأمم المتحدة) .وتظهر هذه النتيجة موقفا جديدا أكثر تأييدا للمعايير بين الدول الأعضاء في الأمم المتحدة، على الرغم من أن ذلك قد يكون على حساب المزيد من البطء والتعقيد في العملية .قد يكون هذا النشاط المؤيد للمعايير أيضًا نوعًا من رد فعل الحكومة على المبادرات الخاصة المختلفة التي تجري مؤخرًا بالإضافة إلى ما يسمى بعملية لاهاي، والتي تم إدراج دليل تالين الثاني لعام 2017 فيها، فإن اتفاقية جنيف الرقمية ، التي روجت لها مايكروسوفت منذ عام 2017، تحتل مكانة بارزة .

إذا كان هذا هو ما يحدث على مستوى اللوائح العامة فيما يتعلق بالفضاء السيبراني ،كشفت بعض الدراسات أن أكثر من مليار وثلاثة وعشرين مليون بيانات تمت سرقتها خلال عام 2014. ، فقد حدث تطور فريد في النطاق الأكثر محدودية للجرائم السيبرانية، يشجعه أيضًا انتشار الهجمات السيبرانية ذات المنشأ الخاص. والتي تسبب تكلفة متزايدة بقيمة 600 مليار دولار سنويا، وفقا لتقرير عام 2018.

في مجال الجرائم السيبرانية، تم اعتماد **اتفاقية بودابست** في عام 2001 في إطار مجلس أوروبا وهي اتفاقية تجسد في وقت مبكر التعاون الدولي الناجح، توفر هذه الاتفاقية الحد الأدنى من التنسيق في المسائل القضائية، وعلى وجه التحديد، فيما يتعلق بالوصول إلى الأدلة الرقمية، ومع ذلك، كما هو الحال في حالات أخرى من التعاون القانوني الدولي فإن هذه الاتفاقية يعوقها البطء الكبير في تقديم المساعدة بين الدول الأطراف

(تستغرق الطلبات أشهرا للرد عليها، (الأمر الذي يدفع العديد من الدول الأطراف إلى اللجوء بدلا من ذلك إلى الصكوك الثنائية) ، تلك المعروفة مثل MLAsكما تم انتقاد أن هذه الاتفاقية تسمح للدول بالتحايل على الضمانات الوطنية لصالح حقوق الإنسان..

ونتيجة للفعالية المحدودة للتعاون القانوني الدولي الذي انطلق مع اتفاقية بودابست، بدأت الدول تلجأ إلى آليات انفرادية لمواجهة ظاهرة الجرائم السيبرانية العابرة للحدود الوطنية (2015, GEG) .إحدى تلك الطرق الأحادية هي القرصنة عبر الحدود .وحتى الآن، لا توجد أمثلة على إدانة هذا النوع من الممارسات من قبل أي دولة .ومع ذلك، فإن اليقين بشأن وجود هذا النوع من القدرات يسمح لنا بتخمين أن استخدامه قد تم بالفعل في مواقف معينة (JORF, 6 janvier 1978)

ومن ناحية أخرى، هناك طريقة أخرى أحادية الجانب للوصول إلى الأدلة الرقمية، تتمثل في الحصول على تعاون مباشر من مقدمي الخدمات في دولة الوجهة . والميزة التي توفرها هذه الإمكانية هي أنها تجعل تدخل أو ترخيص سلطات دولة الوجهة غير ضروري لكي تتمكن الدولة الطالبة من الوصول إلى الأدلة الإلكترونية، هذا الاحتمال هو ما فكر فيه قانون السحابة الأمريكي لعام 2018 وهو أيضًا ما ينص عليه توجيه الأدلة الإلكترونية المقترح، والذي يتضمن أمر الإنتاج الأوروبي .

أراد مجلس أوروبا معالجة النقص الحالي في استخدام اتفاقية بودابست، ولهذا السبب بدأت عملية اعتماد بروتوكول جديد لاتفاقية عام 2001. ويهدف هذا البروتوكول الجديد إلى تبسيط عملية المساعدة القانونية بين الدول الأعضاء. الدول الأطراف، مما أدى إلى تحسين الأرقام التي تم الحصول عليها حتى الآن في هذا الصدد .والنتيجة النهائية التي يهدف البروتوكول إلى تحقيقها ستسمح لدولة المصدر بجعل قواعدها المعمول بها في هذا الشأن هي السائدة نتيجة لممارسة ولايتها القضائية لمقاضاة الجريمة السيبرانية المعنية .ومع ذلك، انتقدت المنظمات غير الحكومية مثلEdriأو EFF هذه المحاولة لوضع بروتوكول جديد، لأنها ترى أن ذلك سيعني بالتأكيد تآكل المعايير المطبقة في دولة المقصد .

ومع الأخذ في الاعتبار أنه لا يوجد تنسيق بين المعايير الجنائية (DURKHEIM, 1983) بين دول مجلس أوروبا فحسب، بل إن الأنظمة القانونية الوطنية شديدة التنوع أيضًا، فإن المجالات التي يمكن أن تتأثر أكثر من غيرها هي تلك المتعلقة بحقوق الإنسان المحمية في الاتفاقية. دولة الوجهة، والتي يجب أن نسلط الضوء من بينها الحق في الخصوصية وحماية البيانات الشخصية، بالإضافة إلى الضمانات الإجرائية المطبقة في دولة الوجهة المذكورة.

وعلى مستوى الأمم المتحدة، تم رفض الاقتراح الروسي بشأن اتفاقية مكافحة الجرائم السيبرانية بالفعل في عام 2010. وفي عام 2011، أنشأت لجنة منع الجريمة والعدالة الجنائية (CPDJP) فريق الخبراء، بناء على طلب الجمعية العامة، لتنفيذ دراسة شاملة عن الجرائم الإلكترونية، بهدف إعداد ردود قانونية أو غير قانونية، وطنية أو دولية، لمواجهة هذه الظاهرة. أنشئت لجنة منع الجريمة والعدالة الجنائية بموجب قرار المجلس الاقتصادي والاجتماعي 1/1992، بناء على طلب قرار الجمعية العامة 152/46، باعتبارها إحدى لجانه الوظيفية.

تم إجراء دراسة شاملة حول الجرائم الإلكترونية بتكليف من مكتب الأمم المتحدة المعني بالمخدرات والجريمة وتم الانتهاء منها في عام 2013. استمر عمل فريق الخبراء حتى عام 2021 ومع ذلك، هناك خلاف داخل إطار الأمم المتحدة حول كيفية مواجهة آفة الجرائم الإلكترونية (ROBERT، février 2014) . فمن ناحية، تدرك الولايات المتحدة وحلفاؤها أن اتفاقية بودابست تشكل نصاً كافياً لمكافحة الجرائم السيبرانية .علاوة على ذلك، فإن عمل فريق الخبراء على وشك الانتهاء، لذا من الأفضل في الوقت الحالي الانتظار لتقييم نتائج ذلك العمل.

من ناحية أخرى، أعلنت روسيا ودول أخرى أنها تفضل صياغة نص عالمي جديد يجسد توافقاً عالمياً في الآراء، وبالتالي، توافقاً في الآراء لا يقتصر على الدول الأطراف في مجلس أوروبا .علاوة على ذلك، يرى أن بعض آليات اتفاقية بودابست، مثل المادة 32 (ب)، تمثل اعتداء على سيادة الدولة الإقليمية، لأنها تنطوي على إمكانية التهرب من الحصول على إذن مسبق من الدولة المذكورة عند الحصول على الأدلة الإلكترونية.

تفاجأت بعض الدول الغربية بموافقة الجمعية العامة للأمم المتحدة مؤخرًا على اقتراح بشأن اتفاقية بشأن الجرائم الإلكترونية في نهاية عام 2019. وفي الواقع، كشفت الأغلبية التي تم التوصل إليها لاعتماد هذا القرار عن تصويت مثير للانقسام79-60-30 .ولكن هذه المرة لصالح المبادرة التنظيمية (وتستند الاتفاقية المقترحة إلى مسودة قدمتها روسيا في عام 2017. وتضمنت هذه المسودة قائمة بالجرائم الإلكترونية التي تخضع للمحاكمة (بما في ذلك القرصنة)، والخيارات المختلفة للتعاون القانوني بين الدول، فضلاً عن إنشاء مركز اتصال للتحقيقات .من أجل المضي قدمًا في الاقتراح الذي وافقت عليه الأمم المتحدة في عام 2019، تم دمج إنشاء لجنة خبراء مفتوحة *مخصصة)*.

تعرض اقتراح الأمم المتحدة هذا لانتقادات من قبل المنظمات غير الحكومية .ويزعم هؤلاء أن هذا الاقتراح، مع الأخذ في الاعتبار أن روسيا هي التي تروج له، لا يمكن أن يؤدي إلا إلى تجريم أكبر للسلوك على الإنترنت، بما يتماشى مع سيطرة الدولة الأكبر التي تروج لها دول مثل روسيا أو الصين على الإنترنت. ورأى أن هذا الاقتراح يسعى إلى تجاوز الأحكام الواردة في اتفاقية بودابست، بحيث يتم تقليل إمكانية رفض طلبات المساعدة من قبل دولة المقصد .

ويُعَد الاقتراح الخاص باتفاقية جديدة للأمم المتحدة بشأن الجرائم السيبرانية مثالاً على الموقف الجديد الأكثر تأييداً للمعايير والذي يبدو أنه يتعزز اليوم ، تراكم لدى اتفاقية بودابست خبرة تمتد إلى عقدين من الزمن ولاقت قبولاً كبيراً بين الدول (هناك 65 دولة طرفاً والعديد منها أدرجتها في تشريعاتها الوطنية) ، وعلى وجه الخصوص، فقد كان موضوع إعلان الدعم من جانب الاتحاد الأوروبي الذي يرفض، إلى جانب الولايات المتحدة، اقتراح الأمم المتحدة .ومن ناحية أخرى، ترى روسيا والصين والعديد من الدول النامية أن اتفاقية بودابست تمثل نادياً محدوداً من الدول، بعيداً عن الإجماع العالمي الذي يمكن التوصل إليه في الأمم المتحدة صادف عام 2024 الذكرى الثلاثين لتوقيع مذكرة بودابست، وهي جزء من اتفاق تخلت بموجبه أوكرانيا عن ترسانتها النووية مقابل ضمانات أمنية من روسيا والولايات المتحدة والمملكة المتحدة. شكّلت المذكرة ، الموقعة في 5 ديسمبر/كانون الأول 1994، حدثًا بارزًا في العلاقات الدولية. ولا تقتصر

أهميتها على سياق تفكك الاتحاد السوفيتي وبداية حقبة ما بعد الحرب الباردة فحسب، بل تُمثّل أيضًا لحظةً محوريةً في حركة الحد من الأسلحة النووية، ومثالًا هامًا على حلّ النزاعات الدولية، لا سيما في سياق العلاقات بين الدول القوية. وفي الواقع، فإن هذا الخيار لاتفاقية جديدة يكتسب وزناً بين الدول الأعضاء في هذه المنظمة، إما لأن ميزان السياسة الخارجية قد تغير (هناك دول أطراف في اتفاقية بودابست، وحتى مجلس أوروبا، صوتت لصالح الاقتراح)، إما لأن هناك جاذبية متزايدة حول معاهدة عالمية جديدة بشأن هذه المسألة وما قد يترتب على ذلك من تعزيز لسيادة الدولة.

من الناحية القانونية، لا ينبغي تجاهل العواقب الناجمة عن اعتماد اتفاقية جديدة بشأن الجرائم السيبرانية (AGNU, 2024) . والتي تطمح إلى التعميم، مثل اتفاقية بودابست .وإذا كانت هناك اتفاقيتان حول نفس الموضوع، فسيكون من الضروري اللجوء إلى المادة 30 من اتفاقية فيينا لقانون المعاهدات .وبغض النظر عن الحل الذي سيتم اعتماده في كل حالة، واللجوء إلى نوع من الثنائية، فالحقيقة هي أن وجود إطارين قانونيين عامين بشأن نفس المسألة لن يساعد في تبسيط المساعدة القانونية بين الدول.

هناك غياب للتوافق التنظيمي الذي يواجه الولايات المتحدة والدول الغربية من جهة، وروسيا والصين والعديد من الدول النامية من جهة أخرى .ويدعو الأولون إلى تطبيق قياسي للمعايير الحالية على الفضاء الإلكتروني، في حين يفضل الثاني تطوير معايير جديدة .وأسباب هذا الافتقار إلى الإجماع سياسية (الإنترنت المفتوح وحماية حقوق الإنسان في مقابل الإنترنت المغلقة وزيادة سيطرة الدولة وإستراتيجية الدفاع عن الميزة التكنولوجية الحالية ضد تمزق الوضع الراهن.

ويشكل عدم التوافق هذا خطراً على استقرار العلاقات الدولية، فضلاً عن القدرة على وقف الهجمات السيبرانية، فضلاً عما ينطوي عليه من التخلي عن الوظائف، وهو ما يفسر انتشار المبادرات التنظيمية الخاصة .علاوة على ذلك، في مجال الجرائم الإلكترونية الأكثر تحديدًا، تحدث مفارقة معينة .إن التصورات حول الدفاع عن سيادة الدولة بأي ثمن، لسبب أو لآخر، تمنع التقدم على مستوى الأنظمة .ومع ذلك،

فإن التعاون الأكبر في هذا المجال من شأنه أن يؤدي إلى حماية أكثر فعالية لمصالح الدولة، لأنه في الوضع الحالي لا تزال الأهواء الأحادية متكررة.

المطلب الأول: الأمن السيبراني شرطًا أساسيًا لتعزيز التحول الرقمي

تعرضت إستونيا في عام 2007، وهي جمهورية سوفييتية سابقة تقع على شواطئ بحر البلطيق، لهجوم كمبيوتر يشكل حتى يومنا هذا دراسة حالة نموذجية من حيث سياسات الأمن السيبراني العام، في 27 أبريل 2007، وقع أول هجوم إلكتروني يستهدف هيكل الدولة في إستونيا. ونسبت السلطات الإستونية هذا الهجوم واسع النطاق ضد البنية التحتية لدولة ثالثة إلى روسيا منذ الأيام الأولى. قررت السلطات الإستونية، التي ترغب في الاحتفال باستقلالها عن شقيقها الأكبر السوفييتي، نقل النصب التذكاري للجيش الأحمر من وسط العاصمة تالين إلى الضواحي. ويمثل هذا القرار دليلا على تقارب إستونيا مع القوى الغربية.

يبدو أن الجواب لم يتأخر طويلاً: فقد استأجرت روسيا مؤقتًا خدمات أصحاب شبكات الروبوتات، وهي شبكات من أجهزة الكمبيوتر الزومبي، لزيادة عدد أجهزة الكمبيوتر المتورطة في هجوم رفض الخدمة الذي تم إطلاقه ضد إستونيا(Thomson, 2007) .في سياق "أزمة الجندي البرونزي" التي واجهتها تلك الدولة مع روسيا، كانت مختلف الوكالات الحكومية والبرلمان والشرطة والصناعة المالية ومقدمي خدمات الإنترنت ووسائل الإعلام هدفًا لهجوم سيبراني على نطاق واسع غير مسبوق، **التي** تمكنت من شل إستونيا لأسابيع .لقد كان نوعًا من *التعتيم* الرقمي.

ما هي الطريقة المستخدمة؟ لقد طغت شبكات الروبوت على أنظمة الكمبيوتر المختلفة في البلاد وعطلتها) بما في ذلك خوادم الويب وخوادم البريد الإلكتروني وخوادم DNS وأجهزة التوجيه (بموجات هائلة من الطلبات الآلية، مما جعلها غير قابلة للوصول ونتيجة لهذا الحادث، لم تدرك إستونيا وحدها ومع ذلك، تواجه الدولة الروسية اتهامات متزايدة بالتدخل. خلال صيف عام 2008، "أظهر الصراع بين روسيا وجورجيا أن الهجمات الإلكترونية لديها القدرة على أن تصبح عنصرا رئيسيا في الحرب التقليدية"، وفقا لحلف شمال الأطلسي ، بل أيضاً العديد من البلدان (بالضرورة)، حجم المشكلة ومستوى الضعف الذي

تعرضت له .لقد أدركوا أن بعض الأنشطة التي تستخدم شبكات الكمبيوتر أو البيئات الافتراضية لها أهمية حيوية للأداء الوطني الطبيعي.

على سبيل المثال، تلك التي تسمح بتقديم الخدمات الأساسية للسكان – وأن الأمن السيبراني يشكل شرطا أساسيا لتعزيز التحول الرقمي، كذلك بما يضمن الحرية الفردية ورفاهية المجتمع .وفي حالة إستونيا على وجه الخصوص، أدى الحادث إلى ثورة في نهجها تجاه تكنولوجيات المعلومات، حيث اعتمدت نهجا شاملا للأمن السيبراني (وهي مسألة تعتبر اليوم مرجعا عالميا، مع الأخذ في الاعتبار مؤشر الأمن السيبراني العالمي)، والذي بدوره وقد دعمت الرقمنة القوية لقطاعاتها الإنتاجية وخدماتها العامة (تظهر إستونيا أعلى الدرجات في الخدمات العامة الرقمية في مؤشر الاقتصاد والمجتمع الرقمي ، الذي يلخص المؤشرات المتعلقة بالأداء الرقمي في أوروبا. .

المطلب الثاني: الحرب السيبرانية وتعرض الفضاءات الرقمية للاستغلال.

قد تؤثر نقاط الضعف المعنية على واحد أو أكثر من العناصر الضرورية للتشغيل الآمن للفضاء السيبراني يستخدم أعضاء العصابة وسائل التواصل الاجتماعي على نطاق واسع، وخاصة الفيسبوك وتويتر. إنهم ينشرون الصور ومقاطع الفيديو والأغاني والنصوص التي تخدم أغراضًا مختلفة: الترويج لثقافة فرعية إجرامية، واستراتيجية إرهابية ضد العصابات المعارضة، والتهديدات الموجهة إلى الشرطة، ومحاولات التأثير على السكان المحليين، وما إلى ذلك. هذه البيانات، المتاحة على الإنترنت، لا تفلت من قوات الأمن، التي تستخدم الآن برامج مبتكرة لمكافحة الجريمة ، والتي تشمل، بالإضافة إلى البنية التحتية وأنظمة الكمبيوتر، القدرات التنظيمية والتشغيلية والفنية اللازمة لتشغيله .وبالتالي، يمكن أن تركز الهجمات الإلكترونية على أي من الروابط التي تشكل جزءًا من نظام رقمي معين، سواء على *الأجهزة* أو *البرامج*أو الأشخاص الذين يديرونها أو يستخدمونها .لقد شهدنا في السنوات الأخيرة انتشار الهجمات الحاسوبية التي ترتكبها مجموعات إجرامية محترفة للغاية، باستخدام تقنيات تظهر مستويات متزايدة من التطور (M، 2012) ويمكن ملاحظة هذا الاحتراف في البرامج الضارة المستخدمة وفي المتجهات المطورة لتوزيعها واختراقها وإصابتها، وفي الآليات المستخدمة لكشف واستغلال الثغرات الأمنية الموجودة في أنظمة الضحايا المحتملين.

ما سبق يرتبط بشكل مباشر بالهدف الذي تسعى هذه العصابات من خلال نشاطها إلى الحصول على منفعة اقتصادية .وبالتالي، فإننا نرى زيادة (في مختلف القطاعات، العامة والخاصة) في هجمات الابتزاز، والتي تسمى برامج *الفدية*، في عام 2023 وحده، استهدفت محاولات هجمات برامج الفدية 10٪ من المؤسسات حول العالم. ويمثل هذا ارتفاعًا ملحوظًا مقارنةً بـ 7٪ من المؤسسات التي واجهت تهديدات مماثلة في العام السابق، وهو أعلى معدل مسجل في السنوات الأخيرة والتي تسعى إلى منع الوصول إلى أنظمة ومنصات المنظمة أو التأثير على إمكانية قراءة قواعد بياناتها، ثم طلب فدية مقابل إطلاق سراحه .إنها عمليات اختطاف افتراضية حقيقية .إن المشاكل التشغيلية الواضحة التي يولدها هذا السيناريو، جنباً إلى جنب مع المخاطر التي تهدد السمعة والصورة، غالباً ما تشجع الضحايا على دفع الملايين من المبالغ، مما يمنع الحادث من أن يصبح علنياً .وفي شيلي، تسببت الهجمات السيبرانية التي تعرضت لها كيانات وطنية مختلفة مؤخرا في إثارة القلق والانزعاج.

من ناحية، شهدت السلطات أو الخدمات العامة الرقمية للغاية (السلطة القضائية وخدمة المستهلك الوطنية ولجنة الاعتماد الوطنية)، والتي تعتمد إلى حد كبير على القنوات *عبر الإنترنت* أو أنظمة الكمبيوتر لأداء وظائفها، استغلال بعض الثغرات الأمنية الموجودة في نظامها الرقمي والنظم البيئية، مما يؤدي إلى مقاطعة عملها بشكل خطير أو التأثير على سلامة قواعد بياناتها .ومن ناحية أخرى، تأثر عنصر أساسي في الدفاع الوطني ونظام الاستخبارات، مثل هيئة الأركان المشتركة، بالوصول غير المصرح به إلى عدد كبير من الرسائل الواردة في رسائل البريد الإلكتروني، في 2022/09/22، مما يثير الشكوك حول مدى خطورة المعلومات موضوع التسريب وتأثيرها المحتمل على أمن البلاد (طُوِّرت تقنية برامج الفدية لأول مرة على يد عالم الأحياء التطوري جوزيف ل. بوب، الذي تلقى تعليمه في جامعة هارفارد. أطلق بوب فيروس الإيدز بتوزيع أقراص مرنة مُصابة ببرامج الفدية على المشاركين في مؤتمر دولي حول الإيدز عقدته منظمة الصحة العالمية في ستوكهولم، السويد. أخفى الفيروس مجلدات الملفات على أجهزة الكمبيوتر الخاصة بهم، وطالب بإرسال 189 دولارًا أمريكيًا إلى بنما لتحرير أجهزة الكمبيوتر الخاصة بهم) .

نظراً لهذه الموجة من الهجمات، من المفيد أيضاً أن نتساءل: إلى أي مدى تأثرت المنظمات الخاصة؟ ما هو مستوى تأثير هجمات *برامج الفدية* بين الشركات؟ نحن لا نعرف على وجه اليقين .ويسلط هذا السيناريو الضوء فقط على الحاجة الملحة إلى وجود تنظيم عام مناسب فيما يتعلق بالأمن السيبراني.

من الضروري تعزيز معالجة القانون الإطار بشأن الأمن السيبراني والبنية التحتية للمعلومات الحيوية، وهو الإجراء الدستوري الأول .ويسعى هذا المشروع، الذي يتبع أفضل المعايير الدولية في هذا الموضوع، إلى ضمان أن يكون نموذج مناسب لإدارة الأمن السيبراني، مع تسليط الضوء على إنشاء إطار مؤسسي في هذا الشأن، كما سعت بعض الدول الى انشاء وكالة وطنية للأمن السيبراني والتي تلعب دورًا رائدًا .والتي ستنظم من بين جوانب أخرى: إدارة حوادث الأمن السيبراني؛ والالتزامات التي تخضع لها بعض الجهات الفاعلة الرئيسية (كل من الهيئات الحكومية وبعض الكيانات الخاصة التي تعتبر بالغة الأهمية)، والتي تشمل واجبات الإبلاغ عن الحوادث واعتماد تدابير أمنية وقائية؛ توليد اللوائح الفنية؛ إنشاء فرق الاستجابة لحوادث أمن الكمبيوتر؛ وإدراج نظام فعال للانتهاكات والعقوبات.

تتزايد ارتباط تقنيات الطاقة التقليدية بالتقنيات والشبكات الرقمية الحديثة. ويزيد تزايد الرقمنة في نظام الطاقة من ذكائه، ويُمكّن المستهلكين من الاستفادة بشكل أفضل من خدمات الطاقة المبتكرة، إلا أنه يُشكّل أيضًا مخاطر كبيرة، إذ إن تزايد التعرض للهجمات الإلكترونية وحوادث الأمن السيبراني قد يُعرّض أمن إمدادات الطاقة وخصوصية بيانات المستهلكين للخطر.

تهدف استراتيجية الاتحاد الأوروبي الأمنية الشاملة(COM/2020/605) ، التي عُرضت في يوليو 2020، إلى ضمان الأمن الأوروبي في العالمين المادي والرقمي في جميع قطاعات المجتمع. وإذ تُقرّ الاستراتيجية بالحاجة إلى مبادرات خاصة بكل قطاع، لا سيما في قطاع الطاقة، فإنها تُحدّد مبادرةً مُرتقبةً لجعل البنية التحتية الحيوية للطاقة أكثر مرونةً في مواجهة التهديدات المادية والسيبرانية والهجينة. وسيضمن ذلك تكافؤ الفرص لمشغّلي الطاقة عبر الحدود.

كل هذه العناصر حاسمة للامتثال السليم للإطار المقترح .على الرغم من وجود مجال للتحسين، إلا أن المشروع يشير إلى الاتجاه الصحيح، بمعنى أن يتم تصوره كأحد الركائز التنظيمية التي يمكن لبلدنا من خلالها إنشاء بيئة رقمية آمنة ومسؤولة، والتي تعمل بدورها كأساس لتحقيق بيئة رقمية موثوقة. والتحول الرقمي

الناجح .تسلط حوادث الأمن السيبراني الأخيرة التي أثرت على البلاد الضوء على الحاجة إلى التصرف بإلحاح .دعونا نأمل أن تشكل هذه الأحداث نقطة تحول بالنسبة لنا، وألا نضطر إلى المعاناة من الشلل الرقمي في أي قطاع قبل التحرك بشكل حاسم نحو الحماية الشاملة لأمن الكمبيوتر لدينا.

المبحث الثاني: الإطار القانوني لحماية البيانات الشخصية

لقد أدى التطور التكنولوجي والاقتصاد الرقمي، من بين العديد من العواقب الأخرى، إلى أهمية المعلومات في جميع القطاعات .الشركات ليست معفاة من القيمة المضافة التي يمكن أن توفرها البيانات الشخصية التي تشكل جزءا من أصولها، ولهذا السبب أصبحت معالجتها بالشكل المناسب قضية ذات صلة في السنوات الأخيرة .عوامل مثل الاستخدام غير السليم للمعلومات أو انتهاك إجراءاتها الأمنية تعرض سمعة الشركات للخطر، ويمكن أن تجعلها عرضة للعقوبات، ولهذا السبب لا بد من دراسة الموضوع من المنظور التنظيمي، والتي تشمل: التشريعات ومعايير القطاع والممارسات الجيدة.

ساهمت اللوائح التنظيمية في السياق الوطني في بناء الحق في حماية البيانات الشخصية، وبالتالي في الالتزامات المباشرة للقطاع الخاص والشركات العامة، التي تقوم، كجزء من عملياتها، بمعالجة المعلومات.سيجد القارئ تحليلاً لخلفية الحق في حماية البيانات الشخصية، والقيمة الاقتصادية والاجتماعية للمعلومات، والإطار القانوني فيما يتعلق بحماية البيانات الشخصية التي تحتفظ بها شركات الخدمات ، تحليلاً لمفهوم ومبادئ تفسير هذا الحق، والتحديات والمقترحات لتنفيذ الالتزام بالقانون.

في مجتمع المعلومات والمعرفة، أصبحت إدارة وتبادل البيانات ممارسة شائعة لشركات الخدمات .إن استخدام تكنولوجيات المعلومات والاتصالات موجود في جميع العمليات تقريبًا، مما أدى إلى تحسين مواردها .ومع ذلك، فقد أدت أيضًا إلى سلسلة من التحديات حول أمن المعلومات وحماية البيانات الشخصية والامتثال للوائح المتعلقة بهذا الشأن.

تغطي البيانات الشخصية الموجودة في حوزة الشركات جانبين: من ناحية، مسؤولية الحفاظ على سرية البيانات الشخصية الموجودة في عهدتها، وكذلك طلب موافقة أصحابها، في حالة إرسال أو نقل

المعلومات؛ ومن ناحية أخرى، حق أصحاب البيانات الشخصية في ممارسة حقوقهم في الوصول إلى البيانات الشخصية أو تصحيحها أو إلغائها أو الاعتراض عليها.

ومما سبق، فإن المشكلة المتكررة التي تنشأ بالنسبة للفاعلين القانونيين هي تلك المتعلقة بالامتثال للوائح المتعلقة بحماية البيانات الشخصية التي تحتفظ بها الشركات .هذا مع الأخذ في الاعتبار، أولاً، **الإطار القانوني الوطني الذي يفرض واجبات والتزامات في معالجة البيانات الشخصية**، ومن ناحية أخرى، **التطور التكنولوجي الذي يسمح بجمع أو معالجة أو نقل أو إرسال المعلومات**.

لقياس الأهمية التي اكتسبها الحق في حماية البيانات الشخصية، من الضروري الحديث عن القيمة الاقتصادية والاجتماعية للمعلومات داخل المنظمات .وذلك لأن سمعة الشركة ونموذج أعمالها يعتمدان على الثقة ومعايير حماية البيانات الشخصية وإجراءات أمن المعلومات التي يتم تنفيذها.من المهم معرفة البعد التنظيمي للحق في حماية البيانات الشخصية التي تحتفظ بها شركات الخدمات المنشأة في المكسيك، من خلال التفكير المنطقي المعياري الذي يسمح بتحليل المبادئ والامتثال للالتزامات والواجبات في هذا الشأن، مع مراعاة خصائص هذا الحق من حقوق الإنسان.

المطلب الأول: القيمة الاقتصادية والاجتماعية للبيانات الشخصية

تشكل البيانات الشخصية معلومات داخل الشركات .ولذلك، فهي تتمتع بقيمة عالية، من حيث السمعة الطيبة في الصناعة وتوحيد نماذج الأعمال، من خلال ثقة العملاء والمستخدمين للخدمات المقدمة. حيث تتمتع البيانات الشخصية بقيمة اقتصادية، يمكن مقارنتها ببعض الأصول غير الملموسة، مثل البرامج أو القيمة التجارية لأسماء النطاقات .وقد أدى ذلك إلى اعتبارهم زيت مجتمع المعلومات والمعرفة.

لا بد من القول إن القيمة الاقتصادية الممنوحة لمعلومات الناس لا تكمن في البيانات نفسها، بل في معالجتها وربطها ببيانات أخرى واستخدامها .وهذا يجعل من الممكن الحصول على الربح، من خلال الاستغلال التجاري للجوانب الخاصة الموجهة للاستهلاك، والتي تهتم حتى بالتنبؤ بالسلوكيات والأنماط السلوكية.

قام بعض العلماء بدراسة البعد المتعلق بحماية البيانات الشخصية المكتسبة من خلال استخدام تكنولوجيا المعلومات والاتصالات ويؤكدون أن هناك نماذج أعمال مثيرة يتم إنشاؤها من معلومات الأشخاص في البيئات الرقمية، بحيث تهتم الشركات بالتأثير على التشريعات المحلية المتعلقة بحماية البيانات الشخصية بيانات .وبنفس المعنى، فإنه يؤكد على الحاجة إلى تنظيم الجمع الدولي للبيانات الشخصية، بما يتجاوز عمليات النقل في نفس السياق .

الشركات العالمية، مثل جوجل أو فيسبوك، تبني نموذج أعمالها على معلومات الأشخاص .وبعيدًا عن المناقشة حول ما إذا كانت هذه الممارسة قانونية ومشروعة، يمكننا التأكيد على أن التطور التكنولوجي جعل من الممكن جمع وتخزين ومعالجة كميات كبيرة من المعلومات في الوقت الفعلي، مما أعطى قيمة مضافة للمعلومات.تتيح تقنيات مثل *البيانات الضخمة* للشركات أن تبني قراراتها على تحليل المعلومات، على سبيل المثال، ملف تعريف الاستهلاك الشهري لعملائها، من أجل تعزيز مبيعاتها والحصول على ميزة على عملائها المنافسين.

بمجرد أن تحدثنا عن أهمية البيانات الشخصية والمخاطر المرتبطة بإساءة استخدامها، فمن المناسب إعطاء بعض الأمثلة على أنواع البيانات الشخصية للعملاء والمستخدمين التي قد تكون في حوزة شركات الخدمات المنشأة .يمكن أن تعكس هذه كل شيء بدءًا من المعلومات العامة، مثل الاسم أو العمر أو العنوان، إلى المعلومات المالية المتعلقة بالمدفوعات المقدمة، أو، في أسوأ الحالات، البيانات الحساسة مثل الحالة الصحية.

لذلك، وبقدر ما يثق المستخدمون في أن هذه المعلومات سيتم الاحتفاظ بها مع الالتزام الكامل باللوائح المتعلقة بحماية البيانات الشخصية، والتي تتضمن معايير الممارسات الجيدة وشروط السرية وقواعد الأخلاق، ستحصل الشركات على سمعة جيدة في إدارة البيانات .ولذلك، لن تخضع هذه الشركات للعقوبات المفروضة بسبب انتهاك الحق في حماية البيانات الشخصية.

ومن ناحية أخرى، نجد الشركات التي تنتمي إلى الدولة، والتي يمكن أن تتراوح بياناتها الشخصية من تلك الواردة في الوثائق الرسمية إلى البيانات الشخصية المتعلقة بقضايا السلامة العامة والأمن القومي .ولذلك، فإن الامتثال الصحيح للتشريعات المتعلقة بحماية البيانات الشخصية واضح.

وكما سبق أن قلنا، لا يمكن تقدير القيمة الاقتصادية للمعلومات، بالنظر فقط إلى البيانات الشخصية المعنية، لأنها ستختلف باختلاف استغلالها والأرباح التي يتم الحصول عليها وأنواع الأعمال التي تستخدم فيها .ومع ذلك، يمكننا تقديم تقدير يعتمد على الوضع المحدد لاستغلال المعلومات.

ومن ناحية أخرى، فيما يتعلق بتأثير معالجة البيانات فيما يتعلق بنفقات تشغيل الشركات، فإن قطاعات تجارة الجملة والخدمات المالية وقطاعات الخدمات الأخرى هي تلك التي تخصص قدرًا أكبر من الموارد لمعالجة البيانات والمعلومات الشخصية .ولهذا الغرض، يجب تحديد طبيعة المعلومات، والتي ستتناول الغرض والخدمات التي تقدمها الشركات، وعدد الشركات التابعة وما إذا كانت تشارك المعلومات أو تتلقها مع شركات خارجية.

وأخيرا، ومن الناحية الاقتصادية، يسعى نشر القانون بشأن حماية البيانات الشخصية التي تحتفظ بها أطراف خاصة والقانون العام بشأن حماية البيانات الشخصية التي تحتفظ بها الجهات الملتزمة إلى تحقيق الاتساق لتلبية المعايير .وذلك بحثًا عن تعزيز التبادل التجاري، على سبيل المثال مع الكتل الاقتصادية مثل الاتحاد الأوروبي، الذي تعد لوائحه التنظيمية عالية في هذا الشأن وتحدد المستوى الأمثل من الضمان في حق حماية البيانات الشخصية، لأغراض العلاقات التجارية .

ومما سبق، يمكن اعتبار الحق في حماية البيانات الشخصية عنصرًا أساسيًا لزيادة الاستثمار الأجنبي المباشر بشكل كبير .

المطلب الثاني: الإطار القانوني للحق في حماية البيانات الشخصية

لفهم أهمية الحق في حماية البيانات الشخصية، يجب أن نذكر أهم السوابق الدولية لهذا الحق .وقد نشأ هذا بعد الحرب العالمية الثانية، عندما اعترفت مختلف الصكوك القانونية الدولية، التي تستشهد بالكرامة الإنسانية، بالحق في عدم التدخل في الحياة الخاصة للناس، كحق من حقوق الإنسان الحق في حماية البيانات الشخصية،

عندما يُعترف به كحق من حقوق الإنسان، يكتسب خصائص ومبادئ تفسير حقوق الإنسان .ولذلك، يجب أن تكون مبادئ مثل التقدمية والعالمية حاضرة عند ضمان هذا الامتياز.. اعترفت خطط الحماية الأولى هذه بالحق في الحياة الخاصة والعائلية كحق أصيل للشخص، فضلاً عن الاحترام وعدم التدخل في شؤون المنزل والمراسلات.

مواد المواثيق الدولية المشار إليها هي: المادة 12 من الإعلان العالمي لحقوق الإنسان، بتاريخ 10 ديسمبر 1948؛ المادة 11 من الاتفاقية الأمريكية لحقوق الإنسان لعام 1966؛ المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية بتاريخ 19 ديسمبر من نفس العام 1966؛ المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان بتاريخ 4 نوفمبر 1950؛ وبالمثل، تم التوقيع على ميثاق الحقوق الأساسية للاتحاد الأوروبي في نيس في 7 ديسمبر 2000.

وعلى الرغم من أننا لا نجد اعترافًا صريحًا بالحق في حماية البيانات الشخصية في الصكوك الدولية المذكورة أعلاه، إلا أنه يمكننا أن نؤكد أن هذا الرقم يجد أهم سابقة له في تطور حقوق الإنسان .وبالإضافة إلى ما سبق، لا بد من القول إن كل دولة اختارت تكوين حق عدم التدخل في الحياة الخاصة للناس، من خلال شخصيات قانونية مختلفة، يتألف هذا الاعتراف من اعتراف دستوري بالحق في حماية البيانات الشخصية، والذي تم تطويره في إطار مسلمات العقيدة الأوروبية وخطط التنظيم الذاتي والتقسيم القطاعي للنظام الأنجلوسكسوني.

ومع ذلك، فإن قبول الحق في حماية البيانات الشخصية والاعتراف به كان لا بد من الانتظار حتى عام 2002، مع صدور القانون الاتحادي للوصول إلى المعلومات العامة الحكومية، والذي كان أول نظام قانوني يعترف بالحق في حماية البيانات الشخصية. للمجال العام .ولكن هذا لم يكن سوى تقييد لممارسة الحق في الوصول إلى المعلومات .وبعد ذلك، في عام 2009، منحت الإصلاحات الدستورية للمادتين 16 و73 الاعتراف الكامل بحماية البيانات الشخصية كحق أساسي ومستقل .وبالمثل، أعطت هذه الإصلاحات الكونغرس الاتحادي صلاحيات التشريع في هذا الشأن.

ومع ذلك، تمت الإشارة إلى مشكلتين رئيسيتين: التشريعات المتعلقة بحماية البيانات الشخصية في القطاع العام لم تضمن جميع حقوق الوصول والتصحيح والإلغاء والاعتراض، 11 وكانت المشكلة الثانية تتعلق بعدم وجود لوائح تنطبق على حماية البيانات الشخصية في القطاع الخاص.

وبهذا المعنى، كان ذلك في عام 2010 عندما كانت هناك لأول مرة أحكام صريحة يجب على الشركات مراعاتها عند معالجة البيانات الشخصية في القطاع الخاص، من خلال القانون الاتحادي بشأن حماية البيانات الشخصية التي تحتفظ بها الأطراف الخاصة.

وأخيرًا، في عام 2017، صدر القانون العام بشأن حماية البيانات الشخصية التي يحتفظ بها الأشخاص الملتزمون، ينطبق هذا التشريع على معالجة البيانات الشخصية في القطاع العام .على عكس القانون العام للشفافية والوصول إلى المعلومات، فإن قائمة الموضوعات الملزمة مختلفة: فيما يتعلق بحماية البيانات الشخصية في القطاع العام، سيتم فهم الموضوعات الملزمة على المستوى الفيدرالي ومستوى الولايات والبلديات. أي سلطة وكيان وجهاز وتنظيم للسلطات التنفيذية والتشريعية والقضائية والهيئات المستقلة والأحزاب السياسية والصناديق الاستئمانية والأموال العامة .والذي تم استكمال اللوائح التنظيمية المتعلقة بهذه المسألة في المكسيك معه .وبالتالي، هناك قانونان محددان يحددان الالتزامات والواجبات والإجراءات والعقوبات والموارد في هذا الشأن، لكل من القطاعين العام والخاص.

الفرع الأول: مفهوم ومبادئ تفسير الحق في حماية البيانات الشخصية

لفهم أهمية الحق في حماية البيانات الشخصية في مجتمع المعلومات والمعرفة، فيما يتعلق بالحق في الوصول إلى المعلومات، فإن اسم الموظف العام ومعلومات الاتصال به هي بيانات شخصية (لأنها تسمح بالتعرف على الفرد)، ولكنها ليست بالضرورة سرية –كما تملي القاعدة العامة .وهذا يفرض تحديات على الفاعلين القانونيين، من أجل تقييم المواقف وتحديدها بطريقة جدلية، بغض النظر عن اثنين أو أكثر من حقوق الإنسان في النزاع.من الضروري تحليل مكونات المفهوم، وكذلك تصنيف البيانات الشخصية، وفقًا لنوع المعلومات التي تعكسها.وبهذا المعنى، فإن مالك البيانات الشخصية هو الفرد نفسه وحمايته حق معترف به

مؤخرًا في المكسيك .تعتبر بيانات الفرد شخصية وله الحق في السرية والسرية أو في تغطية أكبر لحرية الخصوصية.

تشير البيانات الشخصية إلى معلومات الفرد، والتي تسمح بالتعرف عليه من خلال وصفه وأصله ومكان إقامته ومسيرته الأكاديمية والعملية، من بين أمور أخرى .يمكن أن تكون البيانات الشخصية أيضًا حساسة، وتصف جوانب تتعلق بالفرد، مثل طريقة تفكيره، وحالته الصحية، وخصائصه الجسدية، وأيديولوجيته، وحياته الجنسية، من بين أمور أخرى .

ليست كل البيانات الشخصية تتمتع بنفس الصرامة في الحماية، ويشير إلى التمييز الذي وضعه فيما يتعلق بدرجة حمايتها في:

- البيانات التي يتم تداولها بحرية، مثل تحديد الهوية: الاسم واللقب ووثيقة الهوية والهوية الضريبية أو التقاعدية والمهنة وتاريخ الميلاد والعنوان.
- الذين يقتصر تداولهم على قطاع أو نشاط معين، ويكونون عرضة للعلاج ما دام تقديم مبرر مشروع وبالحدود التي تترتب على ذلك التخصص.
- تلك التي يُمنع جمعها، لأنها تؤثر على الخصوصية الشخصية أو العائلية، والتي تسمى البيانات الحساسة .

قدمت العديد من الصكوك تعريفًا للبيانات الشخصية، ومن بينها اتفاقية مجلس أوروبا رقم 108 لحماية الأفراد فيما يتعلق بالمعالجة الآلية لبياناتهم الشخصية، بالإضافة إلى المبادئ التوجيهية لمنظمة التعاون والتنمية الاقتصادية. بشأن حماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود والتوجيه EC 46/95/ الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن حماية البيانات الشخصية الصادر في عام 1995. ويعرّف هذا الأخير البيانات الشخصية بأنها "جميع المعلومات المتعلقة شخص طبيعي محدد أو يمكن تحديد هويته.

يُعرّف القانون بشأن حماية البيانات الشخصية التي تحتفظ بها أطراف خاصة البيانات الشخصية بأنها أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديد هويته .ويقدم تعريفًا للبيانات الشخصية الحساسة،

تلك التي تشير إلى البيانات الشخصية التي تؤثر على المجال الأكثر حميمية لصاحبها أو التي يمكن أن يؤدي استخدامها غير السليم إلى التمييز أو ينطوي على خطر جسيم على المالك تعتبر البيانات الحساسة بيانات يمكن أن تكشف عن جوانب مثل الأصل العرقي أو الإثني، والحالة الصحية الحالية والمستقبلية، والمعلومات الجينية، والمعتقدات الدينية والفلسفية والأخلاقية، وعضوية النقابات، والآراء السياسية، والتفضيل الجنسي ..

هناك العديد من خصائص البيانات الشخصية، والتي تعتمد أهميتها ومعناها على استخدام المعلومات التي تشكلها .بمجرد تحديد مفهومي البيانات الشخصية والبيانات الشخصية الحساسة، سيتمكن القارئ من ملاحظة أن المعلومات التي تستخدمها شركات الخدمات المنشأة تشمل هاتين الفئتين من البيانات، ولهذا السبب يعد الامتثال للتشريع أمرًا ضروريًا .بمجرد تحليل مفهوم الحق في حماية البيانات الشخصية، فمن الضروري الحديث عن المبادئ المتعلقة بهذا الشأن .ولهذا الغرض، من المناسب تحديد المقصود بالمبدأ في المجال القانوني .وفقًا لأليكسي، فإن المبادئ هي تفويضات التحسين؛ أي أنها قواعد تأمر بأداء الشيء في حدود الإمكانيات القانونية والحقيقية.

تتميز هذه المبادئ بإمكانية تحقيقها بدرجات مختلفة، حيث أن تحقيقها لا يعتمد على الإمكانيات الحقيقية فحسب، بل على الإمكانيات القانونية أيضًا .وهذا بدوره تحدده القواعد، وقبل كل شيء، المبادئ التي تعمل في الاتجاه المعاكس.

الفرع الثاني: مبادئ حماية البيانات الشخصية

إن الحق في حماية البيانات الشخصية له مبادئ منصوص عليها في التشريعات المطبقة على إدارة المعلومات، سواء بالنسبة للشركات العامة أو الخاصة.

- مبدأ الشرعية: يجب جمع البيانات الشخصية بشكل قانوني، وفقًا للأحكام المنصوص عليها في التشريع المتعلق بالبيانات الشخصية .لا يمكن الحصول على البيانات من خلال طرق خادعة أو احتيالية .
- مبدأ الغرض: يجب تبرير جميع عمليات معالجة البيانات الشخصية التي يقوم بها المراقب بأغراض محددة وقانونية وصريحة ومشروعة، تتعلق بالصلاحيات التي تمنحها اللوائح المعمول بها، أو في حالة

الشركات الخاصة، أن معالجة البيانات تقتصر البيانات الشخصية على الامتثال للأغراض المنصوص عليها في إشعار الخصوصية .

- مبدأ الولاء: لا يجوز للشخص المسؤول الحصول على البيانات الشخصية ومعالجتها من خلال وسائل خادعة أو احتيالية .سيتعين عليها إعطاء الأولوية لحماية مصالح مالك البيانات الشخصية والتوقع المعقول للخصوصية، وسوف تضمن الامتثال لمبادئ حماية البيانات الشخصية المنصوص عليها في التشريع، ويجب أن تتخذ التدابير اللازمة لتطبيقها .
- مبدأ الموافقة: ستخضع جميع معالجة البيانات الشخصية لموافقة مالكها، باستثناء الاستثناءات المنصوص عليها في التشريعات المتعلقة بهذا الشأن .وتكون الموافقة صريحة عندما يتم التعبير عن الوصية شفهياً، أو كتابياً، أو إلكترونياً، أو بصرياً، أو أي تقنية أخرى، أو بالإشارات الواضحة .سيكون من المفهوم أن المالك يوافق ضمنيًا على معالجة بياناته عندما لا يعرب عن معارضته، بعد أن أتاح له إشعار الخصوصية .في حالة البيانات الشخصية الحساسة، يجب على الشخص المسؤول الحصول على موافقة كتابية صريحة من المالك لمعالجتها، من خلال التوقيع المكتوب بخط اليد أو التوقيع الإلكتروني أو أي آلية توثيق منشأة لهذا الغرض، باستثناء الاستثناءات التي ينص عليها القانون .
- مبدأ الجودة: يتأكد الشخص المسؤول من أن البيانات الشخصية الواردة في قواعد البيانات ذات صلة وصحيحة ومحدثة وفقًا للأغراض التي تم جمعها من أجلها .من المفترض أن يتم تلبية جودة البيانات الشخصية عندما يتم تقديمها مباشرة من قبل المالك وحتى يعلن المالك ويثبت خلاف ذلك .
- مبدأ التناسب: ستكون معالجة البيانات الشخصية هي ما هو ضروري ومناسب وذو صلة فيما يتعلق بالأغراض المنصوص عليها في إشعار الخصوصية .يجب على المراقب معالجة البيانات الشخصية المناسبة وذات الصلة والضرورية تمامًا للغرض الذي يبرر معالجتها فقط .

- مبدأ المعلومات: يلتزم الشخص المسؤول بإبلاغ أصحاب البيانات بالمعلومات التي تم جمعها منهم والغرض منها .يجب على الشخص المسؤول إبلاغ المالك، من خلال إشعار الخصوصية، بوجود المعالجة التي ستخضع لها بياناته الشخصية وخصائصها الرئيسية، حتى يتمكن من اتخاذ قرارات مستنيرة في هذا الصدد .وبالمثل، يشير هذا المصطلح إلى السلطة التي يمنحها القانون لمعرفة مقدمًا الخصائص الأساسية للمعالجة التي ستخضع لها البيانات الشخصية المقدمة إلى كيان أو شركة خاصة .يجب أن يكون إشعار الخصوصية مكتوبًا بلغة واضحة ومفهومة.
- مبدأ المسؤولية: يجب على الشخص المسؤول اتخاذ التدابير اللازمة والكافية لضمان احترام إشعار الخصوصية الذي تم إبلاغ المالك به في جميع الأوقات من قبله أو من قبل أطراف ثالثة تربطه به علاقة قانونية .

بالإضافة إلى المبادئ السابقة، هناك واجبات تتعلق بحماية البيانات الشخصية .وتتكون هذه من الحفاظ على سرية المعلومات ووضع تدابير أمنية للمعلومات، مناسبة ومتساوية لتلك التي تستخدمها الشركات لتخزين معلوماتها الخاصة.

أخيرًا، فيما يتعلق بمبادئ الحق في حماية البيانات الشخصية، فإن القوانين المحددة في هذا الشأن لا تعترف صراحةً بمبدأ المصالح الفضلى للقاصر .ومع ذلك، فإن تطبيقه ذو طبيعة عرضية، ليس فقط فيما يتعلق بالحق في حماية البيانات الشخصية، ولكن أيضًا فيما يتعلق بالحماية الفعالة لحقوق الإنسان .ويمكن الاحتجاج بهذا المبدأ عندما يتعلق الأمر بحماية بيانات الأطفال أو المراهقين، مما يعني الحماية الأوسع لهم، وفقا للتشريعات المتعلقة بهذا الشأن .

الخاتمة

إن الحق في عدم التدخل في الحياة الخاصة للأشخاص هو حق من حقوق الإنسان معترف به منذ الإعلان العالمي لحقوق الإنسان لعام 1948. ومع ذلك، كان الاعتراف الصريح بنظام حماية البيانات الشخصية التي بحوزة الشركات أمرًا ضروريًا. حتى عام 2010، مما أدى إلى فجوة في التنظيم في هذا الشأن.

البيانات الشخصية لها قيمة اقتصادية واجتماعية عالية .وفي حمايتها تكمن فرصة لتوليد الثقة بين العملاء ومستخدمي الخدمة، من أجل تعزيز نماذج الأعمال.

على الرغم من أن تعزيز التنظيم المتعلق بحماية البيانات الشخصية للشركات المنشأة يتناول ضمان حق من حقوق الإنسان، إلا أنه يجد أصله أيضًا في الجوانب الاقتصادية على المستوى الدولي .لقد كان تحقيق معايير المستويات الكافية لحماية المعلومات شرطًا لكي تعلن الدولة أنها آمنة في التبادل التجاري.

على الرغم من أن الإطار القانوني المتعلق بحماية البيانات الشخصية التي تحتفظ بها شركات الخدمات المنشأة يتضمن معايير دولية ويوفر ضمانات للحماية الفعالة لهذا الحق، فإن الامتثال للأحكام يواجه تحديات كبيرة .ومن الأمثلة على ذلك عدم المعرفة بالآثار القانونية لمعالجة المعلومات، وانعدام الأخلاقيات في المعالجة المذكورة، وعدم الحساسية من تداعيات سوء استخدام المعلومات، وعدم المعرفة بالآليات القانونية للمطالبة بهذا الحق.

يعد الحق في حماية البيانات الشخصية أحد حقوق الإنسان المعترف بها على المستوى الدستوري، وبالمثل، فهي تعترف بالتشريعات القطاعية، التي تفرض أحكامًا محددة، على سبيل المثال، عندما يتعلق الأمر بالبيانات الضريبية أو المالية أو الصحية .ولهذا السبب يحتاج المشغلون القانونيون إلى معرفة مجموعة من المستندات، بعضها غير ملزم، حتى يتمكنوا من الامتثال لجميع متطلبات حماية المعلومات.

تساعد مبادئ الحق في حماية البيانات الشخصية على تفسيره، خاصة في مواجهة تصادم حقوق الإنسان مثل الوصول إلى المعلومات وحماية البيانات الشخصية .وبهذا المعنى، وعلى الرغم من عدم الاعتراف به صراحة

في القانون في هذا الشأن، فإن مبدأ المصلحة الفضلى للقاصر يجب أن يؤخذ في الاعتبار كمحور عرضي في ضمان البيانات الشخصية للفتيات والفتيان والمراهقين.

إن الامتثال للتشريعات المتعلقة بحماية البيانات الشخصية التي تحتفظ بها شركات الخدمات هو الحد الأدنى، نتيجة للجهل بالقانون .تجدر الإشارة إلى أن خطط الممارسات الجيدة والاستخدام الأخلاقي للمعلومات يمكن أن تؤدي إلى ضمان فعال للحق في حماية البيانات الشخصية، حتى أفضل من القانون نفسه.

المراجع :

2015, GEG. *NORMES FACULTATIVESET NON CONTRAIGNENTESDE COMPORTEMENT DES ETATS.* NEW YORK: NATIONS UNIES.

AGNU. (2024). الاتفاقية الدوليةالعامة لمكافحة استعمال تكنواوجيات المعلومات والاتصالات للاغراض الاجرامية.

DURKHEIM, É. (1983). *Les règles de la méthode sociologique.* Paris: PUF.

JORF. (6 janvier 1978, 1 6). Les « données » désignent les informations créées et utilisées par le biais d'un logicieiL du , , 7 janvier 1978 (Légifrance. *JORF* .

M, L. (2012). *Cyberspace is Not a War Fighting Domain.* Journal of Law and Policy.

ONU. (2021). ONU.

ONU. (2013). *الدورة68.* ONU. ONU.

ONU. (2015). *الدورة70.* ONU.

otan. (2022). *droit international de cyberspace.* https://cyberlaw.ccdcoe.org/wiki/category:national_position.

OTAN. (2013-2017). *TALLIN.* OTAN.

ROBERT, M. (février 2014). *Rapport sur la cybercriminalité,.*

Thomson, I. (2007). La Russie impliquée dans la cyber-attaque contre l'Estonie. *"Russia 'hired botnets' for Estonia cyber war. 3.* LONDON: journaldunet.com.